電子記録応用基盤に関する
調査検討報告書 2012

-ケース指向電子記録管理及び電子署名の新たなパラダイム-

電子記録応用基盤フォーラム(eRAP)

平成25年3月

一般財団法人日本情報経済社会推進協会

序　文

組織として記録を適切に管理、活用することによるメリットは多い。例えば、外部監査での説明責任を果たす際に利用する、あるいは新たな業務を行う際に過去似たような業務で作成した記録を活用し、効率的にかつ質の高い業務活動につなげるなどが挙げられる。一般に記録を適切に管理することにより、現在組織活動に求められている「スピード・グリーン・効率性・透明性・安全性・持続性・創造性」の実現に有効であるとされ、組織活動を推進、発展させるために不可欠である。

このように記録管理は組織活動にとって重要であるにもかかわらず、日本の記録管理は、属人的で、かつ組織全体で記録を管理活用する、組織全体の共有財産であるという意識が薄く、適切な記録管理が行われているとは言い難い状況である。人材の流動性が少なく、同じ文化の人同士で組織活動を行う社会を前提にした場合は、このような属人的な記録管理でも組織活動を推進することが出来ていたが、企業の事業の多角化、グローバル化、コンプライアンス重視、業務効率化が進む中、属人的な記録管理では対応できない場合が多くなってきた。また、ビッグデータに代表される膨大な電子情報を扱うなど、記録管理の手法も変えていかなければならない状況である。

更に、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管理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管理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、ケース管理をはじめとする電子記録管理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(eRAP)はかかる状況に鑑み平成 22 年 4 月に発足し、次世代電子商取引推進協議会(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を電子記録管理の分野に生かし、電子記録管理を推進してきた団体、企業、個人と連携をとり、また、ETSI(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。

本報告書は、一般財団法人日本情報経済社会推進協会(JIPDEC)の eRAP が平成 23 年度に実施した、ケース指向電子記録管理システムの適用事例や実証実験、システム間の相互運用性を確保するためのパッケージ構造、記録管理の成熟度モデル、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。本報告書が、電子記録管理の発展の一助になれば幸いである。

平成 25 年 3 月

一般財団法人日本情報経済社会推進協会

目　次

第１部　電子記録マネジメント基盤

まえがき

日本の企業における記録管理の現状は、法定保存文書を除けば、最終文書に至るまでの記録が残っていないこと以前の問題として、最終文書を管理した状態で残すことすら十分とは言えず、折角残された記録も十分に活用されているとは言い難い。

電子記録応用基盤フォーラム(以下“eRAP”とする)はこのような現状に鑑み、以下の 3 点を主要課題と認識し検討を進めてきた。

・業務遂行者が記録する負担の軽減(業務遂行に伴い自然と記録が残る)
・最終文書・結果だけでなくそれに至った経緯・判断材料の記録
・記録した文書の全社横断的な活用

本報告書では、これらの課題に対する eRAP の 3 年間の活動の総括として、「ケース指向電子記録管理システム」を提案しその有効性を提示するとともに、組織の記録管理の成熟度モデルなど記録管理関連の調査検討結果を述べる。

第 1 部の各章・節の内容は次の通りである。

第 1 章「ケース管理とは」では、まず「はじめに」において、現状の日本企業における記録管理の現状と課題、及びその解決策としての「ケース指向電子記録管理システム」を概説する。この部分は、「ケース管理」に馴染みのない読者への導入部となっている。

続いて、1.1 節から 1.4 節において、日本型記録管理の問題とその解決策としてのケース管理、非定型業務へのケース管理の導入について述べ、最後に一事例として、豊島区役所殿の統合文書管理システムを紹介する。

第 2 章「ケース指向電子記録管理システムの適用」では、2.1 節から 2.4 節にかけて「ケース指向電子記録管理システム」の実装や応用について述べる。

まず 2.1 節で、業務中心の「ケース指向電子記録管理システム」の目的を述べ、2.2 節で「ケース指向電子記録管理システム」の特徴、アーキテクチャを紹介し、実装のサブセットを提案する。

2.3 節では、住宅施工業務及びプロジェクト管理への「ケース指向電子記録管理システム」の適用事例と課題について述べる。

最後に、2.4 節で既存のツールを用いて実際の業務にケース管理を適用した実証実験結果を紹介する。

第 3 章「パッケージ構造」では、記録とメタデータ、及びケースとメタデータを一体化するパッケージの標準形式案を紹介する。読者が本章だけ読んでも完結するよう、3.1 節に「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とケース管理について概略を加えた。パッケージ構造については、3.2 節でパッケージに関する標準化動向を述べ、3.3 節で eRAP が提案するパ

ッケージ構造を紹介し、3.4 節にその課題を述べる。

第 4 章「記録の管理と成熟度モデル」では、4.1 節から 4.3 節にかけて既に存在する記録管理関連標準と、これから注目されると考えられる、組織の記録管理の成熟度モデルを紹介する。

4.1 節では、組織における記録管理の成熟度モデルとして、米国の“情報ガバナンスに関する成熟度モデル”(ARMA International Maturity Model for Information Governance)と、豪州の HB-278:2009 (Recordkeeping Compliance)について概説するとともに、成熟度評価ツールの留意点を述べる。4.2 節では、広く知られた記録管理の標準を紹介し、4.3 節で、eRAP が提案する記録管理モデルの概念図を紹介する。

最後に、第 1 部「電子記録マネジメント基盤」執筆にあたり、適切な助言とご支援を頂いた豊島区役所の高橋邦夫氏、日本マイクロソフト株式会社の米野宏明氏に心から感謝申し上げるとともに、本報告が、日本の記録管理の現状打破の一助として活用されれば幸いである。

第１章　ケース管理とは

(現状)

日本企業における記録管理の現状は、概ね以下のような状態にある。

・法定保存文書を除けば、最終文書を管理した状態で残すことすら、十分とは言えない。

・最終文書になった経緯を残すことが、必要とされる状況にはなって来たが、経緯まで、記録に残そうとすると業務遂行する人の負担が大きく、記録が残らない。

・せっかく残された記録が十分に活用されていない。

(課題)

eRAP では、このような状態の対策をすべく、以下の 3 点課題として検討を進めた。

①業務遂行に伴い自然と記録が残ることを目指し、業務遂行者が記録する負担を軽減する。

②最終文書・結果だけでなく、それに至った経緯・判断材料も残す。

③記録した文書を組織横断的に活用する。(作成した人以外が、活用しやすい)

企業の業務は概ね図 1-1 のように、業務の案件(ケース)毎に、文書中心ではなく、業務中心で遂行される。このような業務の案件毎に管理する手法はケース管理と呼ばれるが、ケース管理では、業務記録をケースファイルに記録し、また、過去のケースファイルを参照しながら、業務を遂行する。

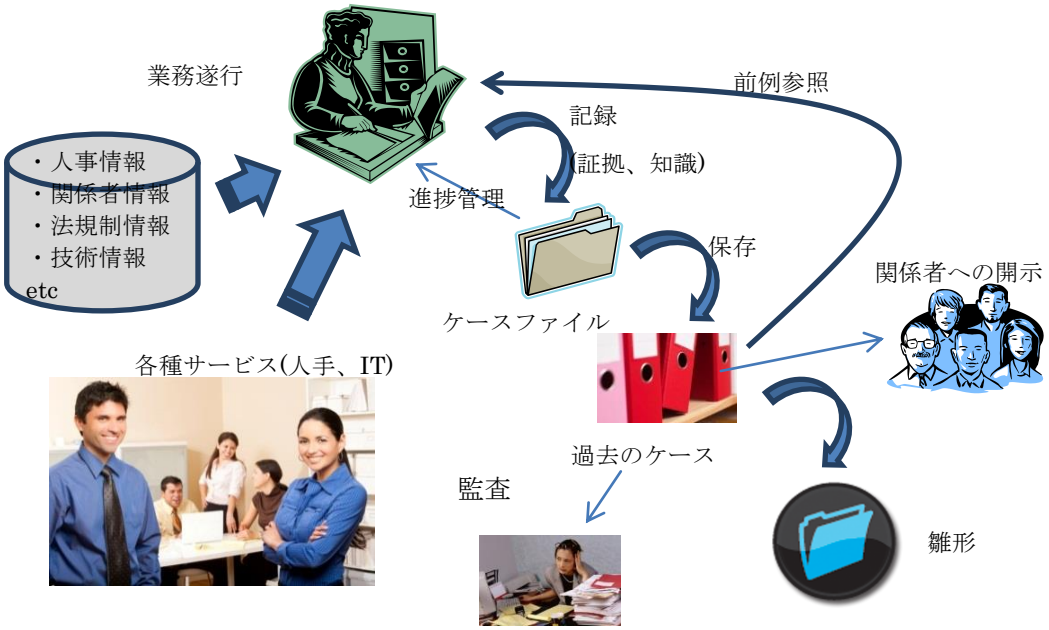


図 1-1　業務の遂行とケース管理のイメージ

(対策)

本報告では、上記①、②、③の対策の実現を支援する手段として、従来の電子文書管理システムにケース管理から見たインタフェース、管理機能、可視化機能を持った「ケース指向電子記録

管理システム」を提案し、その有効性を提示する。

企業における「ケース指向電子記録管理システム」導入検討にあたっては、ケース管理の対象とする業務の分析や最終文書・結果に至った判断材料も残すための記録の識別は、このシステムの外の事項であり、並行して検討する必要がある。

「最終文書・結果に至った経緯・判断材料も残す。」とはどういうことなのか会社間の契約書を例に挙げ説明を行う。契約文書の場合、最終成果物は、契約書そのものと、契約する決裁者が契約を決裁した決裁文書である。一方、契約書の締結には図 1-2 のようなプロセスを踏むものと仮定する。

①契約書原案作成(または入手)とその契約主旨説明書の作成を行う。
②法務部等の社内関連部署から契約書に関する指摘点や留意事項を受け取る。
③それら指摘事項や留意事項をもとに、契約先と電子メールや打合せ等で交渉する。
④社内関連部署の指摘事項への対応まとめと最終契約書案の作成を行う。
⑤決裁者への補足説明書を作成する。
⑥決裁者に、補足説明書を利用して契約内容を説明し、契約決裁を頂く。

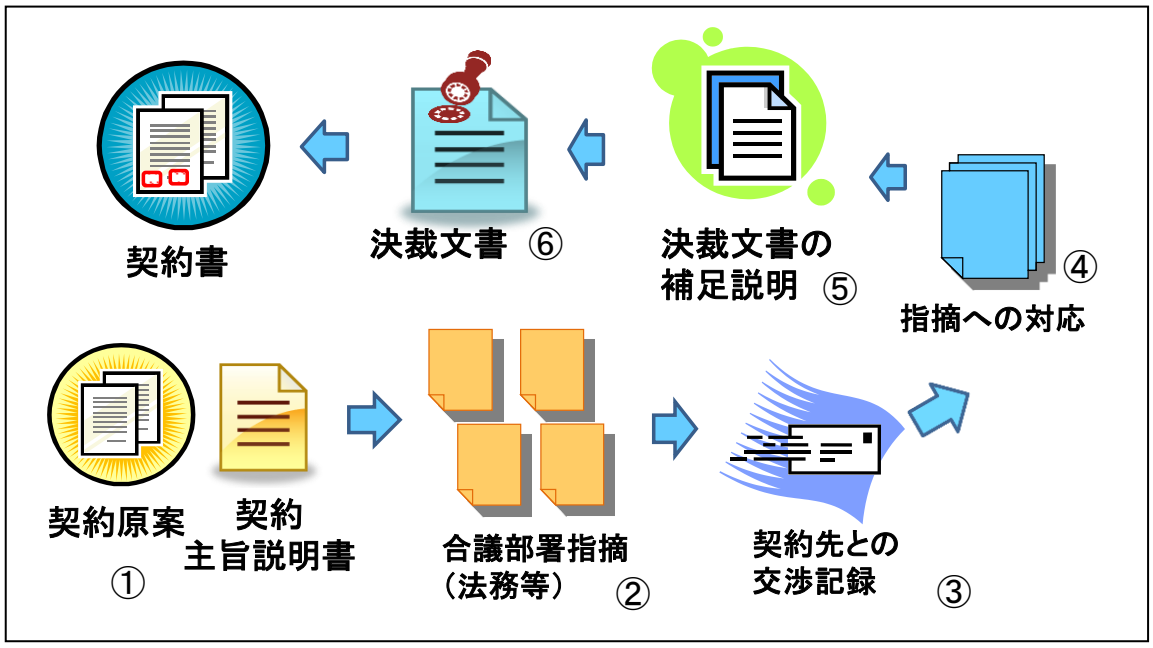


図 1-2　契約プロセス

契約書は、その性質上、自社もしくは相手先どちらか一方が有利になっていることが多く、次案件に利用・流用する際、自ら相手有利な条件を提示しないためには契約に至った経緯、特に④の「指摘への対応まとめ」を残して置くことが必要である。また、契約先とのトラブルを防ぐためには、③「契約先との交渉記録」を残して置くことも効果がある。

「最終文書・結果に至った経緯・判断材料も残す。」という意味では、どの段階の文書までを残すのかは各社のポリシに委ねられるが、最終契書に至った判断材料を残すためには、少なくとも⑤「決裁文書補足説明」や④「指摘への対応まとめ」までは記録として残すのが妥当である。

eRAP が提案する「ケース指向電子記録管理システム」は従来の電子文書管理システムに加えて、次の 2 つの特徴を持つ。

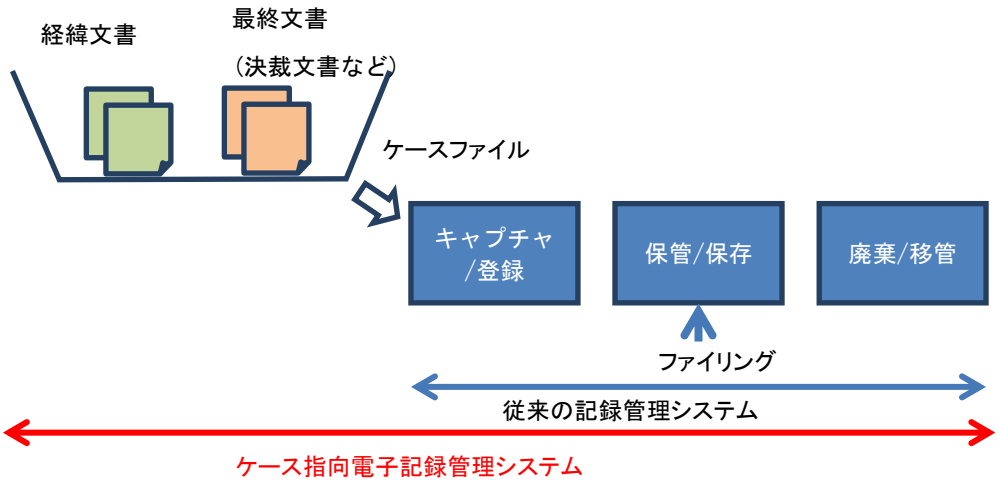


図 1-3　ケース指向電子記録管理システム　モデル

①図 1-3 のように、最終文書だけでなく、そこに至るまでの経緯を含む必要十分な文書を関連付けて、1 つの入れ物(ケース)で管理できる。
②活用のために、ケースや文書に付随するメタデータ(ケースや文書の ID、説明、日時、事象(受理、作成、参照など)を共に管理できる。

2010 年から eRAP では、デンマーク政府が導入しているケースマネジメントをはじめとして、韓国、ハンガリ、ドイツ、イギリス、シンガポールなどの電子文書管理システムについて、調査してきた。「ケース指向電子記録管理システム」の実現のため、ケースマネジメントシステムとして完成度の高いデンマークのケースマネジメントシステムを参考にした。

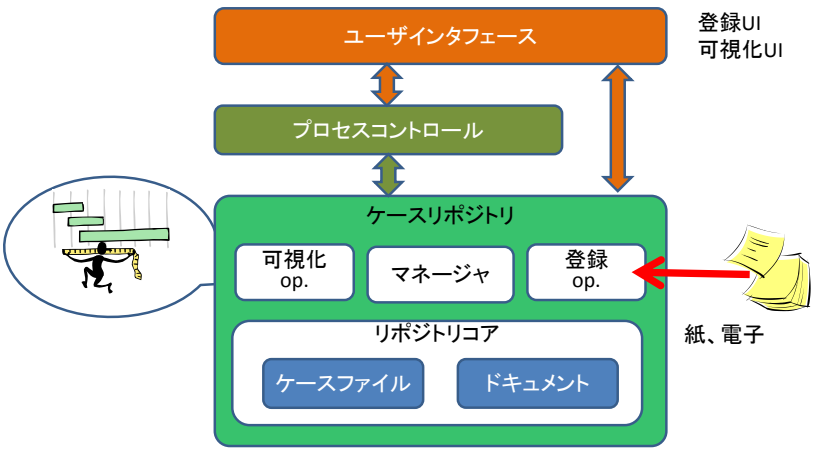


図 1-4　eRAP の提案する「ケース指向電子記録管理システム」のアーキテクチャ

しかしながら、デンマークの「ケースマネジメント」のシステムは、高度なインプリメンテー

ションをしているため、そのままの形では導入に相当の時間を要するとの認識から、国内企業への導入を容易にした形での図 1-4 のようなアーキテクチャを提案する。

また、eRAP の提案する「ケース指向電子記録管理システム」のアーキテクチャを実装している製品や、実証実験また適用例の検討などを通し、その有効性を確認した。

1.1　日本型記録管理の問題

日本型業務遂行と欧米型業務遂行の差を図 1-5 に示し、その結果、記録管理に、どのような差異が生じていたか。また、昨今の環境の変化に対し、対応すべきことについてまとめた。

日本型業務遂行では、これまで長期雇用慣行を前提としていたため、業務遂行はボトムアップで実施され、チーム作業が重視される中で、責任が曖昧になっていた。このような背景の下、調整／根回しを重用視するものの、記録は属人的になり、組織的に継承されづらい状況にあった。

一方、欧米型業務遂行では、契約ベースであり、いつ従業員がやめるかも知れない、また、いつ従業員をやめさせるかも知れないという随意の雇用形態を前提としているため業務遂行はトップダウン的に実施され、従業員は細かな職務記述に従うため、責任も明確である。

そのため、業務の定型化が進み、記録も組織的に管理されていた。

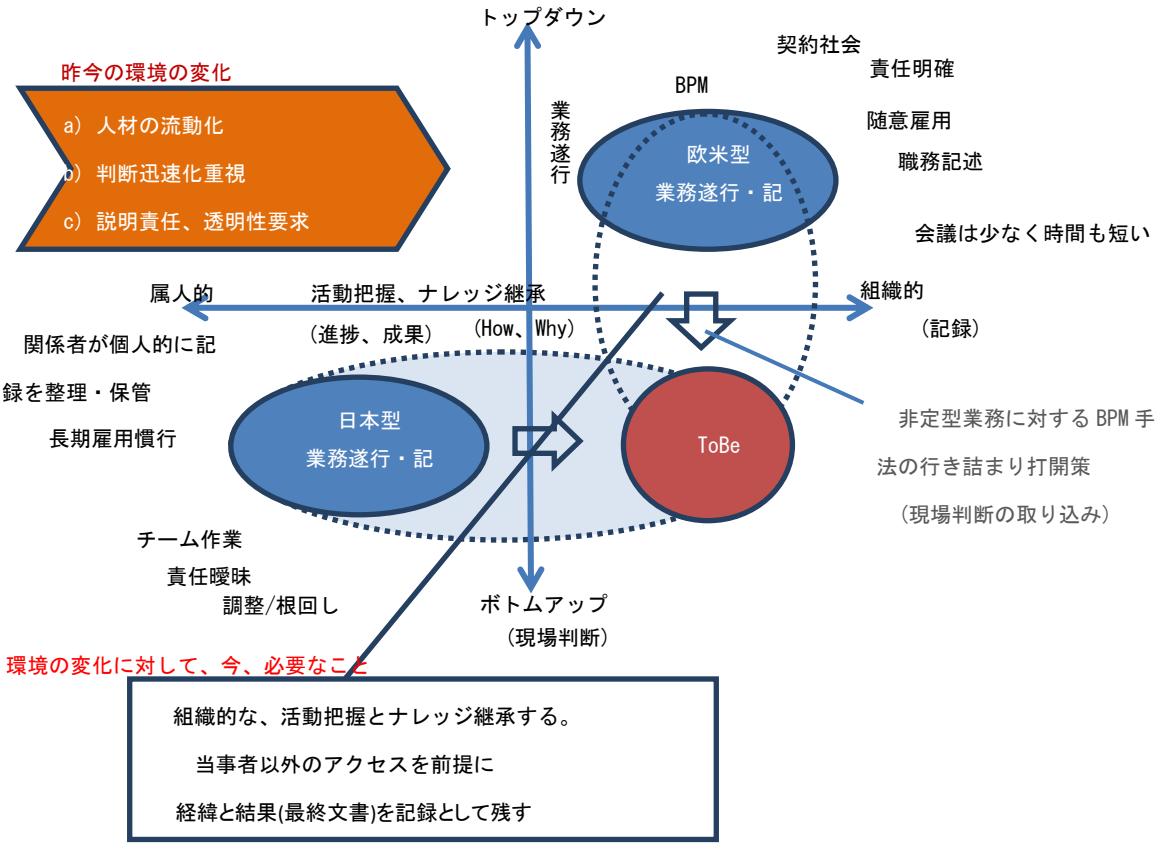


図 1-5　日本型記録管理と欧米型記録管理の差異

昨今は日本でも、以下のように環境が変化している。

⑴人材の流動化が激しくなった。
⑵判断の迅速性が重要視される。
⑶判断の説明責任、透明性が要求される。
⑷業務が複雑化し、その情報量は爆発的に増えた。

そこで、求められるのは、組織的な活動の把握とナレッジの継承である。属人的にならないよう当事者以外でも利用できる形態で、経緯と結果を残すことが必要である。しかしながら、「経緯まで、記録に残そうとすると業務遂行する人の負担が大きく、記録が残らない。」という課題を抱えている。

1.2　日本型記録管理の問題解決とケース管理

これまで長期雇用の慣例から法定保存文書を除けば、最終文書をきちんと残すこと自体十分な状態とはいえない状況であり、今後の課題は次の 3 点である。

①業務遂行に伴い自然と記録が残ることを目指し、業務遂行者が記録する負担を軽減する。
②最終文書・結果だけでなく、それに至った経緯・判断材料も残す。
③記録した文書を組織横断的に活用する。(作成した人以外が、活用しやすい)

図 1-6 のような「ケース管理」の手法で実施した業務結果について、記録管理について、「業務毎にケースファイルを作成し」、「最終文書・結果だけでなく、経緯も残し」、「関係者からの参照を許す」ことを実現する「ケース指向」の機能をもった記録管理システムを導入することが、解決への道筋となる。

ただし、活用のために、どの範囲まで経緯として残すのかは、システムの範囲外ではあるが、重要な事項である。

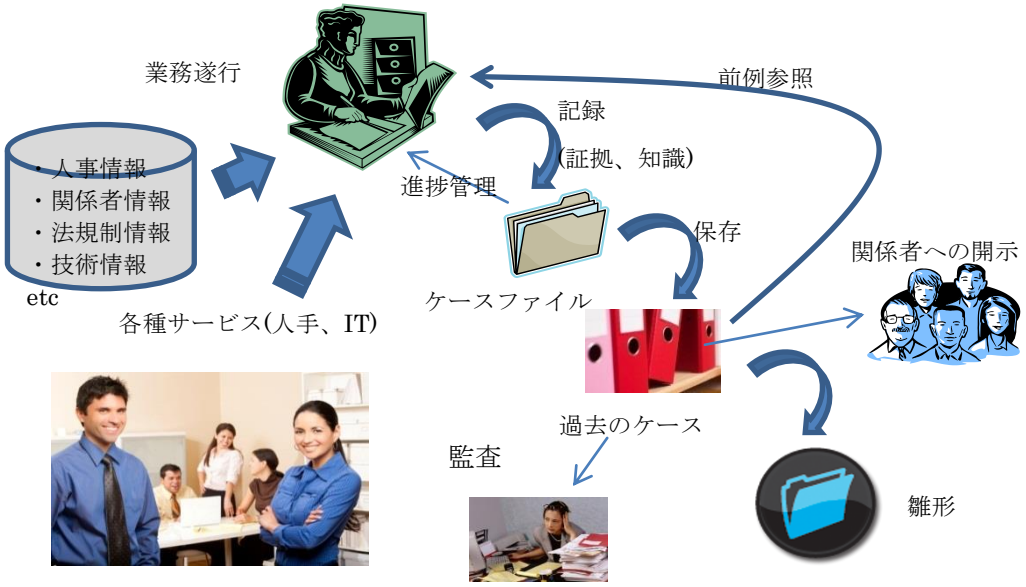


図 1-6　業務の遂行とケース管理のイメージ

1.3　非定型業務への対応例

業務には、大きく分けて、定型業務と非定型業務がある。案件(ケース)の中の最小の実行単位を「タスク」として定義し、管理していくことで、非定型業務の記録が管理しやすくなる。すなわち、記録定型業務の場合、例えば、図 1-7 のように、案件(ケース)は、タクス 1、2、3 で構成される。それぞれのタスクの進行に合わせて、結果・経緯をケースファイルに記録できる。

一方、非定型業務の場合、例えば、図 1-8 のように、タクス 1、2、3 で 1 つのケース(業務)が完了していたところに、新たなタスクをタスク 2 と 3 の間に実施する必要が生じた場合、新たなブランクタスクを生成し、ケースの中、タスク 2 と 3 の間に埋め込み、それぞれのタスクの進行に合わせて、結果・経緯をケースファイルに記録できる。

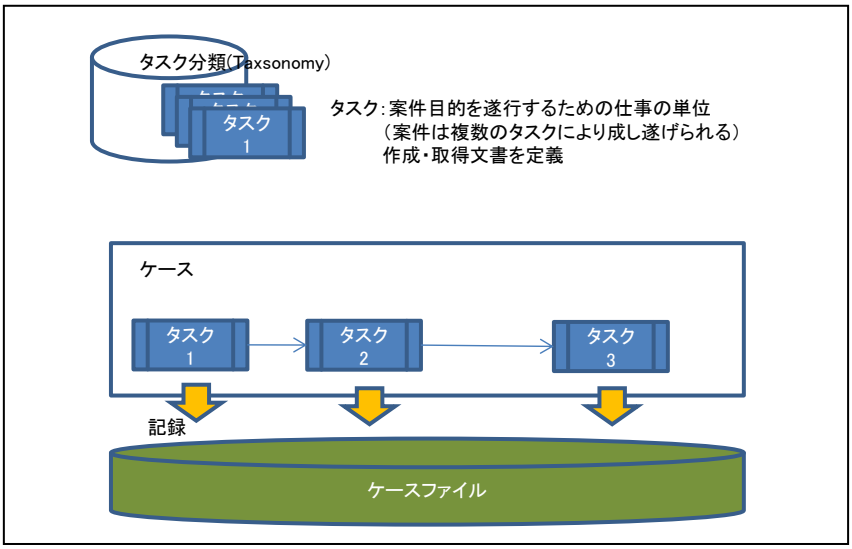


図 1-7　定常業務の記録

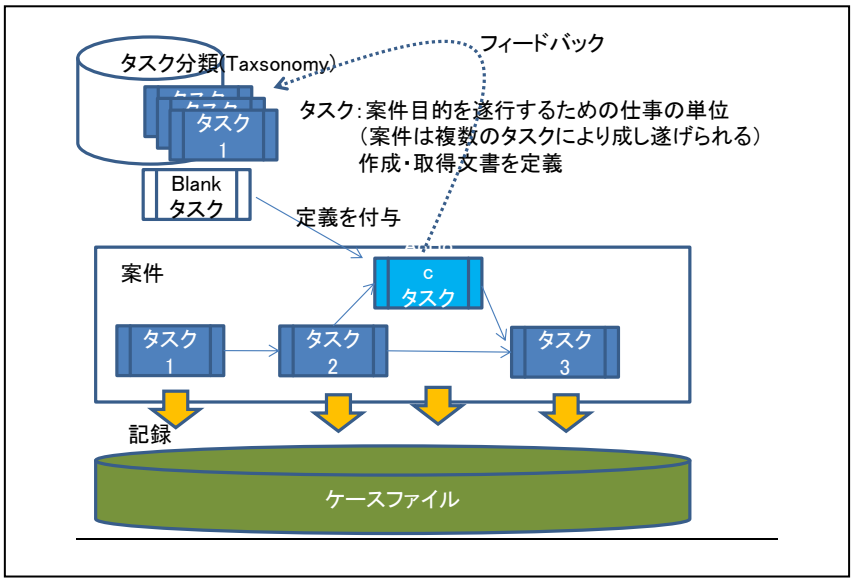


図 1-8　非定型業務の記録の例

1.4　ケース管理の視点から、豊島区役所殿　統合文書管理システムの例

豊島区役所殿では、区役所移転計画と同期して、行政文書の統合文書管理システムを新たに平成 21 年度から稼働させている。このシステムについて、ケース管理の視点からヒアリングと分析を行った。「図 1-9　豊島区が目指す統合文書管理システム」を参照しながら説明する。

(経緯)

数年前まで職場で、紙情報が山積となり、パソコンやファイルサーバに情報が溢れており、「他人の担当している業務文書をすぐ取り出せない。」のような文書管理の状況であった。新庁舎移転を契機に区民に開かれた庁舎を目指すこととなり、情報の一元管理を目指すこととした。

(先行事例分析)

先行導入した多くの自治体から「文書管理システムを導入したものの、電子化が思ったほど、進んでいない。」という情報を得た。これを、図 1-9 の上半分に示す。収受から起案、決裁、施行、公開、保管を受け持つ文書管理システムとそこに起案文書の作成が分かれており、2 重管理になっている。また、起案文書はファイルサーバやローカル PC、グループウェアなどで作成されており、管理された状況にはなっていなかった。

ケース管理視点で言えば、「最終文書」は管理された状況にあるが、その判断材料である「経緯文書」、「最終文書の原稿」を辿ることは困難な仕組みであった。

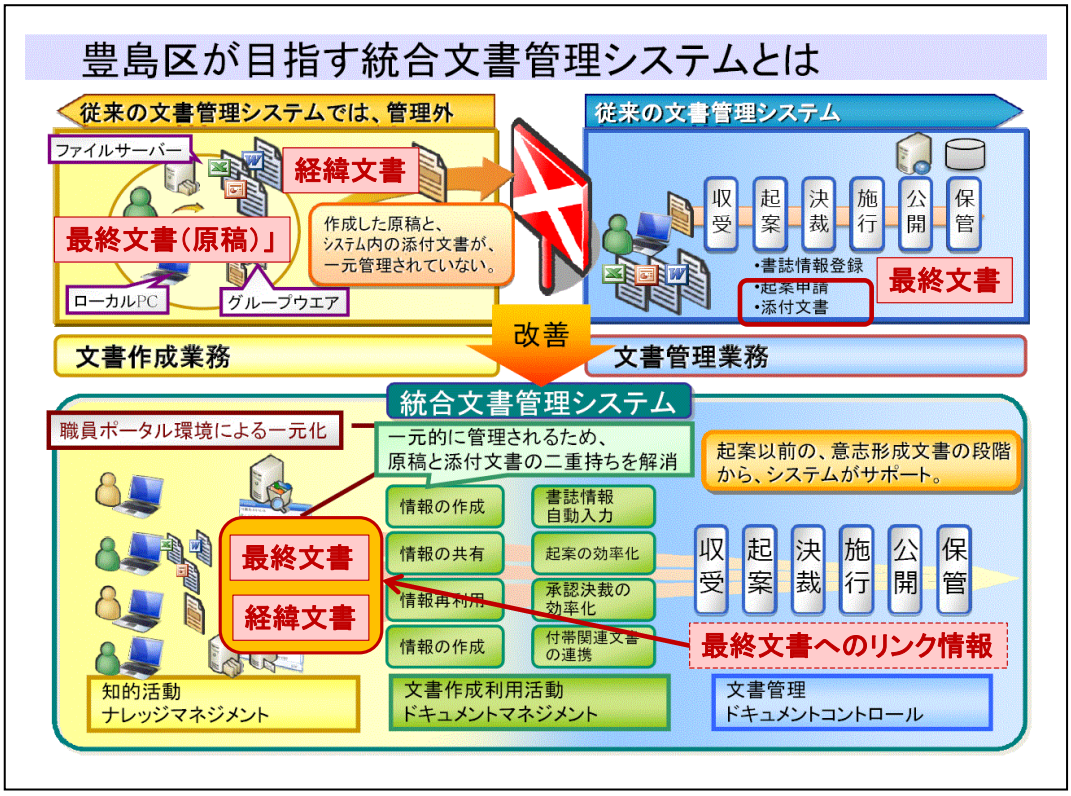


図 1-9　豊島区が目指す統合文書管理システム

平成 23 年 3 月 1 日　ERMC 報告会資料(豊島区役所殿講演)に追記

(目指したシステム)

「起案文書を作成した後、一度パソコンに保存してから文書管理システムに乗せるために別のシステムに入れ直すという従来型の業務を見直し、作成した文書をそのままフローに乗せることで、2 重管理を避ける。」を目標に、統合文書管理システムを構築した。

(ケース管理の視点からの分析)

図 1-9 のように、「統合文書管理システム」導入により、職員ポータルを一元化し、収受案件毎に、共有フォルダを作成、起案前の意思形成文書の「経緯文書」もここに置き、収受から起案、決裁、施行、公開、保管の対象の「最終文書」については、この共有フォルダ内の文書番号をリンクする。これにより、「最終文書」と「経緯文書」を一元的に管理できる仕組みとなった。

すなわち、決裁経緯を知りたければ、収受番号をキーに、収受案件毎の共有フォルダを探し出し、そのフォルダ内の文書を参照することで解決できる。

また、行政文書については、年度毎の参照率が高いので、以前の類似ケースを見つければ、新規の案件の検討や処理の仕方に非常に役立つ。

豊島区役所の事例は、ケース管理の視点から見た日本型記録管理の以下の 3 つの課題を解決していると言える。

①業務遂行に伴い自然と記録が残ることを目指し、業務遂行者が記録する負担を軽減する。
②最終文書・結果だけでなく、それに至った経緯・判断材料も残す。
③記録した文書を組織横断的に活用する。(作成した人以外が、活用しやすい)

第 2 章　ケース指向電子記録管理システムの適用

2.1　ケース指向電子記録管理システムの目的

eRAP は、企業活動における文書管理において、従来型の文書中心の電子記録管理システムに対し、業務を中心とする「ケース指向電子記録管理システム」を提案する。

その目的は、次の 3 点であり、業務遂行中、②、③は業務完了後を対象とするものである。

①業務遂行関係者への進捗状況の公開。(業務遂行の見える化、レスポンシビリティ)

②最終文書・結果に至った説明を利害関係者に行うために、経緯を含めた記録を残すこと。(アカウンタビリティ)

③記録を利用して、次業務の参考にする、業務改善・業務改革や新商品開発などに活かす。(リユーザビリティ、クリエイティビティ、業務改善、業務改革)

これらは、ケースマネジメント説明図 2-1 中で示すと、①は業務遂行、②は監査、③は関係者への開示の部分に関連する。

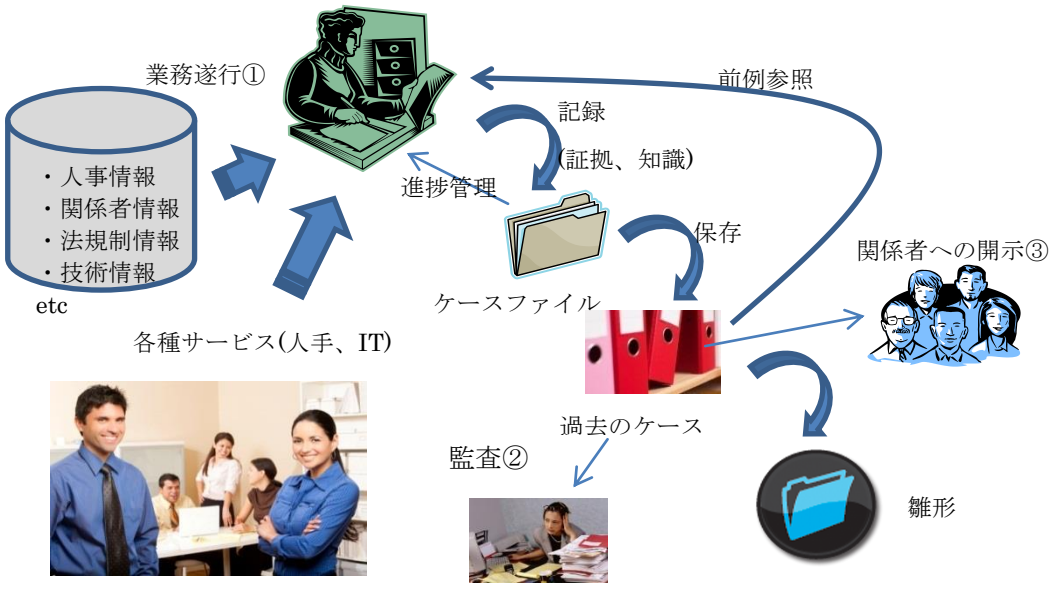


図 2-1　ケース指向電子記録管理システムの目的

このような目的の下、「ケース指向電子記録管理システム」は従来の電子文書管理システムに加えて、次の 2 つの特徴を持つ。

①図 2-2 のように、最終文書だけでなく、そこに至るまでの経緯を含む必要十分な文書を関連付けて、1 つの入れ物(ケース)で管理できる。

②活用のために、ケースや文書に付随するメタデータ(ケースや文書の ID、説明、日時、事象(受理、作成、参照など))を共に管理できる。

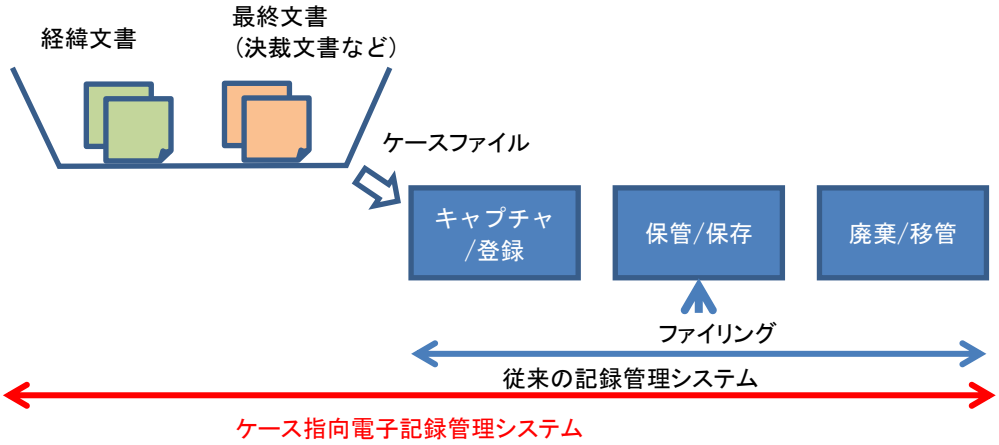


図 2-2　ケース指向電子記録管理システム　モデル

2.2　ケース指向型電子記録管理システム

2010 年から eRAP では、デンマーク政府が導入しているケースマネジメントをはじめとして、韓国、ハンガリ、ドイツ、イギリス、シンガポールなどの電子文書管理システムについて、調査してきた。「ケース指向電子記録管理システム」の実現のため、ケースマネジメントシステムとして完成度の高いデンマークのケースマネジメントシステムを参考にした。しかしながら、デンマークの「ケースマネジメント」のシステムは、高度なインプリメンテーションをしているため、そのままの形では導入に相当の時間を要するとの認識から、国内企業への導入を容易にした「ケース指向電子記録管理システム」を提案する。

2.2.1　ケース指向の特徴

「ケース指向電子記録管理システム」の特徴である「ケース指向」について説明する。

(1) ケースファイルとケース属性

ケースに関する最終結果・文書をケースファイルに格納するものとする。このケースファイルにはケース属性、状態、関係を紐づける。図 2-3 に標準的な例を示す。

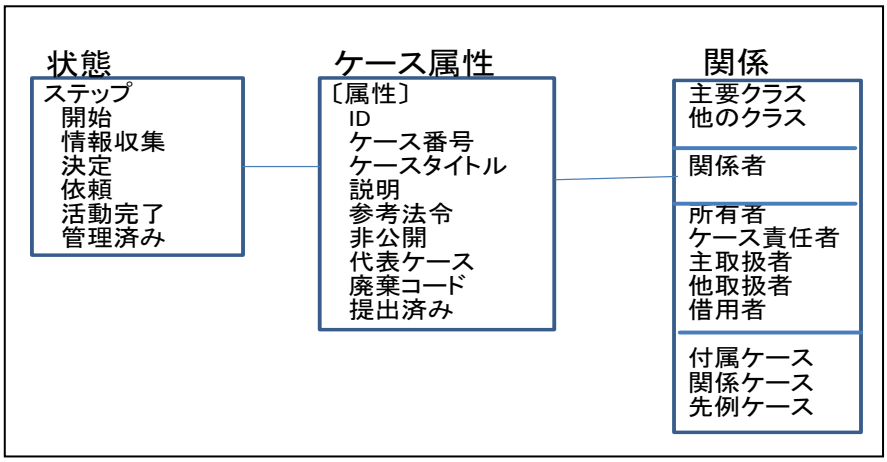


図 2-3　ケースファイルのメタ情報　標準的な例

(2) ケース状態

個々のケースの進捗状態を管理するものであり、ケース管理特有のものである。

ケースの進捗を管理しない場合でも、最低限　開始(Open)、管理済(CLOSE)については、管理する必要がある。デフォルト値は、開始、情報収集、決定、依頼、活動完了、管理済みであるが、進捗状態の記述は用途によって再定義可能である。

(3) ケースの関係性

ケース属性の一部で、複数のケースが同時に処理される場合のケース間の関係性を表現する。

図 2-4 のように、ケース間に親子関係がある場合、子ケースでは、親ケースの子として、「付属ケース」に親ケースの ID を記述する。親ケースは「キーケース」とも呼ばれる。参照するケースについては「関係ケース」に、参照するケース ID を記述する。

BPM (Business Process Management)ソフトにおいては、キーケースを「ケース」、キーケースに付属するケースを「タスクまたはプロセス」と呼ぶことがある。そのような言い換えをすると本ケースモデルは、BPM ソフトの構造と同一であり、その処理記録を残すことにも適していると言える。

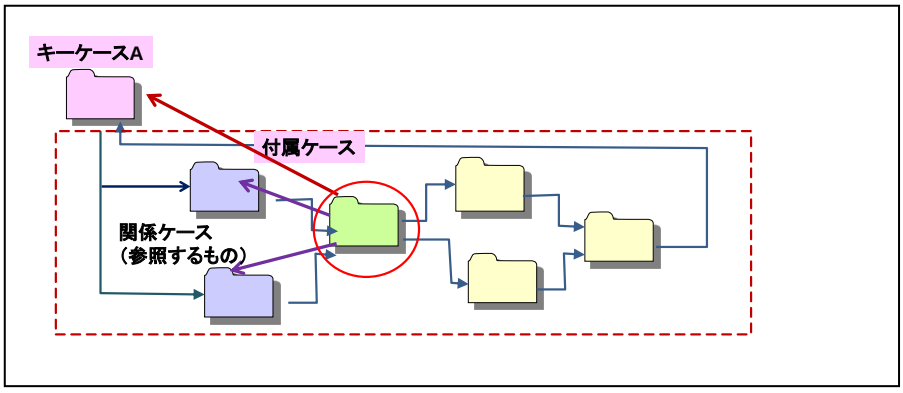


図 2-4　ケースの関係性

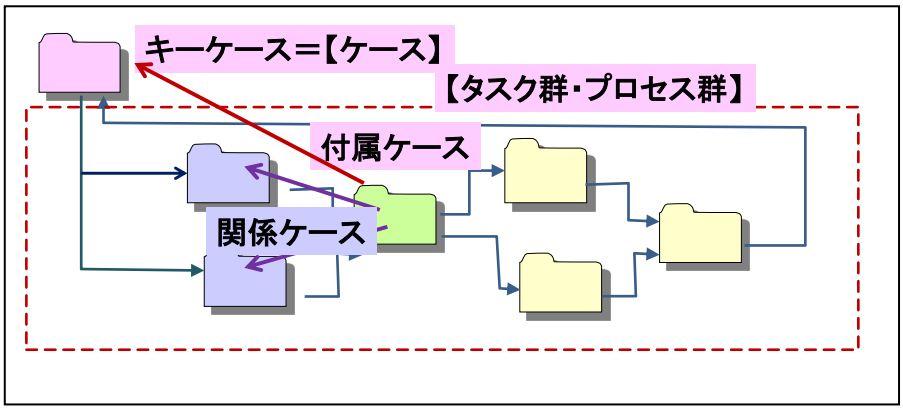


図 2-5　BPM ソフトとケースの関係性

(4) 非定型業務の取扱い例

もともとタスク 1、2、3 を実施予定であったが、予期せず、タスク 2 と 3 の間に新たなタスクが発生した場合、このタスクは非定型業務となる。ブランクタスクをタスク 4 として割り当てる。こうすることで、非定型業務でも記録を確実に残すことができる。

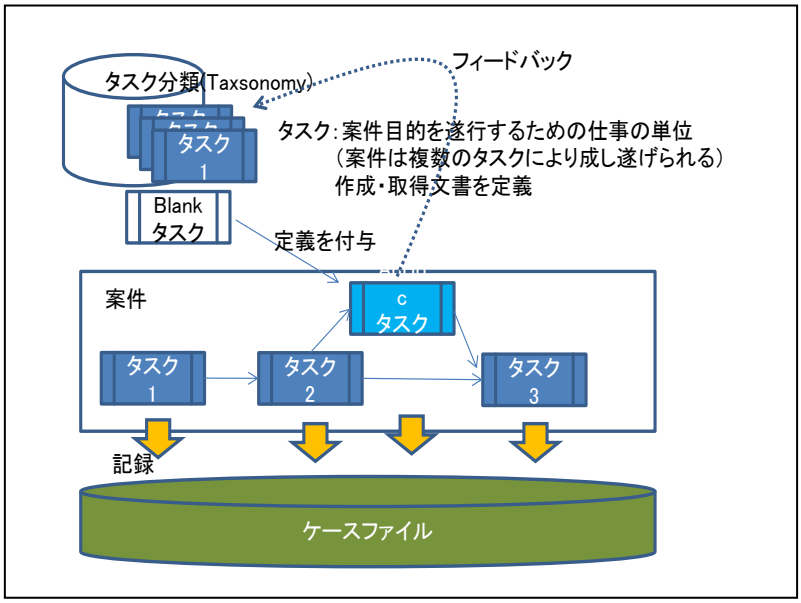


図 2-6　非定型業務の対応例

(5) ケース管理の階層

大きくは次の 3 階層がある。

①「ケースファイルの内部管理」
②「ケースルファイルの管理」
③「ケース実行プロセス管理」(BPM ソフト、ワークフロー、人手)

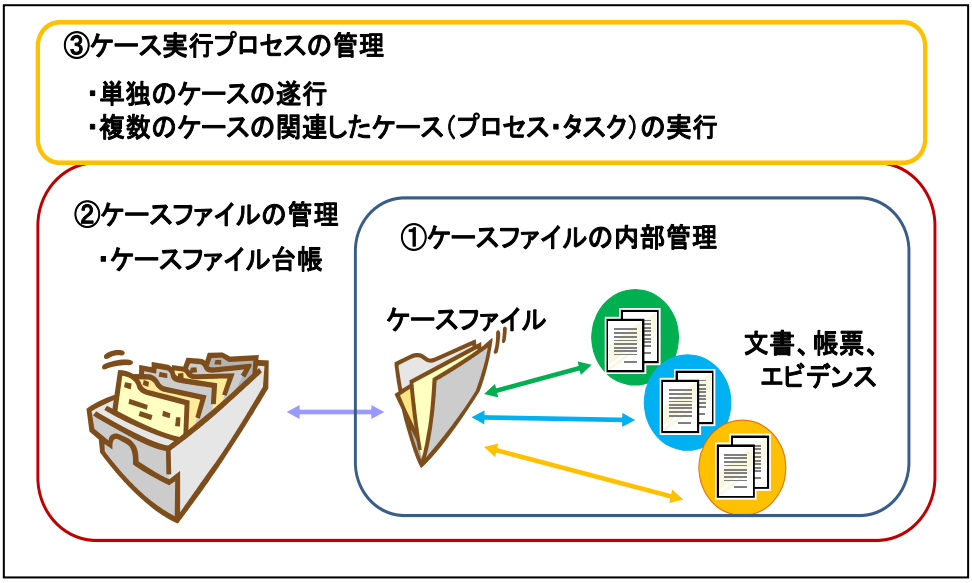


図 2-7　ケース管理の構造

2.2.2　基本アーキテクチャ

eRAP が提案する「ケース指向電子記録管理システム」の基本アーキテクチャを図 2-8 に示す。

・ケースリポジトリ、プロセスコントロール、ユーザインタフェースで構成される。
・ケースリポジトリはケースファイルとドキュメントを合わせた基本部分である「リポジトリコア」とケースファイル群を管理する機能を「マネージャ」、ケースファイルやドキュメントの状態をユーザから見て可視化するため「可視化オプション」と紙・電子ファイルの登録時に属性情報等を付与するための「登録オプション」で構成される。

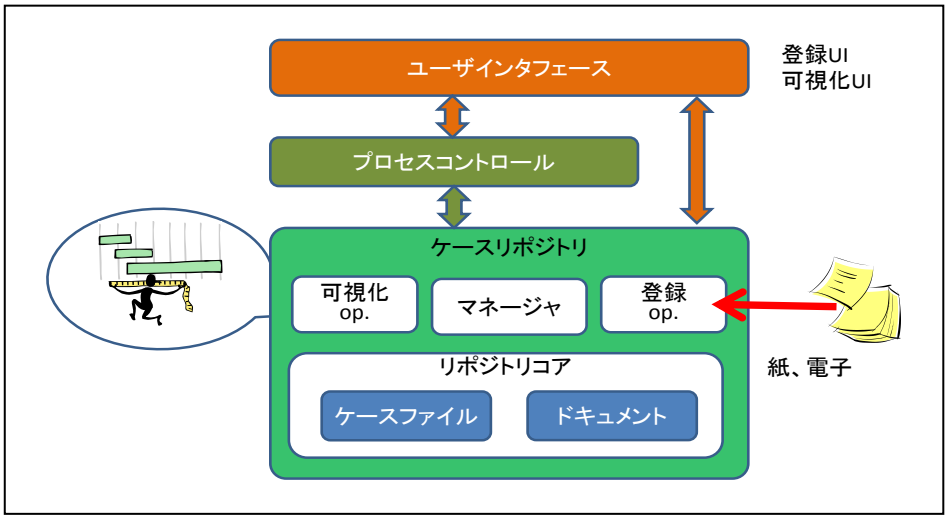


図 2-8　「ケース指向電子記録管理システム」の基本アーキテクチャ

・プロセスコントロールでは、ケース、プロセス・タスクなどの実行を管理する。BPM ソフトやワークフローなど IT で行う場合と人手で回すケースがある。
・ユーザインタフェースは非常に重要で、業務を行っている人が、文書の登録時、属性情報を

付けることを IT で補助する登録ユーザインタフェースや、ケースの実行状況等を見やすくする可視化ユーザインタフェースなどが含まれる。

eRAP が提案する基本アーキテクチャとデンマークのアーキテクチャとの関係を図 2-9 に示す。

- 「ユーザインタフェース」はデンマークの「ダイヤログレイヤ」に相当する。主に登録ユーザインタフェース、可視化ユーザインタフェースを持つ。
- 「プロセスコントロール」はデンマークの「望ましいビジネスサービス」に相当する。プロセスの推進を制御する部分で、人手または IT での処理となる。
- 「マネージャ」はデンマークの「プロセスレイヤ」に相当する。
- 「リポジトリコア」はデンマークの「システムコア」に相当する。
- IT インフラ、人事・組織情報はいずれの場合もアーキテクチャの前提である。

「eRAP が提案する基本アーキテクチャ」は、全てを IT で実現することを要請するのではなく、プロセスコントロール部、マネージャ部を人手で実行することも許す柔軟性の高いものである。

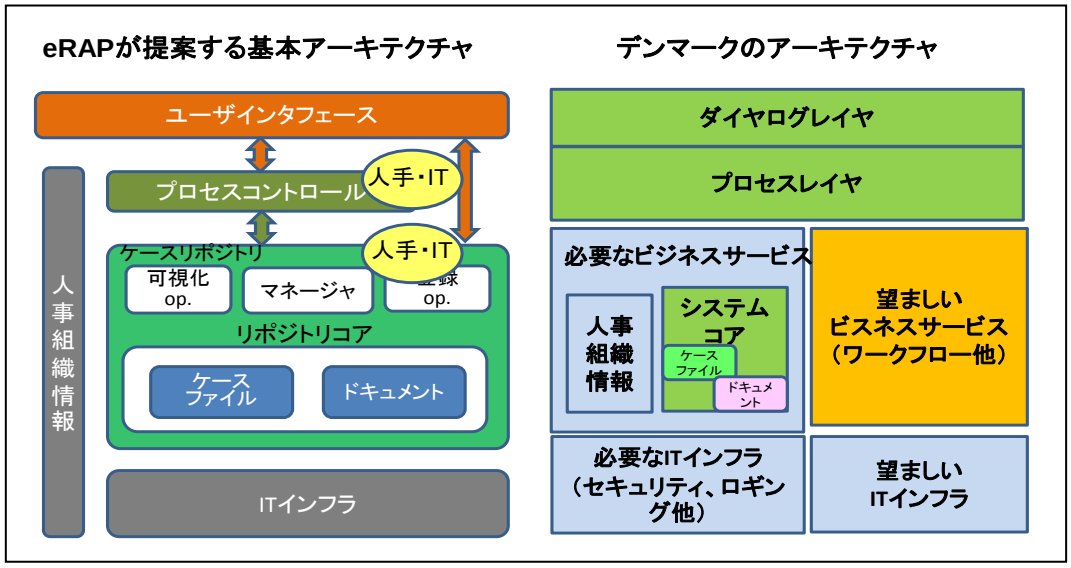


図 2-9　eRAP の提案するアーキテクチャとデンマークのアーキテクチャの関係

2.2.3　サブセット提案

この基本アーキテチャを図 2-10 のようにサブセットに分け、各企業の導入段階に応じて、選択できるようにした。

(1)Basic　レベル

ケース属性、状態管理、ケーステンプレート定義、ケース生成・ケース台帳管理ならびに、紙文書も管理できるドキュメントカード方式も保有する。

このオプションとして、電子ファイル・紙文書の登録をするユーザインタフェース、登録文書やケースの可視化を行うインタフェース、更に、システム間の移管インタフェース、並びにワー

クフロー／BPM との連携を行う。

(2)Advanced　レベル

非定型業務も扱える。このオプションとして、ケースへの記録・参照のログを残すジャーナル機能を持つ。

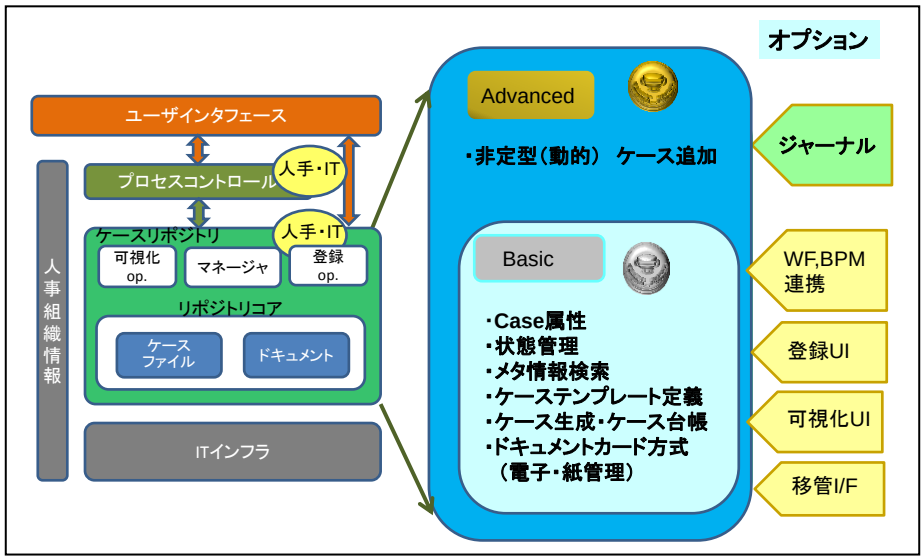


図 2-10　サブセット提案

2.2.4　一般の文書管理システムの利用

ケース管理の導入のハードルを下げるため、ケース管理専用システムではなく、一般の文書管理システムをベースにする場合も検討した。詳細は、eRAP から別途報告する「簡易型ケースフォルダの技術要件」に記載するが、図 2-11 に示すように、フォルダをケースフォルダとして扱い、このフォルダの属性(メタ情報)を管理、検索できるように機能を追加する。

このフォルダ属性に「ケース属性」として、ケース ID、ケースタイトル、「ケース関連」として、業務 ID や付属ケース、関連ケース、「状態」として、ケースオープンやクローズ、その時の時刻などを入れていく。特に、枠で囲んだ項目は重要である。

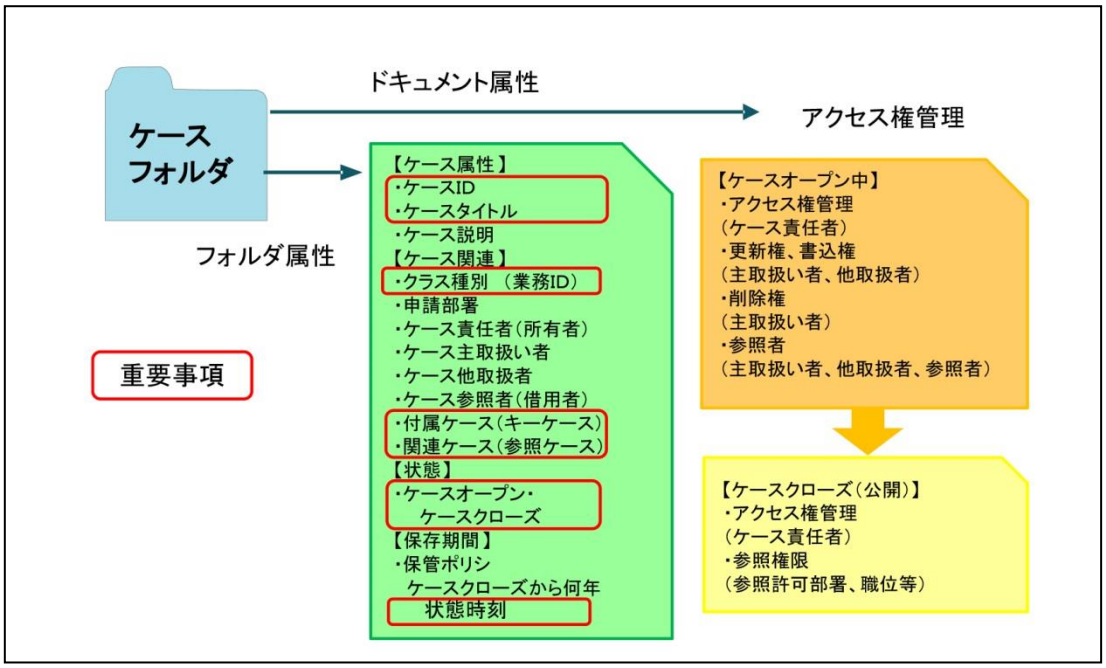


図 2-11　一般の文書管理システムの利用

2.3　ケース指向電子記録管理システムの適用例

2.3.1　Apeos PEMaster

本項では、富士ゼロックス株式会社(以下“富士ゼロックス”とする)のケース指向電子記録管理システムである Apeos PEMaster について報告する。従来の文書管理システムを用いてケース指向の電子記録管理を実現する場合の課題を Apeos PEMaster がどのように解決するかを説明し、具体的な適用事例を紹介する。

(1)従来の文書管理システムを用いる場合の課題

一般的な申請業務に関わる文書をケース指向で管理する場合を考える。

業務を遂行した結果や経緯を表す文書をケース指向で管理するために、ケース単位でフォルダ階層を作成する。必要な文書をフォルダ階層の正しい位置に登録するのは作業者の責任となる。文書の登録状況は、個々のフォルダを開いて確認する。どのケースでどの文書が必要なのかは、作業者が業務ルールを把握した上で判断する。

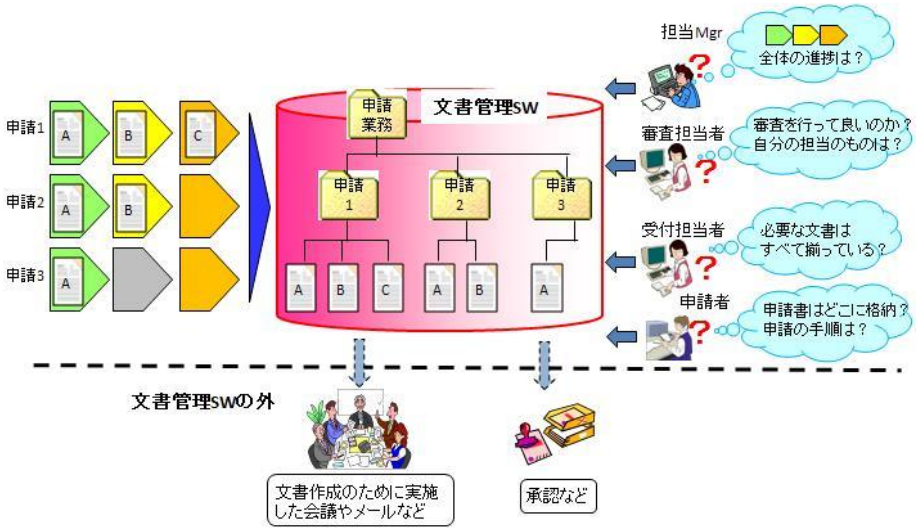


図 2-12　従来の文書管理システムでケース管理を実現した場合

この場合、以下のような課題が挙げられる。

- 業務の状況を把握することが難しい。
  - 文書の登録状況を確認するためには、個々のフォルダを開く必要がある。
  - 複数のケースの状況を一度に参照できないので、業務全体の進捗状況が分からない。
- 正しく運用することが難しい。
  - 申請を行う際にどのような文書を用意するべきか、個々の申請者が業務ルールを正しく理解していなければならない。
  - 文書を登録する際は、管理上必要なメタ情報を正しく付与して、正しい位置に登録しなければならない。
- 文書以外の情報を管理するのが難しい。
  - 文書だけでなく、業務遂行の経緯(関与者間のやりとりや、正しい承認手続きを踏んだ記録など)もケースに関連付けて管理したい。

(2) Apeos PEMaster を用いる場合

富士ゼロックスの Apeos PEMaster は、文書管理システムである Evidence Manager と、業務を支援する Workflow・Collabo Space・Evidence Tracker などのアプリケーション群で構成される。

Evidence Manager は、大量のコンテンツをメタ情報と合わせて保管することができる。

Workflow は、文書を扱う定型的な手続きの遂行を支援する。文書をしかるべき手順で承認して登録する場合などに利用できる。

Collabo Space は、複数の関与者が互いにやり取りしながら進めていく非定型な作業の遂行を支援する。個々の作業毎に Web 上のコミュニケーション場を作成して複数の関与者を割り当てることができる。コミュニケーション場では関与者間のコミュニケーションが簡単な操作で行え、関連文書を共有することができる。コミュニケーションや文書の変遷が記録されるので、コミュニケーション場を参照することで過去の経緯を把握することができる。

Evidence Tracker は、業務プロセスの構造とさまざまな関連情報を結びつけて管理し、個々のケースの状況がひと目でわかるように可視化する。

これらのコンポーネントを組み合わせて、ケース指向電子記録管理システムを実現する。

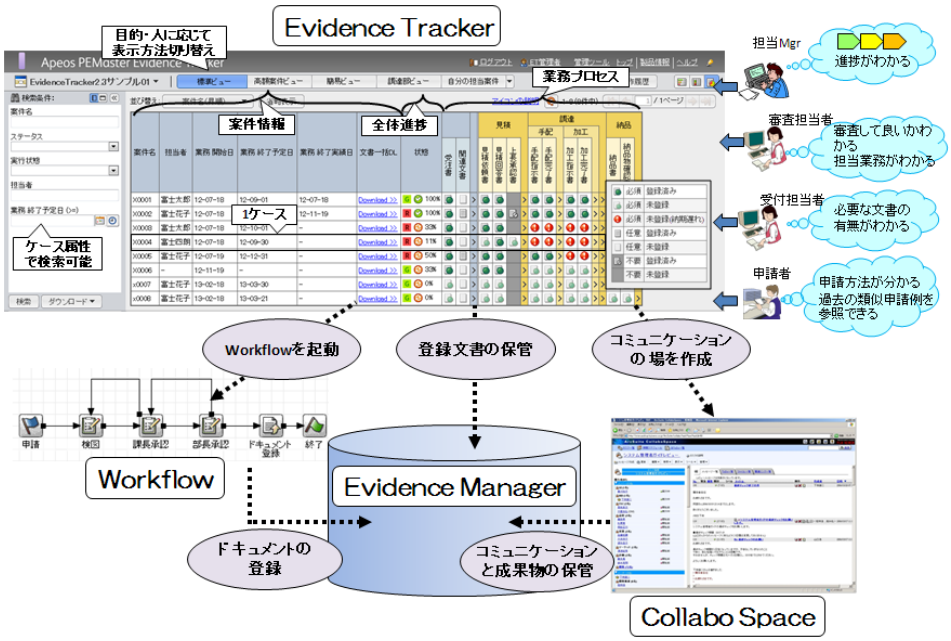


図 2-13　Apeos PEMaster でケース管理を実現した場合

図 2-13 は Apeos PEMaster を用いて構築したケース指向電子記録管理システムの例である。

作業者や業務管理者は、Evidence Tracker の画面を起点として個々の作業を遂行する。

業務の状況を確認したい場合は Evidence Tracker の画面を参照すれば良い。1 行が 1 ケースに対応しており、必要な文書がアイコンで表示される。それぞれの文書の状況(登録済、未登録、納期遅れ)や必要度(必須、任意、不要)がアイコンの色や形状で表現されるので、ひと目でケースの状況を把握できる。参照したいケースの条件を指定して検索できるので、自分が担当する複数のケース全体の状況を俯瞰できる。また、検索条件や表示形式の設定を予め複数用意しておけるので、利用目的に適した画面を簡単に参照できる。

Evidence Tracker には、業務ルールを予め定義してあるので、ケースの条件に応じて進捗状況や必要となる文書が自動的に判定される。文書を登録する際は、ドラッグアンドドロップ操作を利用できる。デスクトップ上の文書アイコンをドラッグし、Evidence Tracker 画面上の文書アイコン上にドロップすることで、管理に必要なメタ情報が自動的に付与され、Evidence Manager の正しい位置に登録される。

業務で利用するワークフローやコミュニケーション場をケースに関連付けて管理することもできる。ケースに設定されているリンクから、ワークフローを起動して承認手続きを遂行したり、ワークフローの実行結果や経路を参照したりできる。同様に、ケースに設定されているリンクから作業場にアクセスし、他の関与者とコミュニケーションを行ったり、過去の経緯を参照したりできる。

このように、Apeos PEMaster を利用すれば、文書だけでなく業務遂行の経緯もケースに関係

付けて管理できる。そして、個々のケースや業務全体の状況がひと目で把握できるようになる。

(3) 住宅設備機器施工業務における適用事例

ケース指向電子記録管理システムを適用した事例として、ある住宅設備機器会社(以下“A 社”とする)の施工業務に Apeos PEMaster を適用した事例を紹介する。

①住宅設備機器施工業務の現状

住宅設備機器施工業務とは、建物や住宅に設備機器を設置する業務である。カスタマーセンタは、代理店営業を通して代理店(ハウスメーカなど)から設備機器設置の依頼を受け、一連の作業の手配やスケジュールの調整を行う。施工現場における現地調査や施工作業は施工店(施工契約を結んでいる工務店など)に依頼する。

図 2-14 にあるように、カスタマーセンタと代理店営業や施工店との間では契約書、作業指示書、調査結果報告書、図面などさまざまな文書のやり取りを主に FAX で行っている。FAX で送付された文書は、カスタマーセンタの担当者が紙文書のまま保管していた。

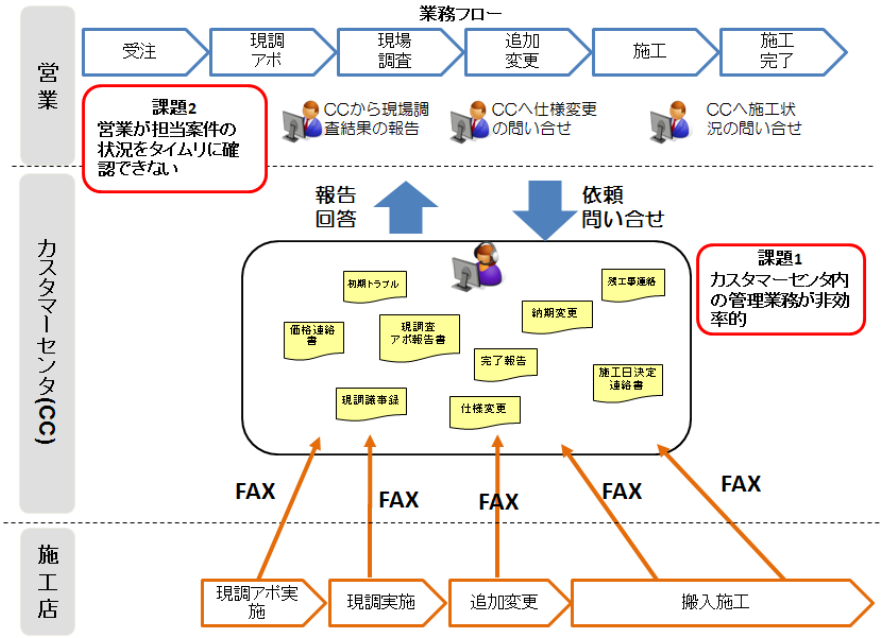


図 2-14　住宅設備機器施工業務の現状

②住宅設備機器施工業務の課題

このような現状に対して以下のような課題があった。

1：カスタマーセンタ内の管理業務が非効率的

- 案件の状況を確認するためには、紙文書の山から対象案件に関連する文書を探し出して内容を確認しなければならず、毎回余計な作業を強いられていた。
- FAX で入力された文書が埋もれてしまったり、納期を過ぎても完了していない作業を見過ごしてしまったりといった作業漏れが発生しがちであった。

- 案件によって、扱う設備機器(トイレや風呂など)や現場の状況(マンションや 1 戸建など)はさまざまであるが、作業内容の判断はカスタマーセンタの担当者が個々に行っており、作業ミスが発生しがちであった。

2：代理店営業が担当案件の状況をタイムリに確認できない

- 代理店営業が案件の進捗状況を確認するためには、都度カスタマーセンタに問い合わせが必要であったが、カスタマーセンタからのレスポンスが悪く、お客様への対応がスムーズに行かなかった。

③対策と効果

上記課題 1、2 に対して以下の対策を実施した。

課題 1 への対策

- FAX 入力された文書を電子文書として Evidence Manager に登録するようにした。また、業務と文書の関係を Evidence Tracker に定義し、文書の登録状況が Evidence Tracker の画面で確認できるようにした。
- 業務の手順や進捗状況の判定ルールを Evidence Tracker に定義し、次の作業や進捗状況が自動的に判断されるようにした。また、納期が近づいても完了していない作業がある場合は、自動的に担当者や管理者へ通知されるようにした。
- ケースの状況によってどのような作業や文書が必要になるのかを Evidence Tracker に定義し、自動的に判断されるようにした。

課題 2 への対策

- 代理店営業が参照するのに適した画面を作成し、代理店営業がいつでもアクセスできるようにした。

対策を実施後の全体概要を図 2-15 に示す。

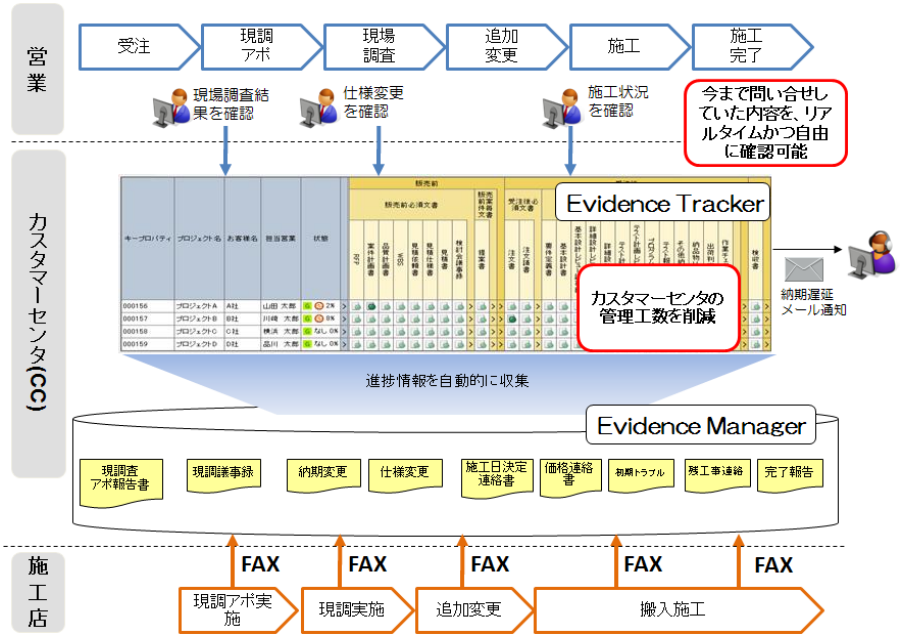


図 2-15　Apeos PEMaster を適用した全体概要

上記の対策を実施した結果、以下の効果が得られた。

カスタマーセンタ

- 作業工数の削減、リードタイムの短縮

  目的の文書を探す無駄な作業が不要となり、代理店営業からの問い合わせに対応する必要もなくなった。また、自分が担当している複数の案件の状況を常時把握できるようになり、効率的なスケジュールを立てられるようになった。

  結果として担当者の工数を大幅に削減でき、個々の案件のリードタイムも短縮できた。

- 作業漏れの低減、作業ミスの低減

  FAX 入力された文書が紛失することがなくなった。自動通知機能によりうっかり納期漏れを見過ごすこともなくなった。

  必要な文書の登録状況を簡単に確認できるようになった。また、個々の作業の内容や作成する文書の内容を判断する場合、同様の条件の事例を簡単に参照できるようになった。

  更に、管理者が全案件の状況を常時把握できるようになったため、問題が発生している可能性のある案件を速やかに発見し、適切な対処を行えるようになった。

  これらにより、作業漏れや作業ミスの発生を大幅に低減することができた。

代理店営業

- お客様対応の品質向上

  担当案件の進捗状況をいつでも簡単に確認できるようになった。このため、お客様からの問い合わせに対して、速やかに適切な対応をとれるようになった。

この事例の主たる目的は、大量の紙文書を扱っていることで発生している無駄な工数の削減で

あった。しかし、結果としてノウハウの共有や効率的な作業計画が可能になるなどの効果も得ることができた。この点で、ケース指向電子記録管理システムが業務品質の向上に有効であることを示唆する好適な例であるといえる。

2.3.2 プロジェクト管理

本項では、ケース指向電子記録管理をプロジェクト管理へ適用する事例として、システム(ソフトウェア)の請負製作プロジェクトを題材に検討した結果を報告する。なお、ここでの報告はプロジェクト管理に適用した場合、どのようなメリットや課題があるかについて考察したものであり実際の適用事例ではない。

本項前半(1)～(3)ではプロジェクト管理における一般的な考察を行い、後半(4)以降ではプロジェクト管理ソフトウェアを活用したケース指向電子記録管理の実現について考察を行う。

(1) プロジェクト管理における文書管理の現状

人、物、金と時間を管理するプロジェクト管理においてドキュメント管理は重要である。

システム(ソフトウェア)請負製作プロジェクトでは、商談開始から契約、仕様策定、実装と試験、稼動、保守といった局面毎に管理すべきドキュメント、エビデンスがある。これらのドキュメントは品質保証や、顧客への説明責任を果たす情報として大切である。

またプロジェクトに投入したコストやリソース､発生した問題点とその対応を記録することは、次の同等のプロジェクト実施にむけての大切なナレッジベースとなる。

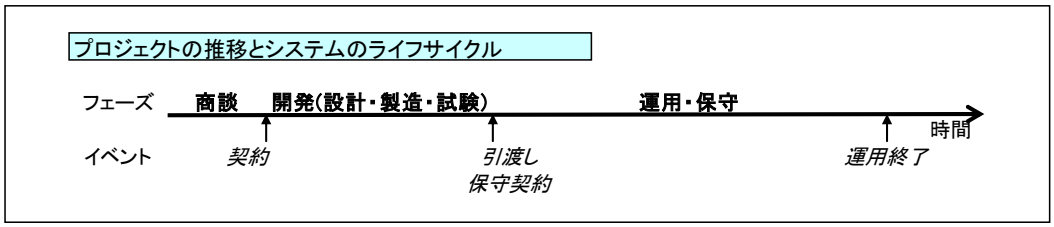


図 2-16　プロジェクトの推移とシステムのライフサイクル

では実際のプロジェクトではどのように文書管理がなされているだろうか？

現在、多くの企業では社内で複数のシステムが稼動し、商談や契約の管理、プロジェクト実行時のプロジェクト情報の管理、文書の保存などがなされている。企業により文書の名称や、稼動しているシステムは様々だが、概ね以下のようになると考えられる。

表 2-1　プロジェクトのフェーズと主なドキュメント、情報

フェーズ	扱う文書、情報	所管部門	備考
商談	商談情報 (営業報告、公募案内など)	営業	
	要求仕様書	顧客	
	社内見積り資料	営業	見積り情報は開発部門からも提示される 最終見積りに至る検討が行われる
	社内審査記録	営業	法務や輸出管理、品質管理が関わることもある

フェーズ	扱う文書、情報	所管部門	備考
	顧客提示見積書、提案書	営業	
	契約書	営業	最終的な契約条件に至る経緯は契約書には含まれない
	メール		システムとしては情報システム部門で管理
開発	設計書	開発、品証	システム要件定義、方式設計、ソフトウェア要件定義、ソフトウェア方式設計、ソフトウェア詳細設計書
	実装コード	開発、品証	
	試験	開発、品証	ソフトウェア結合試験、ソフトウェア適格性確認テスト、システム結合試験、システム適格性確認テスト
	取扱説明書	開発、品証	
	協力会社への発注仕様	開発、調達	協力会社を使う場合の調達関連情報
	協力会社への契約内容	調達	オフショアなら輸出管理が関わる
	協力会社からの納入物件	開発、調達	
	知財調査	開発、知財	
	進捗記録	開発、取引先	
	議事録	多岐	
	メンバの勤怠記録	開発、人事	プロジェクト情報であり、人事(給与)情報である
	旅費、経費等	開発、経理	プロジェクト情報であり、経理情報である
	メール	多岐	仕様検討、進捗報告、意見交換など多岐 システムとしては情報システム部門で管理
引渡し	検収資料	営業、顧客	
保守	保守契約	営業、顧客	保守サービス会社に外注の可能性や他社が請負う可能性もある
	保守状況報告	保守	
	障害管理	保守、開発	
運用終了		顧客	

※補足事項

「開発部門」は企業によっては「技術部門」、「製造部門」などと称される

「調達部門」は企業によっては「資材部門」」などと称される

「品証部門」は品質保証部門を指す

「保守」部門は他の会社である可能性もある

これらの部門は企業規模によって独立部門であったりそうでない場合もある

用語は IPA の「エンタープライズ系プロジェクト」[1]を参考にした

このように、ひとつのプロジェクトでも作成する文書や発生する情報の所管部門が異なる。そして、それぞれの所管部門で管理しやすいように、それぞれのシステムが稼動していることが多いのではないだろうか。

(2) プロジェクト管理における文書管理の問題

プロジェクトでは「プロジェクトを実行している時」に多くの文書が生成され、情報が発生する。その後、「プロジェクトが終了した後」に、プロジェクト実行中に発生した文書を利活用する

[1] http://sec.ipa.go.jp/std/ent.html

可能性が高い。

システム(ソフトウェア)の請負製作を考えた場合、一般にプロジェクト管理というと、「図 2-17 プロジェクトの定義」で示す開発フェーズにプロジェクト管理システムを導入し、プロジェクト実行を通じて発生する文書や情報を管理することが想定される。

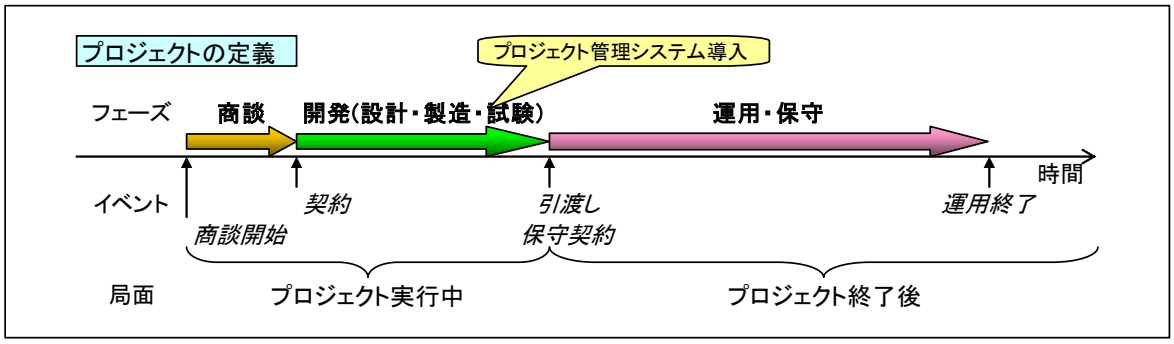


図 2-17　プロジェクトの定義

一方、本報告書で提唱しているケース指向電子記録管理はその目的を「2.1　ケース指向電子記録管理システムの目的」でプロジェクト実施中のレスポンシビリティ、終了後のアカウンタビリティ、リユーザビリティ、クリエイティビティを確保することであると示している。

すなわちプロジェクトを案件全体ととらえ、商談開始から運用終了まで案件を通じて発生する文書や情報を管理することを目指している。

それを踏まえシステム(ソフトウェア)の請負製作案件の「プロジェクト実行中」の範囲を商談開始から引渡し[2]まで、それ以降を「プロジェクト終了後」としケース指向電子記録管理を推進するにあたりプロジェクトの状態にどのような問題があるかを次表に整理する。

表 2-2　プロジェクトのフェーズと文書管理の問題

項番	プロジェクト局面	問題	分類	なぜ？	関係する情報
1	全体	必要な情報を集めるために複数システムから情報を取らないといけない	レスポンシビリティ リユーザビリティ	所管部門毎に最適化されたシステムが運用されているため またそれらのシステムで連携はあまり考慮されていないため	システム間の連携
2	全体	複数プロジェクトを横串にして類似情報を検索ができない	レスポンシビリティ リユーザビリティ	利活用を意識して「何を情報として抽出しておくか」が明確でない	利活用を意識した仕掛け
				プロジェクト管理ソフトの検索機能がそのような使い方を想定していない	プロジェクト管理システムの機能
3	実行中	プロジェクトの開始から終了まで、一貫して追いかけられない	アカウンタビリティ トレーサビリティ	所管部門毎に最適化されたシステムが運用されているため(例えば商談(営業主体)と、開発(開発部門)で一貫した情報管理が行えない)	システム間の連携

[2] 引渡し後の保守は別途保守契約となることが多いのでここでは同一案件の別プロジェクトと考える

項番	プロジェクト局面	問題	分類	なぜ？	関係する情報
4	実行中 終了後	結果はわかる。しかしなぜそうなったのか後からわからない	リユーザビリティ トレーサビリティ アカウンタビリティ	議事録など、結果を示すドキュメントはある。 しかしなぜそうなったかの経緯は口頭での会話やメール授受によって行われシステム内に残りにくい。	経緯情報
5	実行中 終了後	監査がある。必要な文書を探したいが探しにくい	リユーザビリティ アカウンタビリティ	どこかにあるのだが、どこにあるかわからない	管理手順、ルール 管理システム
				見つけたが、それが最新かわからない	
6	実行中 終了後	認証維持のため、エビデンスを提示しなければならないがドキュメントが探しにくい	リユーザビリティ アカウンタビリティ	どこかにあるのだが、どこにあるかわからない	管理手順、ルール 管理システム
				見つけたが、それが最新かわからない	
7	実施中 終了後	知財係争になりそう。証拠として提出できる情報はどれで、どこにあるのかわからない	リユーザビリティ アカウンタビリティ	どこかにあるのだが、どこにあるかわからない	管理手順、ルール 管理システム
				見つけたが、それが最新(最古)かわからない	
				資料の時刻を証明できない	タイムスタンプ
8	実施中 終了後	ファイルサーバに残るたくさんのファイル。どこに管理されているのか、何が最新で、どれが履歴？	リユーザビリティ	プロジェクトの山場を過ぎるとメンバのメンテナンス意欲が下がる	管理手順、ルール 管理システム
				管理ルールが決まっていないか徹底されていない	文書管理システム プロジェクト管理システム
9	実施中 終了後	プロジェクト管理ソフト、実行中は良いが終了後メンテナンスされない	リユーザビリティ	必要なくなるので放置される	管理手順、ルール 管理システム
				管理ソフトも含めたライフサイクル管理がされていない	
10	終了後	担当者が異動または退職した。プロジェクトドキュメントがどのように管理されていたかわからない	リユーザビリティ (アーカイブ)	プロジェクト間での管理方法が統一されていない	管理手順、ルール
11	終了後	部門が統廃合された。このプロジェクトの情報を新しい所管部門に移したいがどのように管理しているかよくわからない	リユーザビリティ (アーカイブ)	部門間での管理方法が統一されていない	管理手順、ルール
12	終了後	製品が市場でトラブルを起こしている。保守情報はどこに？	リユーザビリティ アカウンタビリティ	どこかにあるのだが、どこにあるかわからない	管理手順、ルール 管理システム
				見つけたが、それが最新かわからない	
				なぜ、そのような作りになっているのかよくわからない	経緯情報

項番	プロジェクト局面	問題	分類	なぜ？	関係する情報
13	終了後	同様のプロジェクトを実施することになった。過去の文書を活用して効率化したいがうまく探すことができない	リユーザビリティ アカウンタビリティ クリエイティビティ	過去情報を探すための情報がない(関係者に記憶に頼ることが多い～記憶に残っていなければ死蔵される)	管理手順、ルール 管理システム 利活用の仕掛け 認証
				横串で検索できない	
				検索のためどんな情報を切り出しておくべきかわからない(プロジェクト実施時にやるべきこと)	
				顧客情報等、案件毎の守秘義務情報等と、ナレッジ共有の境が不明確	
14	終了後	プロジェクト終了後、アクセス権を持つメンバが四散(属人的管理で、「プロジェクトの情報」として管理されていない)	リユーザビリティ アカウンタビリティ	プロジェクト情報の所有者が誰か定義されていない	管理手順、ルール 認証
15	終了後	プロジェクト管理ソフトを使っていたが古い時代の情報が読めなくなる危険性がある	リユーザビリティ アカウンタビリティ	プロジェクト管理ソフトに依存してしまう危険性	可読性の問題 文書管理情報の可搬性
				将来の管理、利活用まで考えていない	
16	終了後	プロジェクトの文書は何時まで管理すればよい？(経理情報は？製作物の情報は？法の縛り、製品のライフサイクル)	リユーザビリティ アカウンタビリティ	保存ルールが決まっていない	管理手順、ルール 管理システム
				1 つの案件の中で発生する情報であっても適用される法律や所管部門のルールによって保持期限が違う可能性がある	

このように、プロジェクト実行を通じて発生する文書や情報は何らかのシステムによって記録されているが、システム毎に管理目的や運用組織に応じて最適化されている。

そのためプロジェクトの開始から終了､保守･利活用まで含めた大きな案件と捉えたときには、個々のシステム間の連携の不十分さや、組織としてのルールが確立できていないため、利活用がしにくい状況にあると言える。

以下にプロジェクト実行に関連する様々なシステムの例を示す。

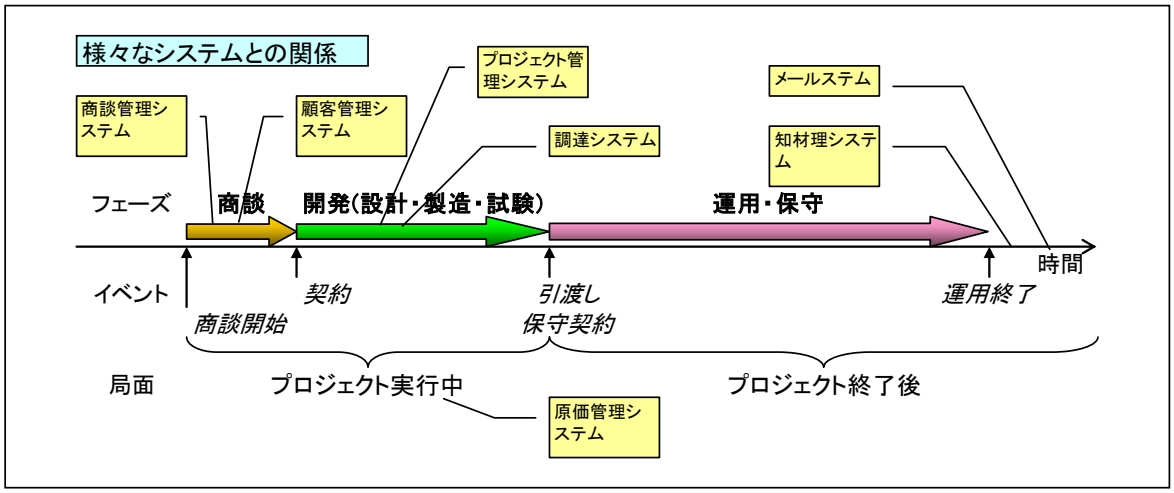


図 2-18　プロジェクトと様々なシステムとの関係

また、文書や情報の利活用を考えた場合、プロジェクト終了後に利活用しやすいような情報をプロジェクト実行中に付加しておく必要がある。例えば、仕様書に記載する実現方式は利活用を考えた場合、なぜその実現方式が選択されたのか、その方式を選んだことによる実際のメリット、デメリットなどが必要になる。しかし、現状は検討結果としてプロジェクト実行に必要な情報だけが記載されているため利活用時に必要な情報が見つけられないという問題につながっていると考えられる。

更に、プロジェクト終了後のプロジェクトの管理担当者変更や、情報を他部門へ移管する可能性がある。その場合のユーザ管理ルールの整備、ユーザ認証をどのように行うのか、プロジェクトに固有の秘密情報をどのように扱うのかという問題が生じてくる。社内規則や部門規則で開発標準が定められプロジェクト実行中の管理方法が決められていても、プロジェクト終了後の情報をどのように管理するかルールが整備され徹底されているかは疑問が残る。

(3)最初のまとめ　～　ケース指向電子記録管理導入で期待される効果と課題

ここでプロジェクト管理にケース指向電子記録管理を導入することで期待できる効果と課題について一旦まとめる。

ケース指向電子記録管理の考え方を導入すると、案件単位に情報を管理でき情報の利活用が進めやすくなることが期待できる。

過去の案件での知識(コスト、技術的対策、発生し得る問題とその解決策など)を活用できるようになることが効率化につながり、対外的な説明責任を果たすための監査や認証での証跡集め、保守時の情報収集が実施しやすくなると予想される。

しかし、現在の企業内の状況を考えるとケース指向電子記録管理導入のためにシステム、運用・管理で解決しなければならないいくつかの課題がある。「2.3.2 (2)プロジェクト管理における文書管理の問題」に示したプロジェクト管理上の問題の原因を分類し、どこに対策を打つべきかをまとめた。

表 2-3　プロジェクト管理におけるケース指向電子記録管理導入のための課題

項番	課題	対策を打つべきところ	表 2-2　プロジェクトのフェーズと文書管理の問題
1	情報利活用のためのシステム間の連携がしにくい	システム	1,2,3,13
2	部門をまたがり一括で案件を管理するシステムが無い	システム	1,2,3,5,6,7,13
3	利活用を前提に文書管理をしていない	システム 管理運用ルール	2,4,5,6,7,12,13,15
4	プロジェクト局面毎のユーザ認証が不十分	システム 管理運用ルール	10,13,14
5	プロジェクト管理システムの機能不足(特に検索機能[3])	システム	2,5,6,7,12,15
6	記録管理ライフサイクルを考慮したシステムの使い勝手がよくない	システム	2,5,6,7,9,12,15
7	現場に負担がかかると文書管理をしにくい	システム 管理運用ルール	4,8,9
8	文書管理ルール、手順が不明確	管理運用ルール	5,6,7,8,9,10,11,14,16
9	文書管理ルールの組織的な適用が不十分	管理運用ルール	5,6,7,8,9,10,11,14,16

このうち、「対策を打つべきところ」で「システム」としている部分はケース指向電子記録管理に対応するためにシステムで問題解決のための改修または新規実装によって解決していく部分と考えられる。

一方、「管理運用ルール」としている部分は組織としてどのように文書管理を行っていくかの管理ルール、運用ルールの部分であり、ここにケース指向電子記録管理の考え方を導入することで利活用の推進を図れると考えられる。

これらについて以降で考察を行う。

(4) ケース指向電子記録管理のシステム化実現への提案

プロジェクト管理にケース指向電子記録管理が必要、あるいは有用であってもシステム化導入には費用の問題がある。また実現できても利用者に使いにくい仕組みでは情報を有効に収集、保存することができない。

eRAP で調査した豊島区のように文書管理システムの背後にある種々のシステムを利用者に意識させない GUI を持ち[4]、管理者による適切な管理が実現できれば利用者の負担なくケース指向電子記録管理を推進できると考えられる。その際、最新の IT 技術を用いクラウド上にケース指向電子記録管理システムを構築し、更に過去からの大量のプロジェクトデータも扱えるようにすることができれば企業内の複数部門をまたがるプロジェクトを管理できる仕組みが構築可能であり、企業内での電子文書の利活用は飛躍的に推進されるであろう。

しかし、昨今の IT システムへの積極投資がしにくい経済環境下では新規にシステムを構築することは難しい。また企業内のインフラとして既に複数のシステムが整備されていることが多く、それらを改修するのにもコストがかかる。

それらを踏まえ、既存システムへの影響を最小限にとどめ低コストでケース指向電子記録管理システムを実現する方法としてプロジェクト管理ソフトウェアを活用するアプローチを検討した。

[3] もともと文書管理やケース指向電子記録管理を想定していないのでやむを得ない

[4] 豊島区の場合はファイルシステムだが、ここでいうシステムはケース指向電子記録管理システムを指す

①プロジェクト管理ソフトウェアを選ぶ理由

システム(ソフトウェア)請負開発プロジェクトは、一般にシステム(ソフトウェア)の開発期間がプロジェクトとして一番多くの人員と費用が投入され、一番多くの情報が発生し、様々な判断が行われるフェーズである。

そのフェーズをターゲットにプロジェクト管理ソフトウェアは有償、無償問わず多数の製品が提供されている。それらはプロジェクト管理を効率化するための工夫が凝らされ、拡張性に富むものも少なくない。ある程度の期間、規模のプロジェクトではプロジェクトを推進するにあたり、作業項目の管理、進捗管理、リソースの管理、関連するドキュメントやソフトウェアのソース管理などを効率よく行うためにプロジェクト管理ソフトウェアや構成管理ツールなどのグループウェアを導入することが多いのではないだろうか？

そこでプロジェクト管理ソフトウェアの使い方の工夫やカスタマイズによりケース指向電子記録管理の考え方をプロジェクト管理の現場に導入できるのではないかと考えた。

本報告ではオープンソースで Web ベースのプロジェクト管理ソフトウェアである Redmine[5]を参考にプロジェクト管理ソフトウェアでケース指向電子記録管理システムを構築することを検討する。

②ケースの捉えかた

ひとつの案件は複数関係部門をまたがり実行される。プロジェクト管理ソフトウェアを用い、1 つの案件を大きなプロジェクトと捉えて管理する。

例として「○○社向け××システム開発」案件を取り上げる。まず案件そのものをひとつの大きなケース(キーケース)と捉える。その中に、商談、開発、保守・運用の 3 つサブケースを想定する。開発ケースの中で、更に開発フェーズに応じたサブケース管理を行う。その様子を「図 2-19　案件におけるケースの定義」に示す。

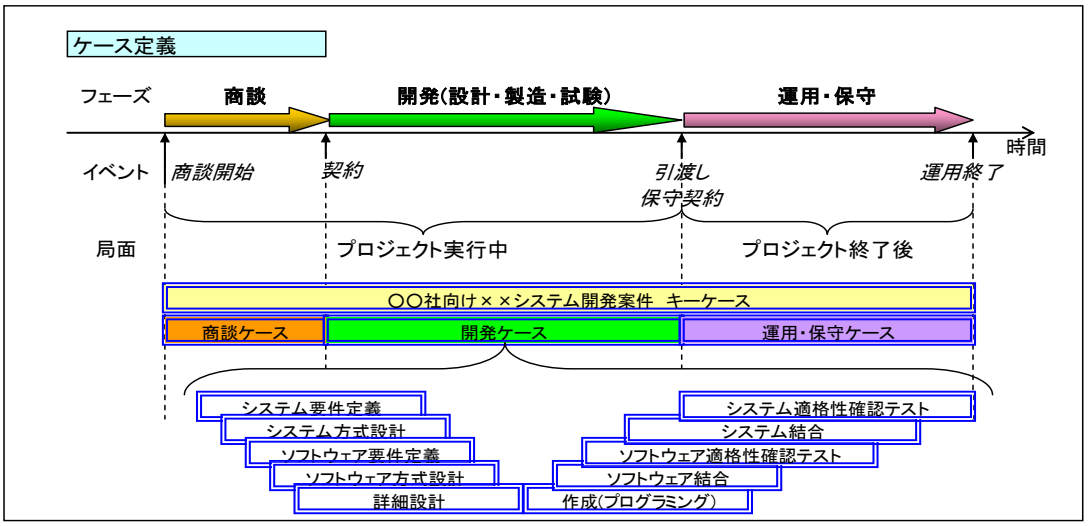


図 2-19　案件におけるケースの定義

[5] http://www.redmine.org/

③プロジェクト管理システムのケース指向電子記録管理システムへの適用

プロジェクト管理システム Redmine はチケット駆動型管理を採用している。ケース指向電子記録管理システムに活用できると考えられる機能について以下に整理する。

表 2-4　Redmine の機能とケース指向電子記録管理への適用

項番	ケース指向電子記録管理で求める事項	実現に役立つ Redmine の主な機能	解説
1	複数部門を跨るアクセス性	Web ベースのシステム	システムは Web ベースで構築される 社内に構築すれば複数部門からのアクセス環境が容易に構築できる
2	タスク実行履歴の記録(発生する情報全てを記録する)	タスク管理 (チケット管理)	①プロジェクトを構成するタスクを「チケット」として管理する ②タスクには進捗状況や実行時の様々な情報が記録できる
3	ひとつのケースの中に複数ケースが存在できる(キーケース、サブケースに分割して管理できる)	プロジェクト管理	①プロジェクトは複数のチケットの集合と考えられる ②Redmine はプロジェクトを複数管理することができる ③プロジェクトは親子構造を持つことができる
4	記録の利活用	Wiki	プロジェクト内の情報共有のため、Wiki を持つことができる。将来にわたり知識ベースとして活用できる
5	全ての文書、記録のリポジトリ	リポジトリとの連携	構成管理ツールとの連携可能 プロジェクトで生成されるソースプログラムだけでなく、文書もバージョン管理できる
6	利活用のためには過去の記録を適切に検索できること	検索	複数プロジェクトをまたがり検索ができる チケットに適切な情報を記載することで利活用につながる
7	適切なアクセスコントロール	ユーザ管理	①プロジェクトに参画するユーザを管理する ②LDAP(Lightweight Directory Access Protocol)[6]と連携可能 企業内のユーザ管理システムとの連携が可能
8	情報の有効活用のためにメタデータが必要	チケット	チケットには担当者や期日などそのタスクに必要な情報を持つ
9	情報のアーカイブ、パッケージ化による移転等	－	Redmine が管理するデータをパッケージ構造化しエクスポート、インポートする機能はない プラグインなどで実現できる可能性は残る

以下にプロジェクト管理ソフト Redmine をケース指向電子記録管理システムに当てはめたイメージ示す。

[6] ユーザや機器を管理するディレクトリサービスへの接続プロトコル

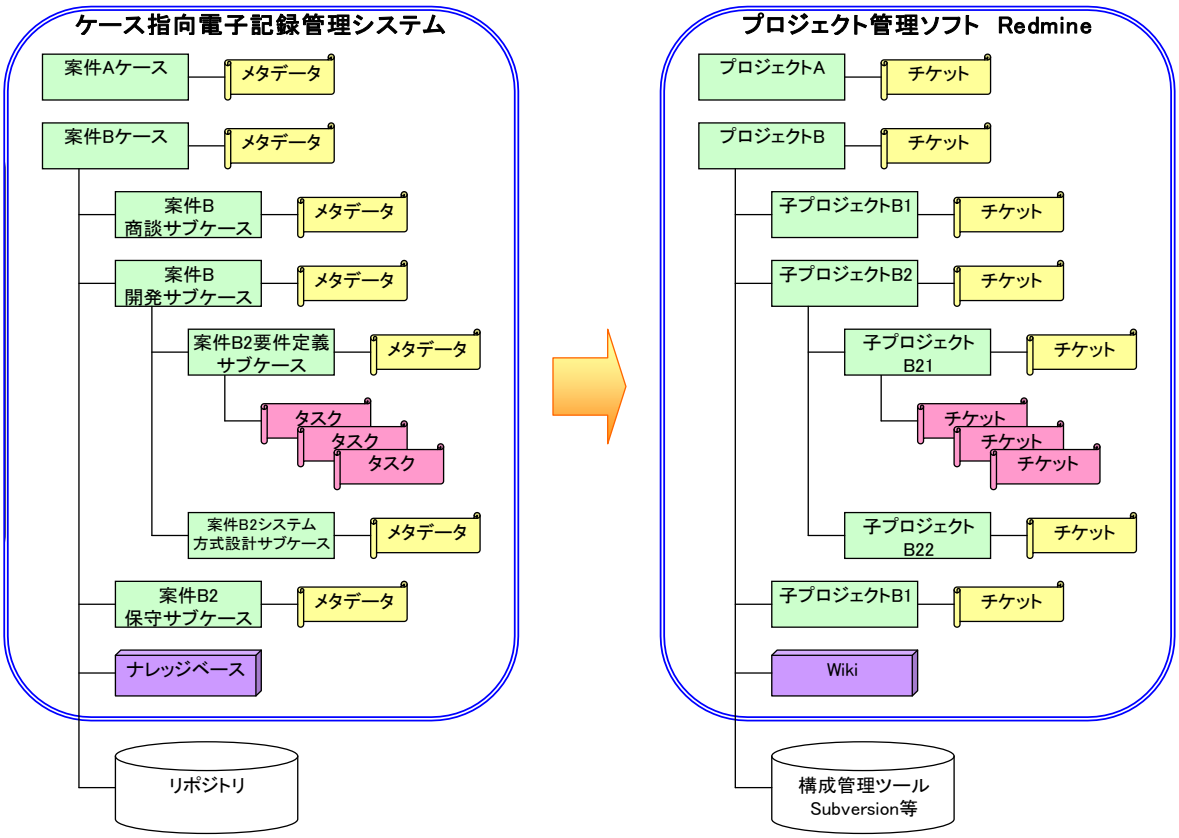


図 2-20　プロジェクト管理ソフトとケース指向電子記録管理システム

④メタデータの定義

ケース指向電子記録管理では記録の情報としてメタデータの定義が必要である。Redmine を用いる場合、チケットを活用することでメタデータを実現できると考えられる。チケットは本来タスクを管理するものであり、タスクの詳細情報として以下[7]の情報が記載できる。

- トラッカー[8]
- 題名
- 説明
- ステータス
- 優先度
- 担当
- 開始日
- 期日
- 添付ファイル

またチケットはステータスをもち、タスクの進行状況に応じてステータスが変化していくほか、「注記」として適宜情報が追記していける。ここに「なぜその対応を行ったか」を記載し

[7] 項目を追加することも可能である
[8] チケットの分類情報

ていけばその結果に至る経緯も記録していくことができる。

⑤運用、ルールで対応すること

ケース指向電子記録管理を行うにあたり運用手順やルールで対応すべき項目もある。

表 2-5　運用、ルールで対応すべき事項

項番	運用、ルールで対応	解説
1	ケース管理者の設定	ケース指向電子記録利活用のために複数組織にまたがりシステムが利用される。 そのため、組織横断的にケースを管理する部門、要員を置くことが望ましい。 ケース管理者は以下の役割を想定している。 ①関連部門からの依頼によりシステムにケースを新規登録 ②ケースの状態遷移に応じたコントロールを行う(新規登録、プロジェクト実行中、プロジェクト終了後、アーカイブ等)
2	ユーザ権限の設定	ケースの運用は営業、開発などの実務部門が行う。 ①ケース管理者は当該ケースにかかわる各部門の責任者の設定を行う ②各部門の責任者は必要に応じて部門のユーザを登録する
3	メタデータ情報の定義	企業内の利活用のため、どのようなメタデータを定義すればよいかを常に確認し、メタデータ定義を更新する
4	文書・記録のライフサイクルの設定	①法規制、社内ルールに基づき、システムで管理する電子記録の利活用期間、保管年限を設定する ②利活用期間を過ぎたものはパッケージとしてアーカイブし保管する。 ③保管年限を過ぎたものは破棄する
5	教育・指導	組織の成熟度モデルに応じて、要員教育を行い、成熟度を高める

(5) ケース指向電子記録管理アーキテクチャとプロジェクト管理ソフトウェアの対比

プロジェクト管理ソフトウェアをケース指向電子記録管理に活用するにあたり、eRAP の考えるアーキテクチャと対比させると、大きな相違がないことが確認できる。

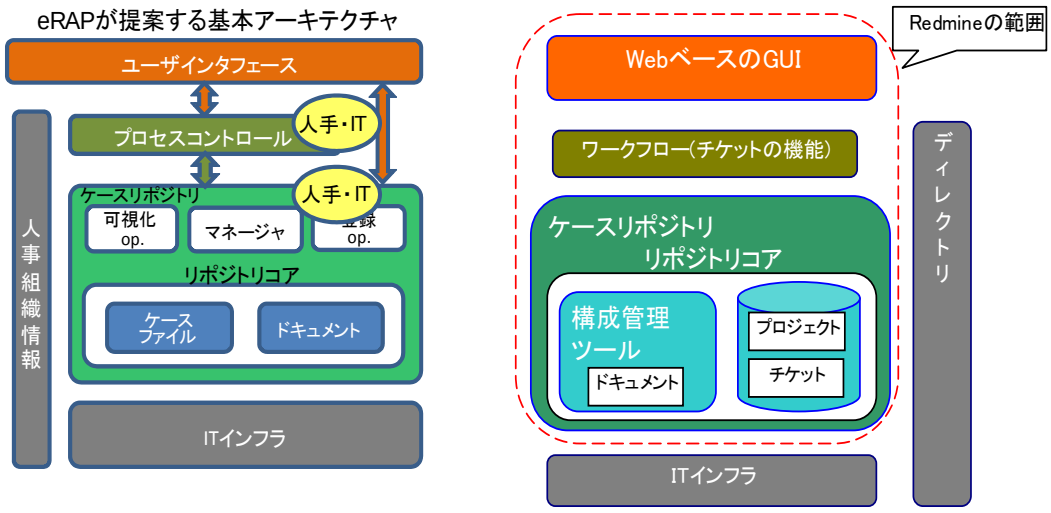


図 2-21　eRAP 基本アーキテクチャとの比較

(6)後半のまとめ　～　プロジェクト管理ソフトウェアで実現できる範囲と今後の課題

①プロジェクト管理ソフトウェアの導入でできること

Redmine の利用と運用ルールの設定によってプロジェクト管理におけるケース指向電子記録管理導入の課題は以下のように解決できると考えられる。以下に「表 2-3　プロジェクト管理におけるケース指向電子記録管理導入のための課題」で示した課題に対し、プロジェクト管理ソフトウェアでの解決可能性をまとめる。

表 2-6　ケース指向電子記録管理の課題とその解決

項番	プロジェクト管理におけるケース指向電子記録管理適用の課題	Redmine 活用による解決策	難易度
1	情報利活用のためのシステム間の連携がしにくい	個々のシステムとの連携用に機能拡張は必要 他のシステムが持つ処理の ID を Redmine 側に引き渡すインタフェースを準備する必要がある	高
2	部門をまたがり一括で案件を管理するシステムが無い	社内各部門からアクセスできるように Redmine を構築する(Web ベースなので容易) プロジェクト管理ソフトにユーザ登録を行いアクセスコントロールする	低
3	利活用を前提に文書管理をしていない	メタデータを定義し、チケットで表現する。それにより以後の検索機能に利用できる	中
4	プロジェクト局面毎のユーザ認証が不十分	LDAP を使えるので社内のユーザ管理システムと連携可能 局面毎にどのユーザのアクセスを認めるかはシステムではなく運用ルールと管理者が解決する	中
5	プロジェクト管理システムの機能不足(特に検索機能[9])	Redmine の検索機能では複数プロジェクトをまたがってチケット検索ができる チケットにメタデータとして必要な情報が全て記載できるかがポイント	中
6	記録管理ライフサイクルを考慮したシステムの使い勝手がよくない	プロジェクトがアクティブな時は Web ベースのインタフェースで使い勝手は良い しかし、プロジェクト終了後アーカイブの場合、十分な機能を持たない。パッケージ化しデータの移動や流通が容易になることが望ましい	中～高
7	現場に負担がかかると文書管理をしにくい	慣れが必要 ルールを定めケース管理者を設定する必要がある	中
8	文書管理ルール、手順が不明確	管理ルールを設定し、Redmin 利用手順を明確にする	－
9	文書管理ルールの組織的な適用が不十分	ケース管理者を設定する 文書管理(保存、利活用、廃棄など)のルールを設定 組織的な教育(成熟度モデル)	－

②今後の課題

・他のプロジェクト管理ソフトウェアの調査

今回調査したのは Redmine のみである。他にも優れたプロジェクト管理ソフトウェアは多数存在しておりそれらでケース指向電子記録管理が実現できるか比較調査する必要がある。

[9] もともと文書管理やケース指向電子記録管理を想定していないのでやむを得ない

・他システムと連携する方式を確立

他のシステムで管理される旅費や協力会社への発注情報などの ID と、プロジェクト管理ソフトウェアの各プロジェクトを紐付けし、プロジェクト管理ソフトウェア側から参照できるような仕組みを作る必要がある。

Redmine ではユーザがプラグインを実装することができるので、他のシステムとの連携ができると考えられる。

・他システムとのデータ互換

Redmine からデータをパッケージ構造でエクスポートできるようにする。それにより他のシステムとの互換を図る。パッケージ構造に格納するデータ、格納方法など検討が必要である。

・時間経過に伴うユーザ情報変化への対応

プロジェクト管理システムだけの問題ではないが、時間経過とともに登録ユーザのロールや所属の変化、退職による権限喪失、所管部門の変更などへの対応方法検討が必要である。

・実証実験の実施

本報告に記載した事項は調査による考察である。実際のプロジェクトに適用し、商談から運用・保守までケース指向電子記録管理が適用できるか、実証実験を行いより具体的な課題を抽出する必要がある。

(7) まとめ

現在のプロジェクト管理における文書・記録管理の問題点を整理し、プロジェクトを広範に案件ととらえ、プロジェクト管理にケース指向電子記録管理を適用することで、これまでより一歩進んだ電子記録利活用の可能性があることが確認できた。

しかし、IT システム化するには範囲が広範に及ぶため費用面で大きなハードルがある。

一方、現場で広く使われているプロジェクト管理ソフトウェアを工夫して使うことで、低コストである程度のケース指向電子記録管理を実践できる可能性が確認できた。現場レベルからケース指向電子記録管理が始まることは、企業の持つノウハウ、知識の活用につながり、企業の競争力強化につながっていくだろう。

そのためには今後実証実験などを行い、現場で無理なくケース指向電子記録管理を導入するためのガイドライン整備などが行われることが望ましいと考える。

2.4 ケース管理の実証実験

2.4.1 概要

(1) 目的

これまで eRAP で検討してきたケース管理の要件等を実際の業務に適用することにより、ケース管理の有効性を検証し、これまで作成したケース管理の成果物の評価を行うことを目的とする。

また、実際の業務でケース指向電子記録管理システムを運用することにより、ケース指向電子

記録管理システムの運用実績を作る。

(2) 期間

2012 年 10 月～2013 年 2 月

(3) 実験方法

以下のシステムをケース管理の要件を満たすようにカスタマイズ(プログラムの追加なしでシステムの提供する機能や設定のみを利用)し、そのケース指向電子記録管理システム上で、実業務で発生する記録を管理、活用する。管理、活用していく中で、ケース管理の有効性や課題を抽出する。

①Microsoft® SharePoint® Server

「ケース指向電子記録管理システム」の基本アーキテクチャのケースリポジトリを実現するため、マイクロソフト株式会社の Microsoft® SharePoint® Server (以下“SharePoint”とする)をカスタマイズし、ケース管理のメリットである記録の管理を容易にし、活用が進むかどうかの検証や課題の抽出を行う。

②Apeos PEMaster

「ケース指向電子記録管理システム」の基本アーキテクチャの全ての基本要素(ケースリポジトリ、プロセスコントロール、ユーザインタフェース)を提供する富士ゼロックスの Apeos PEMaster をカスタマイズし、ケース管理による業務プロセス視点での記録管理の実現、証跡にする記録を業務プロセスに従って管理することによる記録の登録状況並びに業務プロセスの進捗管理を視覚的に把握できることによる業務の効率化、記録の管理の簡易化と記録の活用ができるかを検証する。

なお、実業務で発生する記録は、紙、電子両方あるが、実証実験では、電子の記録のみ扱うこととする。紙の記録は可能な限りスキャニングし、電子記録として管理・活用する。

また、記録は電子稟議システムや経理システムなど他システムでも利用されるが、実証実験では、他システムとの連携は行わないこととする。

2.4.2 適用業務

実証実験で適用する業務の概要、業務フローを説明する。

(1) 業務概要

外部組織からの受託事業である情報セキュリティに関するセミナーを全国 5 か所で実施する。

実施期間は、2012 年 4 月から 2013 年 2 月までであり、セミナーの開催は、10 月から 12 月にかけて行い、セミナー参加者は、700 名程度である。

業務に従事する職員は、10 名である。

なお、当該業務は、過去数年間受託したことがあり、その際に発生した記録を現在でも保持しており、業務を実施する際は、過去に受託した際に発生した記録を活用している。

(2) 業務フロー

①受託

外部組織からの公募に対する提案書、見積りを作成、提出する。落札後、契約書の締結を行う。

②企画

セミナーの講師、講演プログラム、会場、開催日程、広報、パンフレット、デモの案を作成し、発注元に提案し、提案の承認を受ける。

③運営

企画の提案に基づいて、講師への依頼・委嘱、会場の確保、開催日程の調整、広報を実施する。また、パンフレット、講演資料を作成し、印刷会社に発注する。

講演と並行して､講演内容に関係するデモを実施するため､デモに参加する事業者を選定し、依頼を行う。

④後処理

納品物を作成する。関係者へのセミナー終了の礼状を送付する。

⑤監査

監査資料作成・対応などを行う。

(3) 記録の管理状況

適用業務で発生する全ての電子記録は、業務に従事する職員がアクセス可能なファイルサーバや個人 PC で、作成、管理している。このため、同じような電子記録が複数あること、何処に必要な最新の記録が入っているかは担当者が把握しているのみで、他者は探せないなどの問題がある。

(4) 実証実験で管理対象となる記録

これまでのファイルサーバでの管理のように作成した記録を全て管理するのではなく、適用業務の記録を管理する目的に沿った以下の記録のみ管理することとする。

①業務を遂行する際に重要となるスピード・グリーン・効率性・透明性・安全性・持続性・創造性を実現する記録

②外部、内部監査など説明責任の際に必要となる記録

2.4.3 システム要件

ケース指向電子記録管理システムを実現するのに必要となるシステム要件は､「組織の記録管理の問題・課題を解決すること」､「組織の記録管理の現状に対応できること」､「ケース管理の要件

を満足していること」とし、以下をシステム要件とした。

表 2-7　ケース指向電子記録管理システムのシステム要件

システム要件
案件ごとに発生する記録を 1 つの入れ物(ケース)で管理する
ケース、記録に、必要に応じてメタ情報を追加することができる
ケース中の記録を、メタ情報をもとに検索できる
ケース単位の記録の移管、廃棄ができる
ケースの状態を管理できる
ケースの中で管理される記録は、記録そのものではなく、記録のありかを示すリンクまたはユニーク ID である
紙の記録も管理(所在など)できる
複数の関連する記録を管理できる
ケースへのアクセスログ(作成、参照等)を管理できる
記録のメタ情報をある程度自動で設定できる

2.4.4　SharePoint

(1)実現方法

ケース管理を SharePoint で実現し、適用業務で利用する方法を説明する。

①ケース

適用業務は、年度ごとに案件が発生するので、ドキュメントライブラリ内に、年度ごとのフォルダを作成し、メタ情報を付加し、ケースとして利用する。ケースとして利用するフォルダには、メタ情報の集合であるコンテンツタイプを設定する。

ドキュメントライブラリは、SharePoint 上でドキュメントを管理、共有するためのものである。

コンテンツタイプは、SharePoint 上で、メタ情報、セキュリティポリシ、ワークフロー等を管理するためのものであり、このコンテンツタイプをフォルダ、ドキュメントごとに設定することが可能である。

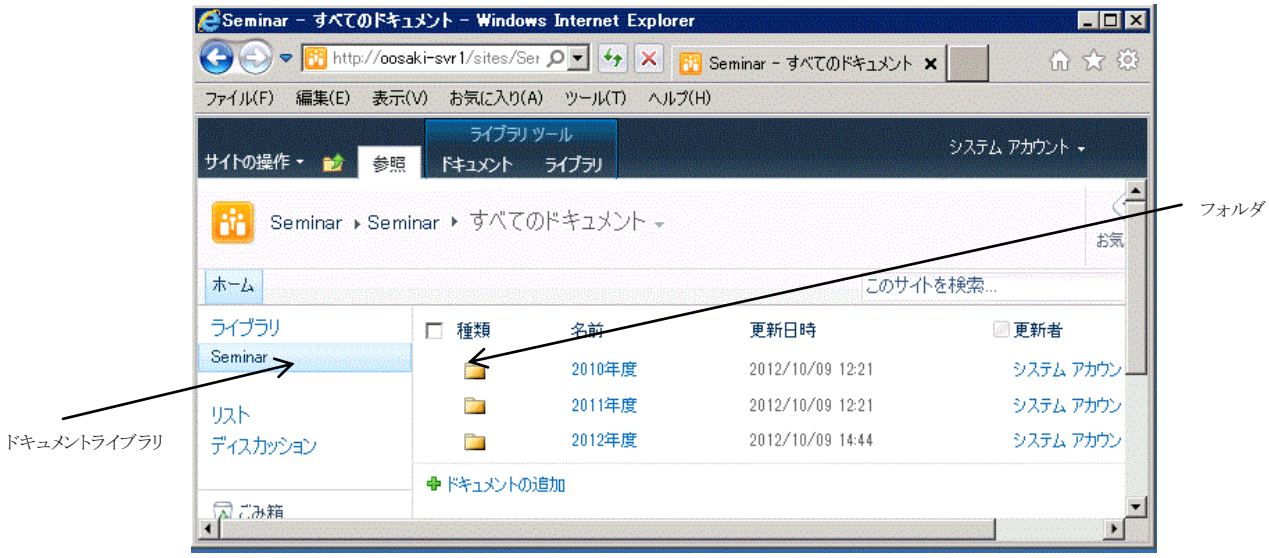


図 2-22　SharePoint によるケース管理画面

②ケース内の記録管理

ケース管理は、非定型な業務における記録管理に有効であるとされる。それは、業務プロセスが定型化できない、あるいは定型化しても変更になるなどの問題に対応できるためである。

ケース管理は、ケースという入れ物に構造化せず記録をメタ情報付きで管理することにより、管理を容易にし、活用(必要な記録を直ぐに見つけることができる)しやすくすることができるというメリットがある。

一方、ケース内に全ての記録を構造化しないで管理すると、必要となる情報は一見しただけでは見つからず、常にメタ情報をもとに検索しないと見つけられないといった問題がある。そもそもどのようなメタ情報があるかを事前に分かっていないと記録を見つけられないといった問題もある。

本来は、メタ情報をもとに、利用者がよく利用する記録を、利用者の要求による形式で表示させるユーザインタフェースを提供すべきであるが、SharePoint でこの機能を実現するには専用のプログラムの作りこみが必要となる。

そこで、よく利用する記録の表示形式を、以下のようにケース内にフォルダを設け、その中に関係する記録を管理することとする(更にフォルダ内の中にフォルダを作成することもある)。

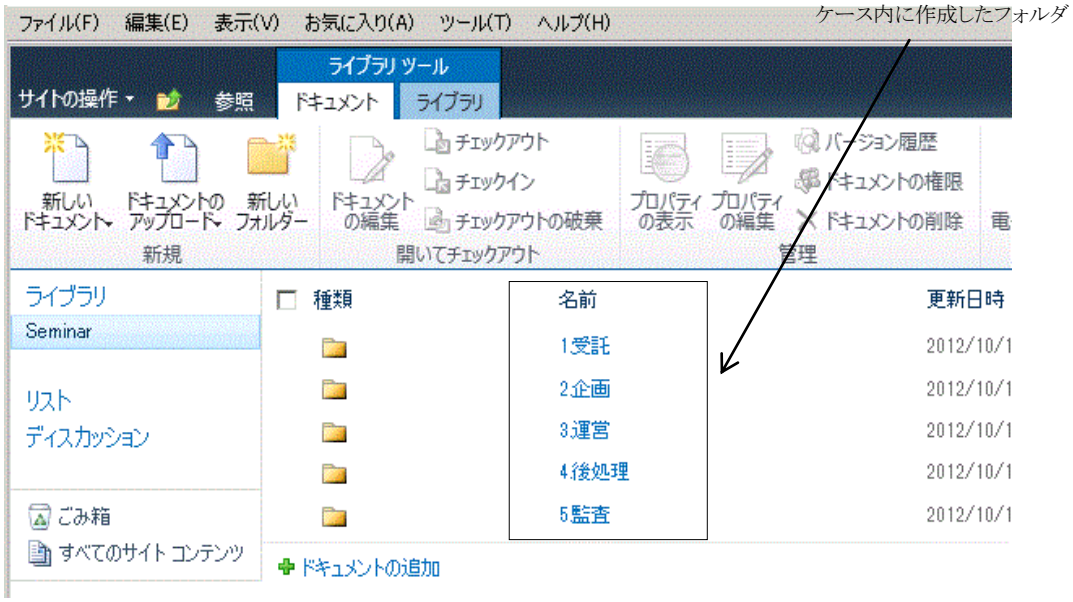


図 2-23　ケース(2012 年度)内のフォルダー覧

③メタ情報

○ケースのメタ情報

以下のメタ情報を持つコンテンツタイプを作成し、ケースに関連付ける。

・ID、説明、状態、所有者、責任者、取扱者、作成日

○記録のメタ情報

分類ごとに分類固有のメタ情報をもつコンテンツタイプを作成し、記録に関連付ける。分類は、記録の分類であり、以下がある。

・会場、講師、広報、講演、印刷物、デモ、監査、契約、稟議

なお、全ての記録に共通するメタ情報には、以下がある。

・ドキュメント ID、説明、状態、所有者、作成日、分類、プロセス名

(2) 実証実験環境

実証実験を行った環境は以下である。

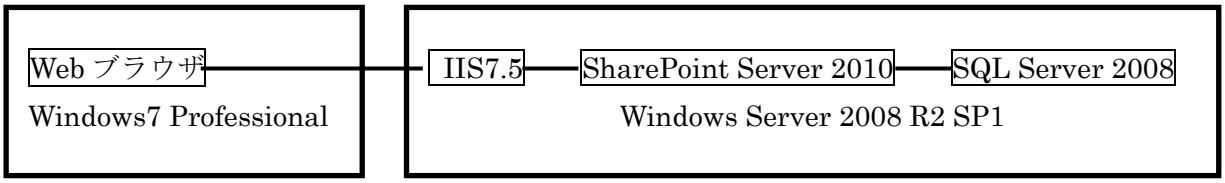


図 2-24　実証実験環境(SharePoint)

(3) 結果

SharePoint を利用した実証実験を行った結果、ケース管理の以下の有効性、課題があることが分かった。

①有効性

○記録の管理が容易

・記録の一括移管・廃棄が容易

ケース内に関係する記録が一括管理されているので、業務終了後の記録の移管、廃棄が容易である。

・記録の重複管理の解消

これまでの記録の管理は、ファイルサーバや担当者の PC で行っており、似た記録が複数散在し、どれが最新か分からない状況であった。ケースで一元管理することにより、このような問題は起こらなくなった。

○記録の活用の推進

・記録の検索が容易

記録作成者以外(あるいは他部署の者)が必要な記録を探す場合、ケース内に記録が一元管理されているので、ケース内を探せばよく、必要な記録の検索が容易となった。

また、メタ情報をもとに必要な記録を直ぐに探すことができるようになった。

○セキュリティの向上

・記録へのアクセスの把握

これまではファイルサーバや個人 PC に記録が散在し、誰がいつ何の記録にアクセスした

かを把握することが出来なかったが、ケースで一元管理し、ケースへのアクセスログから記録へのアクセスを把握することが可能となりセキュリティの向上につながった。

〇組織としての記録管理の推進

これまでは、属人的に記録の管理が行われており、組織として記録を管理する意識が少なかった。

しかし、ケースという入れ物に記録を一元管理し複数部署で記録を管理・活用すること、ケースを管理する責任者を決めたことにより、組織全体として、記録の見える化、責任の明確化が実現でき、組織として記録を管理・活用するという意識が高くなった。

②課題

・記録の表示形式のカスタマイズ機能

記録を検索するのに常にメタ情報をもとに検索するのは、コストがかかることから、よく利用する記録を、メタ情報をもとに、利用者が記録の表示形式を予めカスタマイズする機能が必要である。

例えば、メタ情報をもとに記録の分類、所有者、責任者、作成日ごとに記録をグループ化し表示する機能があると、必要な記録を直ぐに見つけることができる。

・適切なメタ情報の設定

必要な記録は、記録に付与されているメタ情報をもとに記録を検索しみつける。このため、適切なメタ情報が記録に設定されていないと、必要な記録を見つけることができない。

そこで、記録の分類(例えば税務記録、監査記録など)ごとにどのようなメタ情報を付ければよいかを支援する機能など、記録に適切なメタ情報を付与するための支援機能が必要である。

・検索支援機能の提供

記録を検索する際に、適切なメタ情報を指定し、検索を行わないと、必要な記録を検索できないこととなる。そこで、ケース内の記録にどの様なメタ情報があるかなど、検索を支援する機能が必要である。

・メタ情報の入力の簡易化

記録をケースに登録する際にメタ情報を入力する必要がある。メタ情報の入力には多い場合で 10 を超えることもあり、メタ情報入力を支援する、あるいは自動入力する機能が必要である。

2.4.5 Apeos PEMaster

(1)実現方法

ケース管理を Apeos PEMaster で実現し、適用業務で利用する方法を説明する。

①ケース

運用ルールに基づき業務プロセス単位でケースを作成する。業務プロセスは動的に登録、変更、削除が可能である。図のようなユーザインタフェースからメタ情報を付与して文書管理システムに登録する。予めどのようなメタ情報を付与するかケースごとに設定することができ、更に登録の際にも付与する属性を動的に変更することが可能である。ケース単位で管理されており、案件 ID、案件名、担当者等で検索を行うことが可能である。

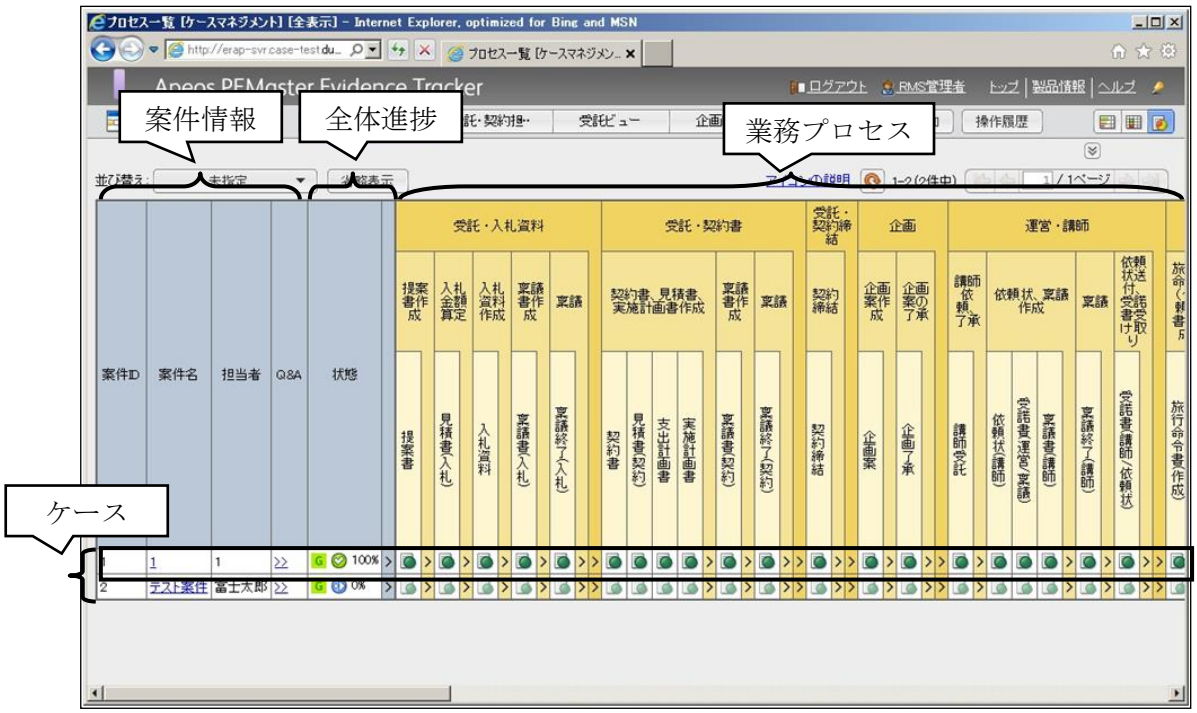


図 2-25　Apeos PEMaster Evidence Tracker による記録管理画面

②ケース内の記録管理

実際の記録管理は文書管理システムである Apeos PEMaster Evidence Manager(以下“Evidence Manager”とする)で行う。利用者が実際に記録を登録、閲覧する場合は、専用のユーザインタフェースである Apeos PEMaster Evidence Tracker(以下“Evidence Tracker”とする)から行う。Evidence Tracker から登録された記録は自動的に予め設定した格納先に Evidence Manager を通して格納される。例えば、契約書を登録する場合、契約書のファイルを Evidence Tracker 上の契約書該当アイコン(図 2-25)にドラッグアンドドロップするだけでよく、利用者がファイルの格納位置を意識する必要はない。また、セキュリティ強化のため登録された記録をユーザが操作した場合、操作ログとして操作したユーザ、操作日時、操作の内容が表示され履歴として残る。

③記録の登録状況の可視化

記録の登録状況をアイコン形式の一覧で表示する。アイコンは記録の必要度(必須、任意、その他)を形状で識別でき、記録の登録状況(登録済み、未登録、未登録(納期遅れ))を色合いで識別することができる。また記録アイコンからポップアップ画面を開いて、文書の属性や内容

を確認することができる。

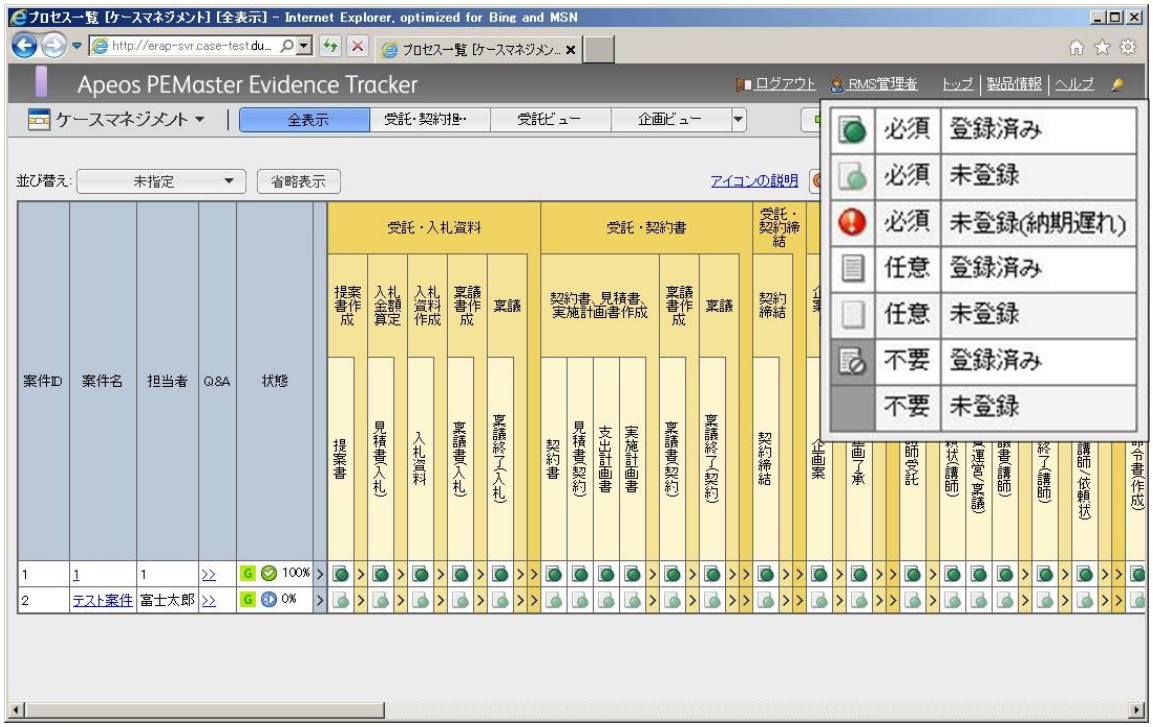


図 2-26　登録状況アイコンの一覧

④業務プロセスの進捗管理の可視化

進捗状況の可視化を行うことによって、記録の登録状況で進捗を管理でき、全体の進捗状況を一目で確認することができる。各フェーズで納期を設定することができ、記録が納期までに登録されていない場合は自動でユーザにメールで納期遅れを通知する。また前フェーズの記録が全て登録されないと次フェーズへは移行できないようにすることが可能である。

(2) 実証実験環境

実証実験を行った環境は以下である。

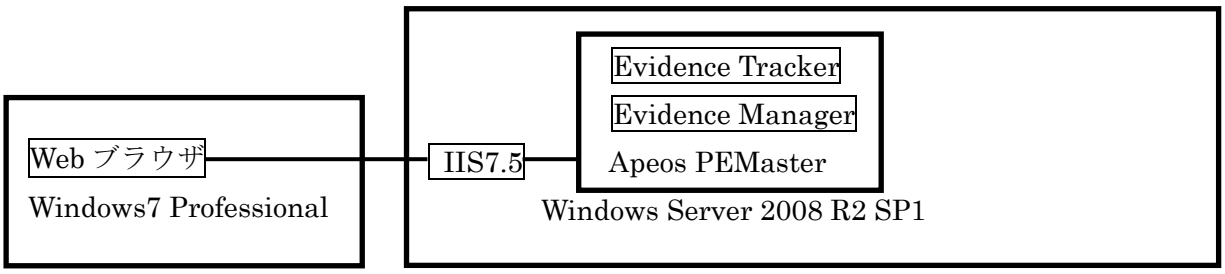


図 2-27　実証実験環境(Apeos PEMaster)

(3) 結果

Apeos PEMaster を利用した実証実験を行った結果、ケース管理には以下の有効性があることが分かった。

①記録の管理が容易

・記録の登録が容易

記録を登録する際は、何処で記録を管理するかなど考える必要がなく、Evidence Tracer が提供するユーザインタフェース上のアイコンに、登録する記録をドラッグアンドドロップするだけで記録を登録できる。利用者は、作成した記録を、マウスを使って登録するだけでよいので、記録の登録が容易である。

②記録の活用が推進

・利用者視点の記録の見える化による記録活用の推進

ケース管理はケースに構造化せず記録を管理する。構造化しないために記録の登録が容易である反面、記録を探す際は記録に付与されたメタ情報をもとに検索する必要がある。頻繁に利用する記録を探す場合も常にメタ情報による検索を行わなければならない。

Apeos PEMaster は、利用者が頻繁に利用する記録の表示形式を、予めメタ情報を指定し、記録をどのように表示するかを複数定義することができる。この機能を利用し、頻繁に利用する記録を直ぐに探すことができる。例えば、業務プロセスで発生する記録を業務プロセスごとに表示するなど、利用者視点の表示が可能であり、記録の検索を容易にし、記録活用の推進につなげることができた。

・業務プロセス視点での記録管理、進捗管理の実現

業務の中には複数の業務プロセスがあり、その業務プロセスの最終成果として記録が作成される。Apeos PEMaster は、業務プロセスと業務プロセスで発生する記録を予め定義することにより、業務プロセスで発生する記録の管理と、記録の業務プロセスへの登録状況から業務の進捗管理の見える化を実現している。大人数が参加し、業務プロセスが多い業務などでは、現在の進捗状況をリアルタイムに把握することは難しい状況であるが、この機能を利用することによりリアルタイムに進捗を把握することが可能である。

更に、必要な記録が全て揃っているかどうかも画面を見ればわかるようになっており、記録の作成漏れが直ぐにわかるようになっている。

③非定型業務での記録管理への対応

・業務プロセス変更への柔軟な対応

業務プロセスと記録を関係づけて記録を管理することによるメリットは多い。特に定型業務のように業務プロセスが変更にならない業務の場合は有効であり、現に、多くの組織で記録を管理するためのシステムが構築され運用されている。一方、業務プロセスが頻繁に変更になる非定型な業務での記録の管理を行う場合、このような業務プロセスと記録を関係づけて管理するのは難しいとされてきた。

Apeos PEMaster は、動的に業務プロセスの登録、変更、削除が可能であり、非定型な業務や、新しくできた業務でどのような業務プロセスが発生するか不定な場合に有効である。

今回の適用業務の場合、セミナーパンフレットを、新たにもう 1 つ作成することとなっ

た。このような場合でも、新たなパンフレットを作成することが決まった段階で、このパンフレット作成のためのタスクを Apeos PEMaster に追加することで、直ぐに対応することが可能であった。

2.4.6 まとめ

これまで eRAP で検討してきたケース管理のシステム要件を使い実証実験を行った結果、実業務で、記録の管理を容易にし、活用を推進できること、及び実業務でのケース管理の運用が十分可能であり、有効であることが分かった。一方で、ケース管理の課題についても抽出することができた。以下にその具体的な有効性や、課題を示す。

(1) 有効性

①記録の管理が容易

ケース管理を導入することにより、「記録の登録が容易」「記録の一括移管・廃棄が容易」「記録の重複管理の解消」が実現でき、記録管理が容易になった。

②記録の活用の推進

ケース内に記録が一元管理され、かつ記録にメタ情報がついているため、必要な記録を検索するのが容易となり、記録活用の推進につながった。

また、ユーザインタフェースを充実させることにより、「利用者視点の記録の見える化」「業務プロセス視点での記録管理、進捗管理の実現」も可能となる。

③セキュリティの向上

ケース内で記録を一元管理することにより、記録へのアクセスを容易に把握することが可能となりセキュリティの向上につながった。

④組織としての記録管理の推進

ケース内に記録を一元管理し複数部署で記録を管理・活用すること、ケースを管理する責任者を決めたことにより、組織全体として、記録の見える化、責任の明確化が実現でき、組織として記録を管理・活用するという意識が高くなった。

(2) 課題

ケース管理をより有効に、かつ使いやすくするには以下を実現する機能が必要である。

①記録の表示形式のカスタマイズ

記録を検索するのに常にメタ情報をもとに検索するのは、コストがかかることから、よく利用する記録を表示する形式を、利用者が予めメタ情報をもとにカスタマイズし、表示する機能が必要である。

②適切なメタ情報の設定

適切なメタ情報が記録に設定されていないと、必要な記録が見つけることができない。そこで、どのようなメタ情報を記録に付ければよいかを支援する機能など、記録に適切なメタ情報を付与するための支援機能が必要である。

③検索支援機能の提供

記録を検索する際に、適切なメタ情報を指定し、検索を行わないと、必要な記録を検索できない。そこで、ケース内の記録にどの様なメタ情報があるかなど、検索を支援する機能が必要である。

④メタ情報の入力の簡易化

記録にメタ情報を設定する際、メタ情報の数が多い場合もあることから、メタ情報入力を簡易に行う(例えば、入力する際に、入力候補を一覧から選択するなど)、あるいは自動入力する機能が必要である。

参考文献

[1] 独立行政法人　情報処理推進機構(IPA). “ソフトウェア・エンジニアリング　エンタプライズ系プロジェクト”. http://sec.ipa.go.jp/std/ent.html

[2] プロジェクト管理ソフトウェア　Redmine. Redmine 公式サイト. http://www.redmine.org/

[3] プロジェクト管理ソフトウェア Redmine 日本語情報. http://redmine.jp/

[4] 前田剛. 入門 Redmine 第 3 版. 株式会社秀和システム, 2012 年 8 月

[5] 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 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-. 一般財団法人日本情報経済社会推進協会, 2012 年 3 月

[6] プロジェクト管理ソフトウェア Redmine に関する各種ブログ、ニュース記事等

第 3 章　パッケージ構造

本章では、記録とメタデータ、及び前節で述べたケースとメタデータを一体化するパッケージの標準形式案を紹介する。2011 年度の報告では、電子記録管理において最も重視される要件を法的証拠性の確保として個々の電子記録を対象としたパッケージ構造の標準形式を提案した。本年度は、複数の記録が含まれるケースを対象としたパッケージ構造の標準形式を提案する。

3.1　電子記録マネジメント基盤とケースファイル

文書や記録の電子化が進展する中、特に国内においては電子文書や電子記録のマネジメントの意識が低く、電子文書や電子記録のマネジメント不在の状態からなかなか脱することができない状況にある。

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。木村らは文献[1] で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。

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、電子記録の証拠としての証明力が重視される。また、デンマークや韓国等では、記録管理を業務と密接に関連付けて統合管理する「ケース管理」に取組んでいる。

本節では基本概念として、電子記録、電子記録マネジメント、電子記録マネジメント基盤、ケース管理について説明する。

3.1.1　電子記録

電子記録の定義は ISO 15489-1[2]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。

3.1.2　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[2]に準じるものである。文献[1] では、MoReq2(Model Requirements for the management of electronic records)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。

3.1.3　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[1]。

電子記録マネジメント基盤の位置付けを図 3-1 に示す。

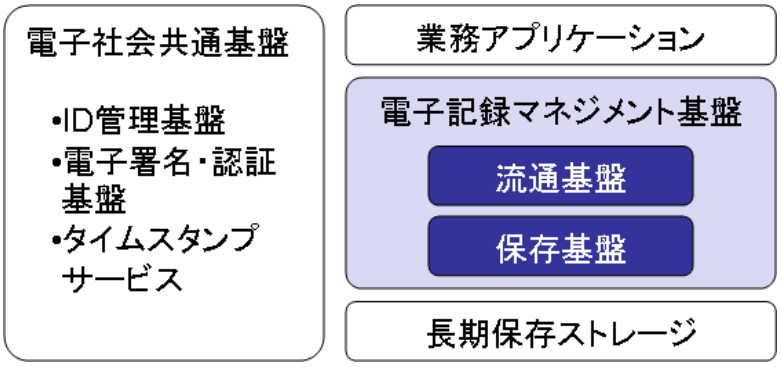


図 3-1　電子記録管理システムの構造と電子記録マネジメント基盤の位置付け

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管理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。

電子記録管理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 つの電子記録管理システム／電子記録マネジメント基盤より他の電子記録管理システム／電子記録マネジメント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。

3.1.4　ケース管理

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管理の概念を導入している[3]。この概念の導入目的は、決定過程を含めた記録の管理と記録の利活用の促進である。

決定過程を含めた記録管理のためには、複数組織にまたが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。

図 3-2 に業務とケース管理の関連を示す。一連の業務からなるケース(案件)が生じると、ケース管理システムは案件に対応するケースファイルを生成する。業務は 1 つあるいは複数の業務プロセス支援システム(IT システムによる支援のない手作業を含む場合もある)が支援し、そこで生じる文書類を各種属性とともに記録としてケース管理システムがそのケースファイルに蓄積していく。ケースはサブケースを含む場合も考えられ、その場合はケースファイルにサブケースが格納される。つまり、ケースファイルは入れ子状態になる場合がある。1 つの案件の開始から終了までの全ての記録及び属性は、最終的に 1 つのケースファイルに格納される。

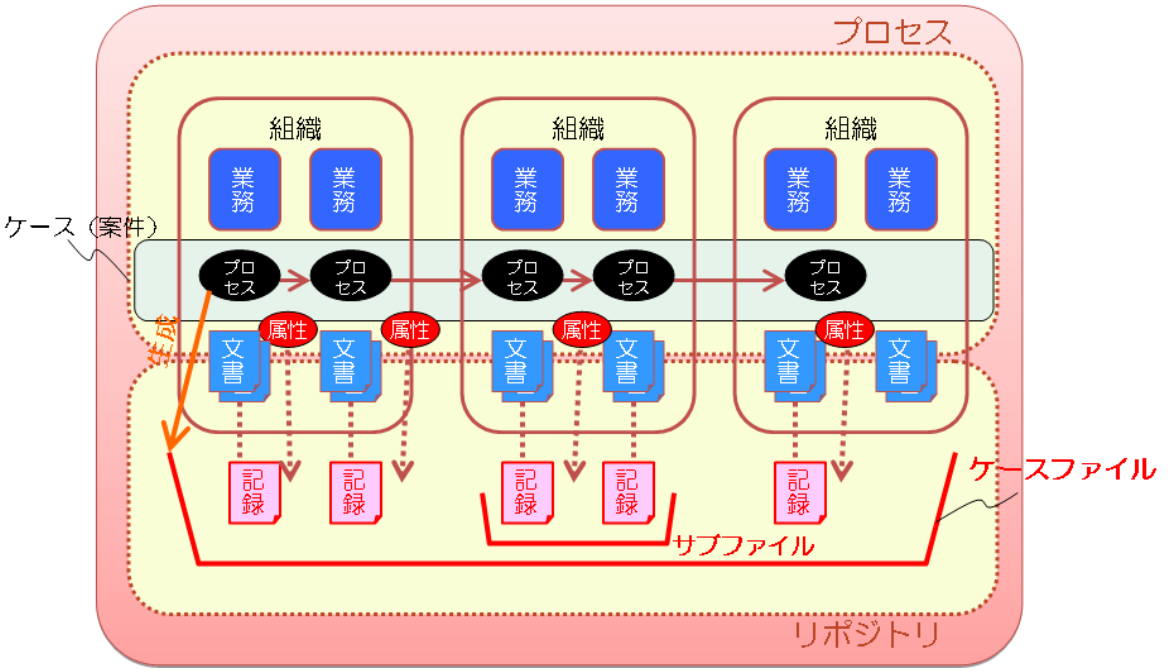


図 3-2　業務とケース管理の関係

1 案件に対して生成される 1 ケースファイルは、図 3-3 のような構造となる。

「属性」は、ケース自体の属性、「状態」はケースの処理の進行段階、「関係」はケースと他のエンティティ(他のケースや担当者)との関係である。

また、ジャーナル項目にはケースに関わる複数の記録が関連付けられる。個々の記録には、それぞれ各種属性が添付される。

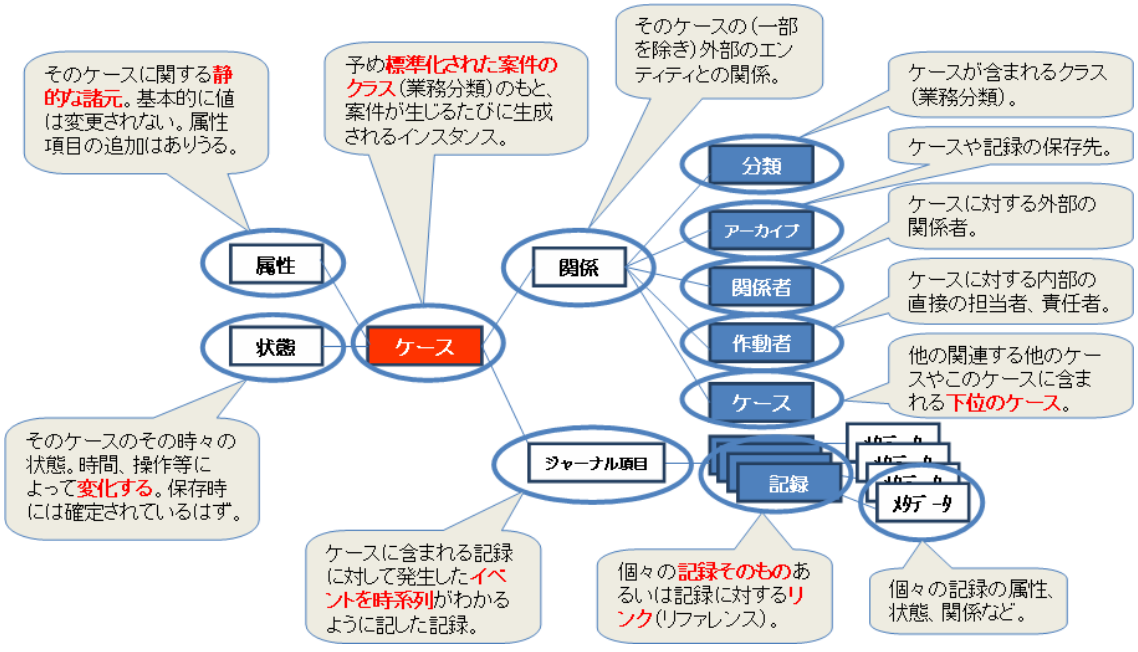


図 3-3　ケースの構造

3.2　パッケージの海外技術動向

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[4]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 3-4 に示す。

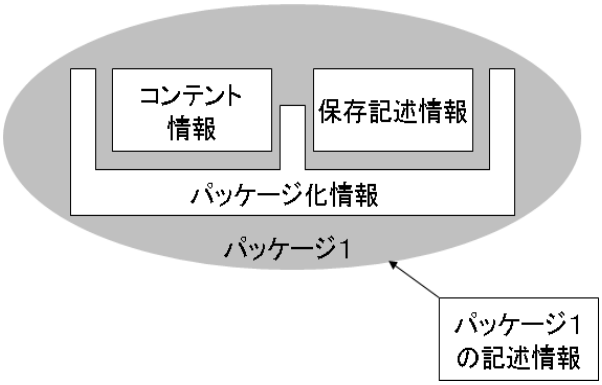


図 3-4　OAIS 参照モデル―パッケージの構造

パッケージの種類として、保管・保存システムを中心に次の 3 種類が定義されている(図 3-5)。

・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。

図 3-5　OAIS 参照モデル―パッケージの種類

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 3-6 に示す。

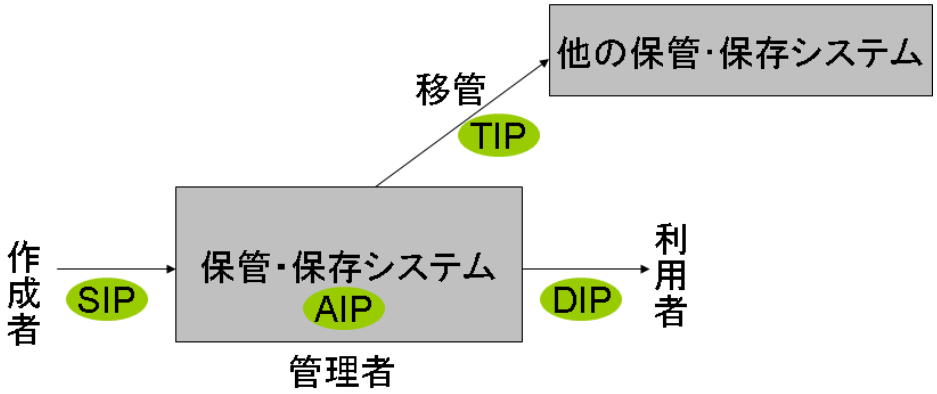


図 3-6　OAIS の拡張

欧州電気通信標準化機構(以下“ETSI”とする)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 Associated Signature Containers (以下“ASiC”とする)[5]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。

コンテナ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 1 つ以上の署名やタイムスタンプを含むコンテナ(図 3-7)
・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 1 つ以上の署名やタイムスタンプを含むコンテナ

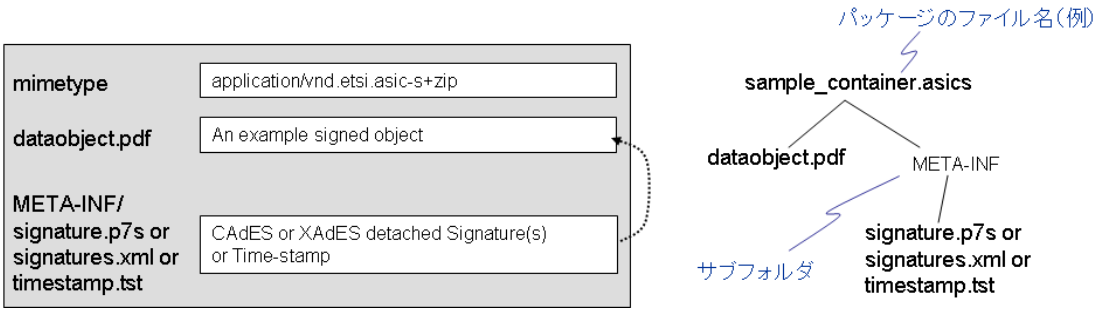


図 3-7　ASiC-S の構造とフォルダ構造の例

ASiC-E には、XML 型の長期署名(以下“XAdES”とする)[6]を含むものと CMS 型の長期署名(以下“CAdES”とする)[7]またはタイムスタンプを含むものがある。それぞれを図 3-8～図 3-9 に示す。

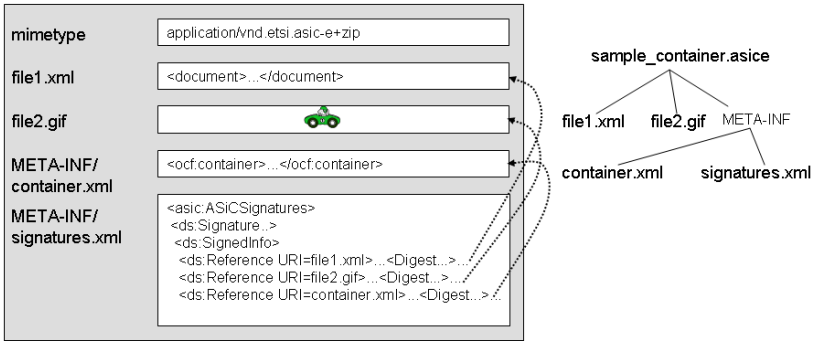


図 3-8　ASiC-E[XAdES を含む形式]の構造とフォルダ構造の例

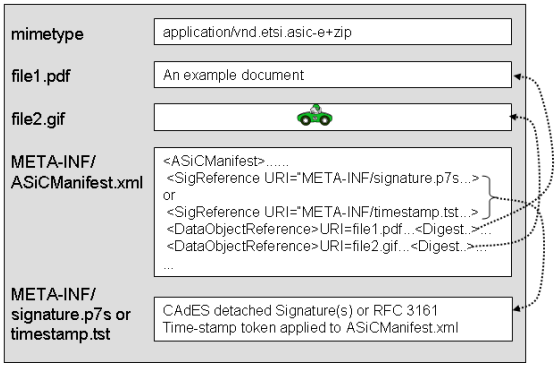


図 3-9　ASiC-E[CAdES またはタイムスタンプを含む形式]の構造の例

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 3-10 に示す。

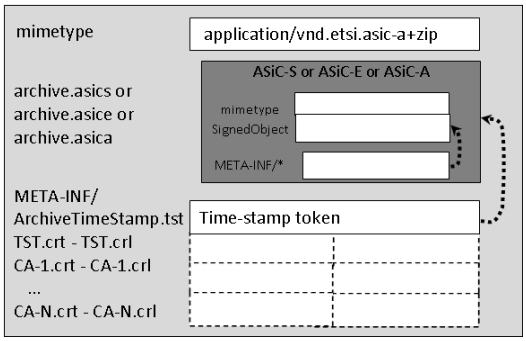


図 3-10　ASiC-A：長期検証型 ASiC の構造の例

3.3　パッケージ構造の提案

3.3.1　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 2011 年度に eRAP に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、記録の受取り／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[6]や CAdES[7]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 3.2 節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[8]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 3-11 に示す。

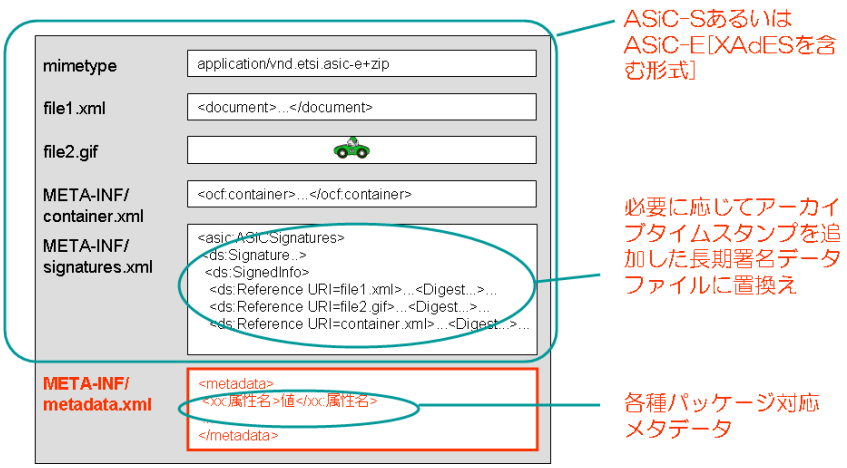


図 3-11　ASiC をベースとした電子記録マネジメントのためのパッケージ構造案

[要件 3]への対応については前述した。図 3-10 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 3-12 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。

[要件 5]に対応するためには、図 3-10 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。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 3-10 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。

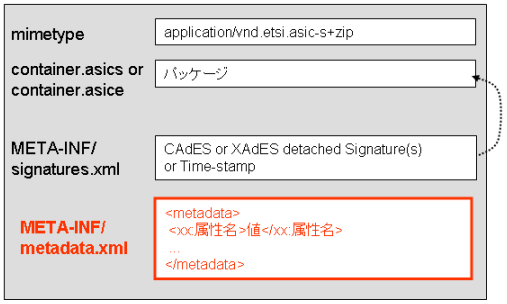


図 3-12　メタデータ自体を記録としたい場合のパッケージ構造例

3.3.2　ケース管理に対応したパッケージ構造提案

更に本項では 2012 年度の新規テーマとして、ケース管理に対応する要件を提案し、その要件を満足するパッケージ構造を提案する。なお、ケース管理システムと電子記録マネジメント基盤の関係は図 3-13 の通りとし、電子記録マネジメント基盤には完了したケースに関する情報が SIP として提出されることを前提とする。

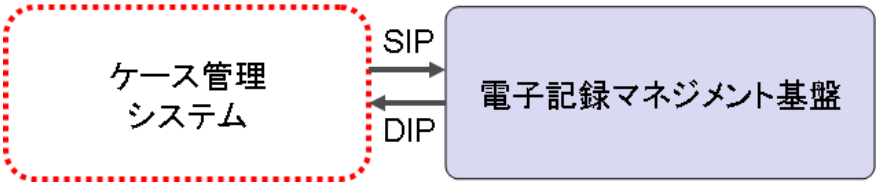


図 3-13　ケース管理システムと電子記録マネジメント基盤との関係

[要件 6] ケースには、ある場合はサブフォルダを伴い、複数のコンテンツが格納される。

[要件 7] ケースにはコンテンツの他に多くの属性(メタデータ)が含まれる。ケースにとって属性は極めて重要な情報であるため、ケースの証拠性を確保するためには属性の正当性の確保が必須である。

[要件 6]にあるように、ケースには複数のコンテンツ(記録)と属性が含まれる。また個々のコンテンツも属性を伴う。また[要件 7]にあるように、ケースに格納される個々のコンテンツ(記録)は個別に証拠性確保のために長期署名を付す必要がある場合と、ケースとして一体化した全体に対して証拠性確保のために長期署名を付せばよい場合が考えられるが、それに加え、ケース全体の証拠性を確保する必要もある。

このとき、コンテンツごとに図 3-11 で示したパッケージ構造を採用する必要があるが、長期署名データを付与する場合とそうでない場合が考えられる。

ケースに対応するパッケージを構築する場合、コンテンツごとのパッケージとサブファイルが存在する場合はそこに含まれるコンテンツに対するパッケージを更にパッケージ化し、それらケース内のコンテンツ及びサブフォルダのパッケージを集め、ケースの属性を与えてパッケージを構成する。更にケースの証拠性確保のため、更に外側にパッケージ構造をかぶせ、長期署名を付す。この構造を図 3-14 に示す。

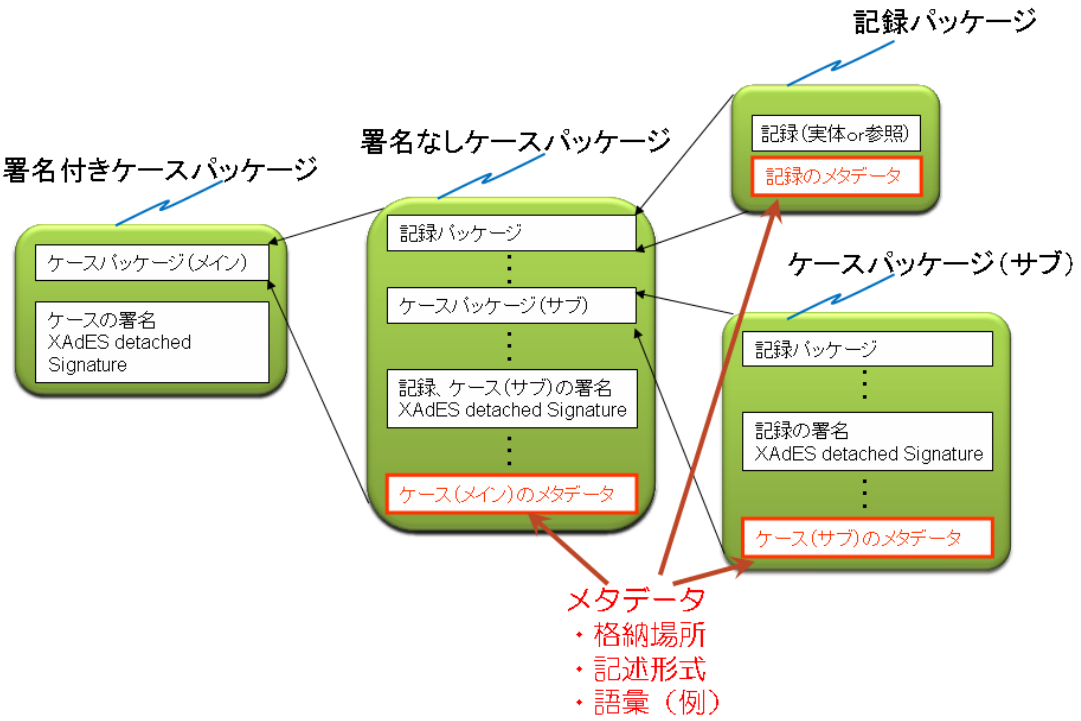


図 3-14　ケースのパッケージ構造

上記のようにケースに対するパッケージを構成すると、コンテンツの容量や数によってはパッケージの容量が膨大となる可能性がある。ケースのパッケージでは主に属性やそこに含まれるコンテンツの包含関係のみを集約し、コンテンツ自体は切り離して管理することが都合のよい場合も考えられる。このような場合、ケースのパッケージに格納するコンテンツの情報としては、URI やユニーク ID 等のコンテンツへの参照情報とコンテンツのハッシュ値のみを格納することが考えられる(図 3-15)。ハッシュ値を格納することにより、ケースとしてのコンテンツまでを含めた証拠性確保が可能となる。しかしこのとき、将来にわたって充分に安全性が確保できるハッシュアルゴリズムを採用することに注意が必要である。使用するハッシュアルゴリズムの安全性低下が予想される場合は、旧ハッシュ値とコンテンツを結合した値に対する新たなより安全性の高いハッシュアルゴリズムによるハッシュ値をパッケージに加える等の対処をとる必要がある。

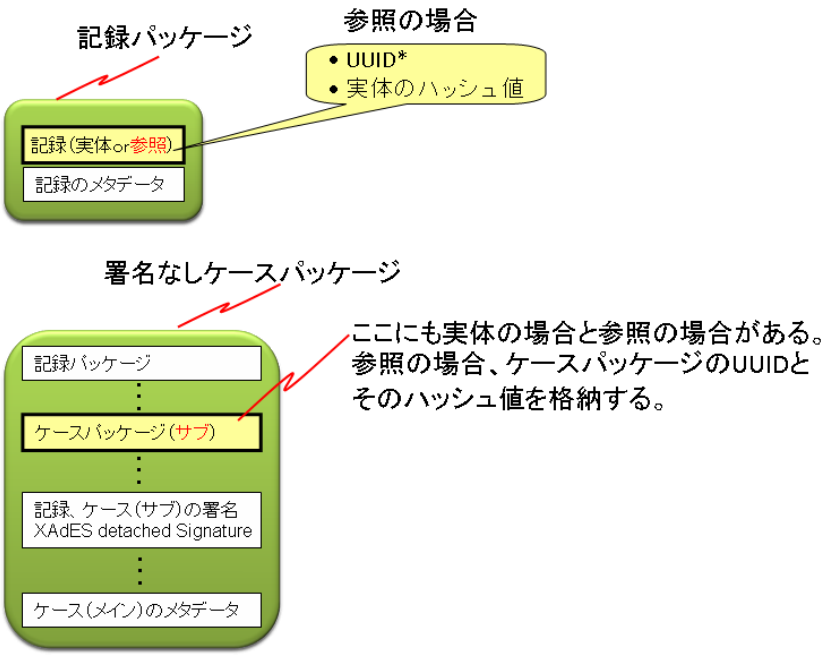


図 3-15　記録／ケースの格納方法

3.4　今後の課題

電子記録マネジメント基盤とこの基盤が導入するケース管理の概念を想定し、個々の記録だけではなく、一連の記録が関連付けられる「ケース」を対象としたパッケージ構造を考案した。複数のコンテンツを扱え、更に階層化も可能な ASiC を基本として、ケースに対応するパッケージを定義できた。運用時の様々な状況からのパッケージ構造の評価が今後の課題である。パッケージが持つべき具体的な属性(メタデータ)に関しても、ISO 23081-2[9]をベースとし、ドイツや韓国の例も参考にしながら検討したい。

参考文献

[1] 木村道弘、前田陽二、辻秀一. クラウド時代の情報流通基盤. 一般社団法人情報処理学会 第 118 回 情報システムと社会環境研究発表会, IS118-05(2012).

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

[3] 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 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-. 2012 年 3 月.

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

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

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

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

[8] 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
[9] ISO 23081-2:2009 Information and documentation -- Managing metadata for records -- Part 2: Conceptual and implementation issues

第 4 章　記録の管理と成熟度モデル

4.1　組織における記録管理の成熟度モデル

以下では、組織における記録管理の成熟度モデルとして、ARMA International によって開発された GARP (The Generally Accepted Recordkeeping Principles) [1]をベースとした“情報ガバナンスに関する成熟度モデル”(ARMA International Maturity Model for Information Governance)[2]、及び、Standards Australia から発行されている HB-278:2009 (Recordkeeping Compliance)[3]について概説する。

これら 2 つの成熟度モデルは、図 4-1 のように競合関係ではなく、相互に補完し合う関係にある。

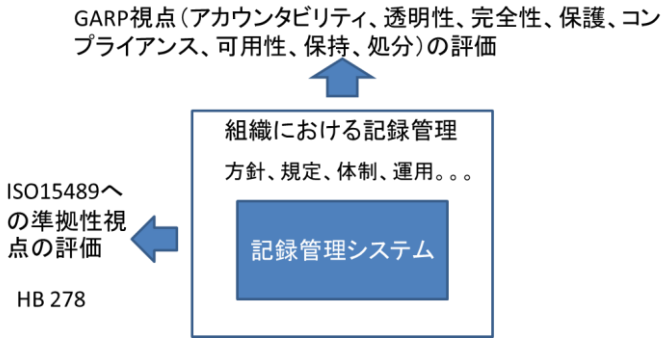


図 4-1　2 つの成熟度モデルの関係

4.1.1　情報ガバナンスに関する成熟度モデル

以下では、“情報ガバナンスに関する成熟度モデル”のベースとなっている”GARP”の概念及び成熟度モデルの概要を紹介するとともに、評価基準の改善提案を行う。

(1) GARP

GARP (The Generally Accepted Recordkeeping Principles) は、広く認められた記録管理の原則であり、次の 8 つの原則から成り立っている。

(a)アカウンタビリティ

上級幹部(あるいは匹敵する権威者)は、記録管理プログラムを監督し、適切な人員にプログラムの責任を委任する。

組織は、従業員をガイドする方針や手順を取り入れ、かつ、プログラムを監査できることを保証する。

(b)透明性 (transparency)

組織の記録管理プログラムのプロセス及び活動は、オープンで、検証可能で、全ての人員及

び適切な利害関係者に利用可能な方法で文書化されている。

(c)完全性（integrity)

記録管理プログラムは、生成される記録や情報が、信憑性と信頼性の合理的かつ適切な保証をもって、組織が管理できるように、構築されなければならない。

(d)保護（protection)

記録管理プログラムは、個人、機密、特権、秘密、業務継続にとって不可欠な、記録及び情報に合理的なレベルの保護を保証するように構築されなければならない。

(e)コンプライアンス

記録管理プログラムは、組織の方針と同様に、準拠法及び他の関連当局に応じて構築されなければならない。

(f)可用性（availability)

組織は、必要とされる情報を、タイムリ、効率的、かつ正確な検索を保証する方法で記録を維持しなければならない。

(g)保持（retention)

組織は、法律、規制、会計、運用上、歴史上の要求を考慮に入れて、適切にその記録及び情報を維持しなければならない。

(h)処分（disposition)

組織は、準拠法及び組織の方針によって最早維持が要求されない記録に安全で適切な処分を供給しなければならない。

(2)GARP に基づく成熟度モデル

前述の GARP を評価基準とした成熟度モデルが“情報ガバナンスに関する成熟度モデル”(ARMA International Maturity Model for Information Governance）である。このモデルでは、表 4-1 に示す 5 段階の成熟度レベルを定義している。

表 4-1　情報ガバナンスに関する成熟度モデルにおける成熟度のレベル

レベル	説明
レベル 1 基準以下	記録が全く管理されていないか限定目的のために管理されている 法規制に合致した対応ができない
レベル 2 開発中	記録が組織に与える影響を認識しているが未だ開発途上にある 法規制に合致した対応に漏れがある
レベル 3 必須	記録管理のために必要な最小限の方針や手順がある 法規制に合致した対応ができる 記録を業務の合理化やコスト削減に活用できていない

レベル	説明
レベル 4 先見行動	事業活動全体にわたる情報ガバナンスプログラムの改良を始めている 定型業務の意思決定と統合化
レベル 5 変革	企業インフラや業務プロセスと全面的に統合化 情報ガバナンスがコスト削減、競争優位、顧客サービスに有効かつ重大な役割を果たすことを認識

表 4-2 は、“情報ガバナンスに関する成熟度モデル”における成熟度レベルの指標(一部)である。評価基準が抽象的な上に指標を列挙してあるだけのため、レベル間の違いが分かり難い。

表 4-2　アカウンタビリティに関する成熟度レベルの指標

レベル	指標
レベル 1 基準以下	記録管理プログラムに責任を負う上級幹部(あるいは匹敵する権威者)がいない。 レコードマネージャの役割は大概存在しないか、あるいは一般職に振り分けられた管理上かつ／または事務的役割である。
レベル 2 開発中	記録管理プログラムに係るあるいは責任を負う取締役(あるいは匹敵する権威者)がいない。 レコードマネージャの役割は認識されているが、既存のプログラムの戦術的なオペレーションに責任を負う。 多くの場合、既存のプログラムは紙記録だけをカバーする。 IT 機能または部門は、デファクト主導で電子情報を格納するが、系統的な方法では行われない。 レコードマネージャは、電子的なシステムの議論に関係しない。
レベル 3 必須	レコードマネージャは組織の役員であり、組織全体に渡って実施中のプログラムの戦術オペレーションに責任を負う。レコードマネージャは、組織の他の役員と共に、戦略的情報・記録管理イニシアチブに活発に従事している。 トップマネジメントはプログラムを認識している。 組織は、アカウンタビリティに関する特定の目標を定義している。
レベル 4 先見行動	レコードマネージャは、プログラムの全戦術・戦略面に責任を負う上級役員である。処分方針及び他の記録管理関連事項をレビュするために、全ての機能的な領域の代表からなるレコードマネージャを座長とするステークホルダ委員会が定期的に開催されている。 記録管理活動は、取締役によって完全に支持されている。
レベル 5 変革	組織のトップマネジメント及びその役員会はプログラムの重要性に大きな重みを置く。 記録管理プログラムは、トップレベルマネジメント(例えばチーフリスクオフィサー、チーフコンプライアンスオフィサー、情報戦略統括オフィサー)の個人々々が直接責任をもつ。 または、組織のトップマネジメントの一員であるチーフレコードオフィサー(あるいは同様の役職)が記録管理プログラムに直接責任を負う。 アカウンタビリティに関して組織が掲げた目標が達成されている。

(3)評価基準の改善提案

eRAP では、前述の問題を解消するために、抽象的な評価基準をより具体的な基準に落としこむべく評価基準の詳細化を試みた。表 4-3 はその結果である。例えば、アカウンタビリティとして一括りであった評価基準を、指標例を分析して、“役割と責任”、“記録戦略”、“目標管理”のように複数の具体的な基準に分解した。これにより、より明快な評価を与えることができるようになる。

表 4-3　組織の情報ガバナンスに関する成熟度レベルの指標

レベル 1 は省略してある

分類	基準	レベル 2	レベル 3	レベル 4	レベル 5
アカウンタビリティ	役割と責任	責任を負う取締役がいないレコードマネージャの役割は認識されている	トップが記録管理プログラムを認識レコードマネージャは役員。組織全体の運用責任を負う	レコードマネージャは上級役員 取締役が完全に支持	トップがプログラムを重視 トップが記録管理プログラムに直接責任をもつ
	記録戦略	多くの場合紙だけをカバー デファクト主導	レコードマネージャが戦略的記録管理を主導	レコードマネージャを座長とする全ステークホルダを対象とした委員会を定期的に開催	
	目標管理		アカウンタビリティの具体的目標を設定している		組織が掲げた目標が達成されている
透明性	組織活動	透明性の重要性を理解 規制が要求する透明性は存在するが系統的かつ全体の運動がない	書面による透明性の方針がある 情報は容易かつ系統的に利用可能		トップマネジメントは透明性を情報ガバナンスの重要要素とみなしている ソフトツールが透明性を助けている
	教育		従業員は透明性の重要性に関し具体的教育を受けている	トレーニングで透明性を強調	
	目標管理		透明性に関し具体的目標を設定している	定期的にコンプライアンスを監視している	組織が掲げた目標が達成されている 連続的な改善プロセスを実施している 利害関係者が透明性に満足
完全性	システム	メタデータ保存が適切かどうかの判断は別部署任せ	システムが要件を満たすことを確認するプロセスを持っている		一貫して記録の正確さを実証できる
	メタデータキャプチャ	メタデータは保存されるが正式プロセスが定義されていない	方針に従ったデータ要素がキャプチャされている	メタデータ要件の明瞭な定義がある セキュリティと署名要件を含む	メタデータキャプチャの定義がされたプロセスがある
	目標管理		完全性に関し具体的目標を設定している		規則的に監査 組織が掲げた目標が達成されている
保護	アクセス制御	書面に書かれた方針はあるが明瞭で決定的なガイドを与えている訳ではない アクセス制御は記録の保持者によって実施されている	機密性、プライバシが定義されている 集中アクセス制御のための書面に書かれた方針をもっている	情報保護を提供するシステムを実装している	トップは情報保護に大きな価値を見出している
	教育	従業員教育は正式化されていない	従業員のトレーニングが可能になっている	従業員教育は正式化され十分文書化されている	

分類	基準	レベル 2	レベル 3	レベル 4	レベル 5
	監査		監査は規制された業務エリアのみ実施される	監査が定期的に行われている	
	目標管理		保護に関し具体的目標を設定している		組織が掲げた目標を達成している 監査情報は定期的に調査され連続的な改良が行われている
コンプライアンス	記録の生成、キャプチャ	法令､規則を特定し、記録管理の慣行を導入している	法令、規定を全て識別している 記録管理原則に従って系統的に行われる	キャプチャし保護するためのシステムを導入 記録はメタデータとリンクしている	
	事業行動	方針は完全ではない、十分に定義されたアカウンタビリティがない	情報ガバナンスと記録管理方針が統合された事業行動規定がある 記録は評価され測定可能となっている		トップが情報の重要性を認識している 情報ガバナンスやコンプライアンス障害の影響を受けない
	プロセス	保持プロセスはあるが、情報管理や開示プロセスと十分統合されていない	保持プロセスは最重要システムの情報管理に統合されている	保持プロセスは反復可能なプロセスによって十分管理されている	
	目標管理		コンプライアンスに関する具体的目標を設定している	従業員は適切にトレーニングされ、監査は定期的に実施 是正措置を通じて改善	監査及び継続的改良プロセスが確立されている 組織が掲げた目標が達成されている
可用性	保存、保持	格納方針はあるが標準が組織横断的に課されている訳ではない	格納、保護、利用基準がある	保存に関する方針が明確に定義されている 実施容易化のための自動化を適用している	
	検索	検索メカニズムが何らかのエリアで実装されている	検索メカニズムが一貫していてタイムリに検索可	記録と情報は一貫して容易に利用可能	
	情報資産の識別、定義	正式、コピー、非記録の識別が可能	最終バージョンが管理されている	情報資産を識別、定義するガイドと棚卸しがある	
	法的開示		法的開示が定義され系統的なプロセスとなっている	法的開示のためのシステムとコントロールがある	
	目標管理		可用性に関する具体的目標を設定している		トップが可用性に影響するプロセスの改良を支援 組織化されたトレーニングと継続的改良プログラムがある 組織が掲げた目標を達成している 測定可能な ROI がある

分類	基準	レベル 2	レベル 3	レベル 4	レベル 5
保持	保持計画	保持計画の利用が部分的あるいは知られていない	保持計画が組織全体に一貫して適用されている	記録保持は主要な関心事である保持計画は定期的にレビュされニーズに沿って調整される	保持はトップマネジメントと役員会の重要案件正式記録だけでなく全ての情報に保持を適用、適切な期間一貫して保持される
	保持	保持方針に関する教育・トレーニングを利用不可	従業員は記録保持の直接責任を理解	従業員は記録を適切に分類する方法を理解	
	目標管理		保持の具体的目標を設定している		組織が掲げた目標が達成されている
処分	処分手続き	初歩的ガイドラインは確立	処分、移管のための正式手続きがある	組織横断的に一貫して適用 方針に従って電子情報を削除ではなく抹消	技術によって支援されている
	処分保留	処分保留の重要性が認識されている	処分保留の方針、手続きがあるが部門ごとに代替手段をもつ	法的保持に伴う処分保留プロセスは組織横断的	
	目標管理		処分の具体的目標を設定している		定期的に評価され改善されている 組織が掲げた目標を達成している

4.1.2 ISO 15489 をベースとした成熟度モデル HB-278

HB-278 (Recordkeeping Compliance) は、ISO 15489 (記録管理)[4] への準拠性の評価モデルであり、組織における記録プロセスの評価やベンチマークを目的としている。

(1) 評価レベルと評価基準

HB-278 で定義されている 5 段階の評価レベルを表 4-4 に示す。

表 4-4 HB-278 の評価レベル

レベル	説明
レベル 1：その場しのぎ(AdHoc)	系統的アプローチが存在しない
レベル 2：定義された(Defined)	プロセスと慣習は様々に定義されているが一貫性がない
レベル 3：反復可能(Repeatable)	プロセスと慣習は文書化され組織横的理解されている
レベル 4：管理された Managed)	日常的に計測され積極的な管理が行われている
レベル 5：最適化(Optimal)	革新とモニタリングとレビュに基づく学習を通して継続的に改善している

表 4-5 は HB-278 で定義されている評価基準である。

表 4-5　HB-278 の評価基準

根拠：ISO15489-1 の該当箇所
区分：O　組織、S　システム

分類	基準	根拠	区分	説明
組織的管理フレームワーク	影響要因特定	8.4(a)	O	組織は、事業環境を分析し記録を作成し保存するニーズに影響を与える要因を特定している。
	記録管理プログラム	7.1	O	必要な期間、真正で、信頼でき、使用可能な記録が作成され、キャプチャされ、保持され、保護されることを保証する包括的な記録管理プログラムが存在する。
	記録戦略	8.4(e), (f)	O	組織の業務内容やリスク露呈に対する適切な記録戦略が策定されている。
	構造化プロセス	8.4	O	記録を管理し、組織の業務ニーズ及びコンプライアンス要件に対して適切な持続可能システムを設計し実装するために構造化されたプロセスが使用されている。
	文書化	9.1	O	組織はその記録管理プロセス、及びシステム(生成、記録のキャプチャ、分類及び処分の決定を含む)を文書化している。
	ポリシと手順	5, 6, 1, 6.2	O	組織の業務ニーズ及び規制環境に対する適切な記録管理ポリシ、手続き及び慣行が確立され、文書化され、維持され、広く促進されている。
	役割・責任の定義とアサイン	6.3	O	記録管理に対する責任と権限が組織全体にわたって定義され、割り当てられ、広く促進されている。
	トレーニングプログラム	11	O	スタッフ、契約者及びボランティアのためのトレーニングプログラムが確立されている。
	継続的モニタリングとレビュ	8.4, 10	O&S	記録を維持するシステムの実行(ポリシ、手続き、インフラストラクチャー及びユーザ)は、実行とユーザ満足度を評価し、是正処置を講じて、不備に取り組み、記録プログラムを改善する機会を識別する、連続監視及び定期的なレビュ対象となっている。
作成	業務とプロセスの定義	8.4(b)	O	企業活動とプロセスが識別されている。また、それらの関係が文書化されている。
	証拠作成・維持要件の評価	5, 7.1, 8.4(c), 9.1	O&S	組織の事業活動(及びそれらを支援するプロセス)の証拠を作成・維持する必要条件が評価されている。
	記録管理システムの評価	8.4(d)	S	既存の記録管理システム及び他の情報システムは、組織の記録要件を満たす能力が評価されている。
	適切な記録の作成	9.1	O	業務を行うためのプロセスに関係なく適切な記録が作成されている。
キャプチャ及び管理	記録形式、構造、技術の規定	7.1(b)	O	組織のポリシ及び業務規定は、記録を作成しキャプチャするための形式及び構造並びに使用される技術を規定している。
	記録管理システムの事業支援	8.2.5	S	記録管理システムは組織の事業活動を全て支援している。
	業務プロセスとの統合	8.4(g)	S	記録フレームワークは計画された方法で業務プロセスや関連するシステムに統合されている。
	定義された手順による運用	8.2.2	S	記録管理システムは、定義された基準と手続きによって定期的かつ継続的に運用される。
	完全性保護コントロール	8.2.3	S	記録管理システムは、記録の完全性を保護するコントロール(アクセスモニタリング、ユーザ検証、認可された破壊、セキュリティのような)を含んでいる。
	系統的キャプチャ	8.2.6	S	記録のキャプチャが、文書化されたポリシ、手続き及び責任に従って系統的に行われる。
	管理システムへのキャプチャ	9.3	S	記録は、記録管理用に設計されたシステム(複数可)にキャプチャされる。

分類	基準	根拠	区分	説明
	メタデータ生成・キャプチャ	9.3	S	記録管理システムは、記録に関するメタデータを生成しキャプチャする過程を含んでいる。
	記録の登録プロセス	9.4	S	記録管理システムは、オブジェクトまたはオブジェクトグループとして記録を管理できるように、キャプチャ時点で記録に関するユニーク識別子及び記述的情報を割り付ける登録プロセスを含んでいる。
	メタデータツールの利用	9.5	S	業務分類システム、インデックス付け、番号付けといったメタデータツールが時を越えて記録を特定し管理するために使用されている。
	個人記録の利用・管理履歴	8.3.2	S	記録管理システムは、個人記録の使用及び管理履歴を文書化している。
	記録に含まれるメタデータ	7.2.1	S	記録は、それらの構造、業務の脈絡(コンテキスト)、他の記録との関係、使用及び管理履歴について記述したメタデータを含んでいるか、または連続的にリンクされている。
	真正性	7.2.2	S	記録は真正である。
	信頼性	7.2.3	S	記録は信頼できる。
	完全性	7.2.4	S	記録はそれらの完全性を保護するために安全かつ着実な環境の中で保存されている。
	利用可能性	7.2.5	S	記録は使用可能である。
検索	メタデータツールの利用			記録を、時を越えて識別し管理するためにメタデータツールとプロセスが使用されている。
	記録を取得する方法の理解			記録管理システムのユーザは、記録を得る方法を理解している。
	記録の分散管理	8.3.4	S	組織のシステムは必要に応じて記録の分散管理を支援している。
アクセス	アクセス権定義	8.3.6	O&S	アクセス権が定義され、記録の完全性及び適切な使用を確保するためのシステム制御がある。
	移動・利用の継続的追跡	9.8	S	記録の移動及び使用を継続的に追跡している。
	タイムリで効率的アクセス	8.3.6, 9.7	S	記録を維持する組織のシステムは、適切で、適時かつ効率的な記録へのアクセスを提供している。
ストレージ及び保存	設計時の考慮	8.3.3	S	メディア、ストレージ及び取扱い条件はシステム設計過程で考慮されている。
	要求を満たすシステムの使用	9.6	S	組織は、必要な期間、記録の真正性、信頼性及びアクセス可能性を維持するシステムを使用している。
	要求に合致したストレージ	9.6	S	ストレージ条件及び取扱いプロセスは組織の記録ニーズに合致している。
	要求に合致したメディア	9.6	S	記録は、必要な期間、アクセス可能性と完全性を保存するメディア上に格納される。
	コピー・変換・移行戦略の実装	8.3.5	O	記録(及び関連するメタデータ)のコピー、変換及び移行戦略を実施しモニタしている。
	災害時管理を含む設計	8.3.3	S	システム設計と実装のプロセスは災害管理戦略を含んでいる。
処分	記録の保持期間の判断	9.2	O	記録の保持期間の判断は、規制、業務、説明責任の必要に応じて行われる。
	日常的な処分の支援	8.3.7	S	日常的に生じる処分は、記録を保持するあらゆるシステムの仕組みで支援される。
	記録破壊の非適用	8.3.7	S	現在の業務にまだ必要な記録に対して破棄は行われない。

分類	基準	根拠	区分	説明
	システムの停止管理	8.5	S	記録を管理するあらゆるシステムの更改が管理されている。
	処分判断の定期的レビュ	9.2	O	処分判断は定期的にレビュされる。
	処分判断のオーソライズ	9.2	O&S	破棄を含む処分判断が承認されている。
	処分判断と処置の監査証跡	8.3.7, 9.2	S	システムは、処分判断と処置の監査証跡を維持している。
	記録の破壊方法	9.9	S	記録の破棄は適切かつ徹底的に行われる。

(2)HB-278 の評価指標

表 4-6 に評価指標の例を示す。HB-278 では、評価基準毎かつ各レベル毎に 5 つないし 7 つのモデル指標が提示されているが、ここでは代表的なもののみを掲載する。

表 4-6　HB-278 のモデル評価指標

分類	基準	レベル 2	レベル 3	レベル 4	レベル 5
組織的管理フレームワーク	影響要因特定		記録管理 PJ 立案、実現性検討	現状の SWOT 分析	SWOT／リスク分析の定期的見直し
	記録管理プログラム	ポリシに基づいてプログラムを文書化	包括的なプログラムを文書化	セキュアで一貫性のあるアクセス管理	
	記録戦略	戦略レポート	潜在的戦略リスト	リスク評価、定期的法務評価	新規業務に必要な記録の評価
	構造化プロセス		構造化プロセスによる設計・実装		
	文書化	未承認管理行為の防止規定	法的、組織的、技術的要件の考慮	適切さの定期的なレビュ	
	ポリシと手順	基本的な管理手順の公式声明	CEO によるポリシの承認、促進	ポリシ・手順の遵守評価プロセス設定	
	役割・責任の定義とアサイン	責任と権限はポリシから導出	業務手順を反映	経営陣が承認し定期的にレビュ	
	トレーニングプログラム	スタッフに求められる原則を実施	定期的トレーニング	標準化されたトレーニングとモニタ	職務記述書に責任を明示した人材育成
	継続的モニタリングとレビュ	運用に対するフィードバックの文化	記録管理運用の計測、報告	基準の標準化、定期的な実行モニタ	BPR
作成	業務とプロセスの定義	記録が必要な機能・活動を文書化	機能・活動・取引を示す業務分類体系	業務プロセス上の文書作成・受領点マップの提供	
	証拠作成・維持要件の評価	全社的ポリシ記述	該当する規制の文書化	証拠に対するリスク評価と最新化	監査、リスク評価、統合的レビュ
	記録管理システムの評価	システムの棚卸	問題発生時の文書化されたレビュ	再分析による目標管理	要件組み込みの自動化設計
	適切な記録の作成		業務通信(電話、会議)の手順化		
キャプチャ及び管理	記録形式、構造、技術の規定	異なる書式利用の得失評価	組織横断的な書式・構成の文書化		

分類	基準	レベル 2	レベル 3	レベル 4	レベル 5
	記録管理システムの事業支援	全社的ポリシへの記載	該当する規制のリスト化	スタッフコンサル、関係者の期待を考慮	進行中の統合的レビュ
	業務プロセスとの統合	実施プロセスを経営者に報告	承認された PJ 計画	定義された PJ 管理	業務改善に伴う実装の変更
	定義された手順による運用	スタッフに求められる原則を実施	システム利用法のトレーニング	例外処理の文書化、モニタリング	最適化されたモニタリング
	完全性保護コントロール	スタッフに求められる原則を実施	不適切利用の制限	首尾一貫した破棄承認アプリ	最適化されたモニタリング
	系統的キャプチャ	スタッフに求められる原則を実施	多様なフォーマットをキャプチャ	システム本項の文書化、自動化	
	管理システムへのキャプチャ	スタッフに求められる原則を実施	業務の一環としてキャプチャ文書定義	監査	
	メタデータ生成・キャプチャ	メタデータキャプチャの推進	メタデータキャプチャの設計文書化	メタデータキャプチャの定期的包括的評価	業務要件変更に伴う手順見直し
	記録の登録プロセス		OBJ 登録と ID による検索		
	メタデータツールの利用	タイトル、インデックスのガイダンス	文書化された分類体系、業務分析	システムへの分類体系の組み込み	
	個人記録の利用・管理履歴	監査ログ	トランザクションの処理結果を文書化	トランザクションの監査ログ／メタデータ	定期的レビュと評価
	記録に含まれるメタデータ	スタッフに求められる原則を実施	システム設計にメタデータ要件を含む	メタデータキャプチャの定期的評価	業務要件変更に伴う手順見直し
	真正性	スタッフに求められる原則を実施	スタッフに対するトレーニング	未承認変更削除防止システム	外部環境脅威評価
	信頼性	スタッフに求められる原則を実施	会議等の記録の必要性認識	記録の業務規程化、メタデータ自動化	信頼性の定期的評価
	完全性	スタッフに求められる原則を実施	完全性を保持する設計ポリシ	管理ツール	完全性に関する定期的評価
	利用可能性	スタッフに求められる原則を実施	内容／検索用メタデータ適用	定義された移行体制	利用者ニーズの定期的評価
検索	メタデータツールの利用	“記録の登録プロセス”、“メタデータツールの利用”、“個人記録の利用・管理履歴”参照			
	記録を取得する方法の理解	“トレーニングプログラム”、“アクセス権定義”参照			
	記録の分散管理	全記録のロケーション知識	分散管理下での識別	ストレージプロバイダとの標準契約	サービスプロバイダの定期的評価
アクセス	アクセス権定義	文書化されたアクセス要求／制限	文書化と経営者による承認	経営者への監査報告	
	移動・利用の継続的追跡	保管場所及び移動先の登録	気付きを与える教育プログラム	定期的監査	定期的モニタ
	タイムリで効率的アクセス	“完全性保護コントロール”、“メタデータツールの利用”、“要求を満たすシステムの使用”参照			
ストレージ及び保存	設計時の考慮	“要求を満たすシステムの使用”、“要求に合致したストレージ”、“要求に合致したメディア”参照			

分類	基準	レベル 2	レベル 3	レベル 4	レベル 5
	要求を満たすシステムの使用	セキュリティ制御	効率的検索	制御され文書化された移行	
	要求に合致したストレージ		経営者が承認した適切なストレージ	契約に基づく外部ストレージへの転送	
	要求に合致したメディア	変換／移行の定義と実施	メディア選択の正当化文書	変換／移行戦略	
	コピー・変換・移行戦略の実装		技術依存	責任者指名	長期保存記録の特定、変換、移行
	災害時管理を含む設計		潜在的災害のリスク評価	承認されたシステムの災害管理計画	
処分	記録の保持期間の判断	未承認処分を防止する基本的規定	公式に承認された処分権限者	法的、業務的なモニタ、リスク評価	関係者によるコンサルテーション
	日常的な処分の支援	承認された処分規定	システムの処分判断とのリンク	スタッフの判定に関するポリシと手順	生成時の判定
	記録破壊の非適用		時機を得た記録処分の承認プロセス	指名スタッフによる破棄許可	
	システムの停止管理	記録維持を考慮した更改	システム更改に伴う破棄実施	移行を支援するポリシ、手順	システム更改管理の監査
	処分判断の定期的レビュ	“記録の保持期間の判断”参照			
	処分判断のオーソライズ		適切な内部承認の取得	指名スタッフによる特定記録の破棄承認	
	処分判断と処置の監査証跡	破棄活動の文書化	監査ログ保持	処分データ維持ポリシ(メタを残す等)	処分データのアクセス可能性評価
	記録の破壊方法	メディア対応の適切な破棄方法／プロセス	破棄証明書	助言を含む処分承認文書	

4.1.3 成熟度評価にあたっての留意点

組織における記録管理の成熟度を評価する入手可能なツールとして、The Principles Assessment[5] がある。ここでは、このツールを題材に、組織における記録管理の成熟度を評価する場合の留意点を述べる。

(1) ツールの概要

The Principles Assessment は、Web ベースの評価ツールであり、評価者ごとにメールで通知される URL をクリックすると評価用画面に移る。各評価者がおのおの全部で 100 問の質問に答えると、集計されスコアが表示される。

以下の表に、質問の概要を示す。

表 4-7　質問の概要

類 分	調査項目
アカウンタビリティ	・記録と情報ガバナンスプログラムに対する上級幹部の役割は？ ・情報ガバナンス運営委員会構成と権限は？ ・情報ガバナンスプログラムは組織横断的か？ ・部門が情報ガバナンスプログラムの責任をもっているか？ ・記録と情報管理に関する責任者の権限と要求される知識は？ ・記録及び情報管理者は記録と情報ガバナンス戦略方針策定にどう係わっているか？ ・情報ガバナンスと RIM 原則が戦略的意思決定にどう考慮されているか？ ・記録や情報ガバナンス方針と一致する文書化された IT 戦略があるか？ ・IT 戦略の作成にどう関与しているか？ ・情報ガバナンスプログラムは紙、電子、メールも管理対象か？ ・電子情報管理に関する意思決定は誰がどのように行うのか？ ・新技術導入はどの様に決めるのか？方針、手続きは？ ・記録と情報ガバナンスプログラムの説明責任の目標は？それはどれだけ達成されているか？ ・記録と情報ガバナンスプログラムに関して上級幹部との間でどのような報告／指示があるか？ ・文書化されたコンプライアンスアセスメントがあるか？
透明性	・上級幹部は透明性のある記録と情報のプロセスとガバナンスプログラムを理解しているか？ ・上級幹部は透明性のある記録と情報のプロセスとガバナンスプログラムの理念をコミットしているか？ ・透明性の目標が十分定義され明文化されているか？ ・従業員は適切な情報取扱いの為に、明文化されたポリシ、手順、その他情報に直ちにアクセス可能か？ ・一貫したアウトプットを生み出し、誤りを防ぐために、記録及び情報プロセスは標準化されているか？ ・文書化された役割と責任の割当てがあるか？従業員はそれを理解してプロセスを実施しているか？ ・監査と改善を含む、記録と情報ガバナンスプロセスの品質検査／管理の仕組みをもっているか？ ・情報の作成とガバナンスプログラムはエラートラップ機能や監査証跡をもっているか？
完全性	・オリジナル記録を文書化するための企業横断的なポリシはあるか？ ・記録の完全性のためのガバナンスに関する幹部の役割は何か？ ・そのコミュニケーションレベルは？ ・従業員とのコミュニケーションの重要性は？ ・記録と情報の安全性の目標は？ ・情報管理者は、情報ガバナンス戦略にどう関与しているか？ ・組織の記録と情報の完全性目標と IT 戦略に矛盾はないか？どう解決しているか？ ・新たに導入したシステムのための過程管理と真正性を定義する公式プロセスはあるか？ ・評価やディスカバリ要求時に記録の真正性を簡単に確認できるか？ ・システム、記録、管理人を識別するためにマップを利用しているか？ ・完全性の観点からどの様に記録のメタデータを定義しキャプチャし保存しているのか？ ・記録とメタデータが改竄されていないことをどの様に確認しているか？ ・完全性のための監査プロセスをもっているか？
保護	・上級幹部は情報保護プログラムの重要性を文書化し支援しているか？ ・情報保護プログラムに関してどのような指示／報告が行われているか？ ・組織の情報セキュリティ及び保護戦略に記録及び情報管理者は関与しているか？ ・組織横断的な情報セキュリティと保護ポリシは十分包括的か？ ・情報資産を識別するリスクベースモデルに従っているか？ ・情報保護のための文書化された目標をどう満たしているか？ ・リスクの高いビジネスプロセスを監視、修正するコントロールをもっているか？ ・インシデントの監視と報告のプロセスはあるか？ ・機密、特権などの情報をどの様に識別し分類しているか？ ・セキュリティ要件を強制する代わりに適切な方法論、物理的保護、技術を使用しているか？ ・機密、特権、秘密情報の転送の方法は？ ・従業員の移転、退職時に機密を守るプロセスは？ ・戦略パートナ、関連会社、ベンダとの間の情報保護手段は？ ・国境を越えた事業の情報保護手段は？ ・個人、機密、特権情報のリポジトリを識別するデータマップをもっているか？ ・完全にテストされた災害復旧計画をもっているか？ ・リスクアセスメントを実施しているか？

類 分	調査項目
	・機密あるいは個人情報漏洩の頻度は？ ・従業員、パートナなどへの定期研修で方針、手順、ツールを提供しているか？
コンプライアンス	・関連法令や規制を識別し文書化しているか？ ・上級幹部がコンプライアンス義務を認識し価値を認め、遵守にどの様なインセンティブ用意しているか？ ・従業員の行動規範を含む記録と情報ガバナンスに関するコンプライアンスポリシがあるか？ ・コンプライアンス違反を報告する公式な仕組みはあるか？ ・文書化されたコンプライアンス目標があるか？ ・スタッフにコンプライアンス意識向上のためのトレーニングプログラムを提供しているか？ ・個人情報保護のための外部委託のポリシが規定されているか？ ・委託先でのコンプライアンスポリシ遵守をどの様に確認しているか？ ・訴訟ホールド／e ディスカバリ遵守にどう対応しているか？ ・コンプライアンス測定基準と継続的改善プロセスはあるか？ ・監査でのコンプライアンス評価結果はどの様に文書化されフィードバックされるのか？ ・失敗を文書化することができるか？
可用性	・組織の記録や情報を戦略的資源として参照しているか？ ・記録及び情報管理者の役割と、特に“file to retrieve”のトレーニングと推進の責任は？ ・記録と情報の可用性に関し定義されたポリシ、手順、目標はあるか？ ・記録と情報の分類方針・基準はあるか？ ・従業員に情報作成と適切な格納の世紀人に関してどのようなガイドを提供して文化を醸成しているか？ ・記録や情報検索メカニズムは？ ・真正な記録の最終バージョンは簡単に見つけられるか？ ・法的開示や類似の規制情報の要求に効果的に対応可能か？ ・アクセス制限のために記録がどの様に編成されているか？ ・メタデータがどの様にキャプチャされ保存されるのか？ ・災害復旧手順が整っているか？ ・冗長性を抑止する組織としてのプロセスはあるか？ ・情報利用の指針は何か？
保持	・記録の保有計画の責任者は幹部か？ ・メールや音声記録などは保有計画の対象になっているか？ ・組織内の記録の保有計画やプロセスの責任者は誰か？ ・業務要件に基づき保有計画が決定されているか？ ・組織横断的な保有計画か？ ・法規制の変更をどの様に保有計画に反映させるのか？ ・保有計画変更の開始、承認、組織内伝達方法は？ ・保有計画の目標を定めているか？ ・保有ポリシとプロセスを遵守する新技術の取得プロセスはあるか？ ・どこに何が保存されているかのデータマップが維持されているか？ ・技術移行において、情報、メタデータ、見読性保護のためにどの様な適切なコントロールが行われるのか？ ・法的ホールドプロセスは自動化されているか？ ・監査結果が保有計画にどのように活かされるのか？
処分	・組織はどの様に処分を定義しているか？ ・どの様な情報に処分方針が適用されるか？ ・幹部は処分方針とプロセスにどう関与しているか？ ・処分プロセス(特に保留)を管理しているか？ ・処分プログラムの目標と実績は？ ・処分プログラムは文書化されているか？ ・どの様に処分プロセスが開始されるか？ ・破壊処分のための承認プロセスをもっているか？ ・所有権移転のためのプロセスをもっているか？ ・一貫性のある処分プロセスとその追跡をどうコントロールしているか？ ・ハードウェア、ソフトウェア廃棄の手順はあるか？ ・アーカイブの手順は？ ・文書化された訴訟保留と解除プロセスはあるか？

出典：The Principles Assessment の質問内容を要約

以下は、質問と回答の選択肢の一例である。

質問　記録と情報ガバナンスのプログラムは、コンプライアンスを確保し、リスクを最小限にし、コアビジネス機能の向上に寄与するために組織全体でどのように包括的ですか？

回答の選択肢

・記録も情報ガバナンスプログラムも存在しません。
・ガバナンスプログラムは部門単位、またはその実装が最小または非公式です。焦点は主にコンプライアンス／監査法人です。
・組織は適切な場所で企業全体の記録と情報ガバナンスプログラムを持っています。プログラムの実装は完全でない場合や一貫していない場合があるが、ギャップに対処するために努力が行われている。

(以下省略)

スコアは、図 4-2 のように、アカウンタビリティ、透明性などの 8 つの評価基準毎に 5 段階で少数第 1 位まで表示される(例えば、2.7)と共に、全体の平均スコアとベースラインスコアが表示される。また、各評価基準毎にスコアアップの対策が表示される。

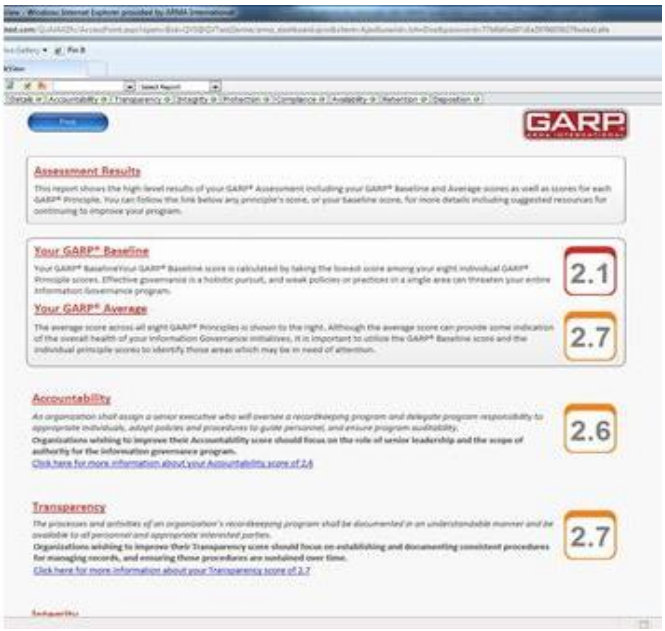


図 4-2　成熟度評価のスコア表示の例

(2) 評価時の留意点

組織の記録管理の成熟度を評価するにあたっては、次の点に留意する必要がある。

①評価ツールはいわゆるレコードマネージャの存在を前提に提供されている。可能であれば、記録管理の専門知識を有する者の支援を受けることが望ましい。

②国内では、全社横断的な記録管理が行われている企業は皆無であり、全社レベルの記録管理に精通している者もいない現状では、部門単位の評価から始めることが現実的である。

③評価ツールを使う準備段階として、より客観的な評価を引き出すためにその部門の記録管理の現状を可能な限り把握しておく必要がある。表 4-7 に事前調査項目を例示する。

4.2　記録管理のモデル

記録管理にはさまざまなモデルがある。ここでは、体系的あるいは構造的(アーキテクチャ的)な観点から主要なモデルを紹介する。

(1) 全体の体系

文書(Document)の管理と証拠としての記録(Record)、歴史的に重要な記録としてのアーカイブは、表 4-8 に示すようにその目的、管理者、取扱いが異なる。

表 4-8　文書、記録、アーカイブの違い

	文　書	記　録	アーカイブ
目的	業務遂行手段	決定や行為の重要な証拠	歴史的に重要な記録
管理者	所有者(作者)	組織	指定組織
変更の可否	自由に変更が可能	変更は不可	変更は不可
削除の可否	自由に削除が可能	通常は削除不可	通常は削除不可

従って、一般論として、文書の管理、記録の管理、及びアーカイブは、明確に分けて管理することが望ましい。諸外国の事例を見ると、多くの場合、図 4-3 のように体系付けられている。いわゆる、伝統的な体系である。文書を記録管理システムに取り込むことを“キャプチャ(capture)”というが、このタイミングは、年一回定期的に取り込んだり、あるいは決裁時に取り込むなど様々である。

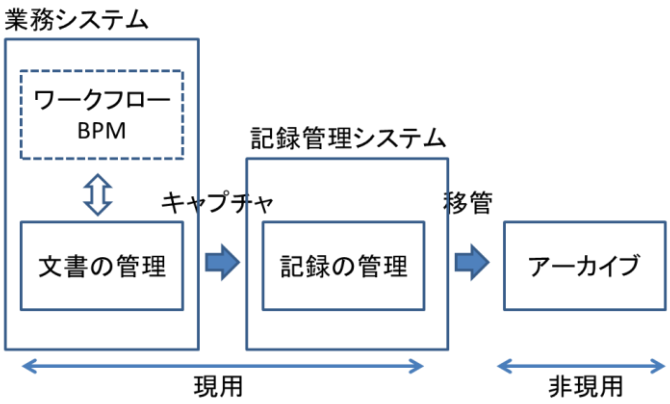


図 4-3　文書及び記録に関する全体の体系

DLM Forum[6] の MoReq 統治委員会[5] の調査では、最近、発生場所で記録を管理する非伝統的な体系が拡大しつつある。図 4-4 に示すように、対象となる記録を記録管理システムに移動

またはコピーすることなく、その記録が発生した業務システムの中で管理する。対象となる記録の蓄積機能なしの記録管理システムであり、メタデータだけを管理する。

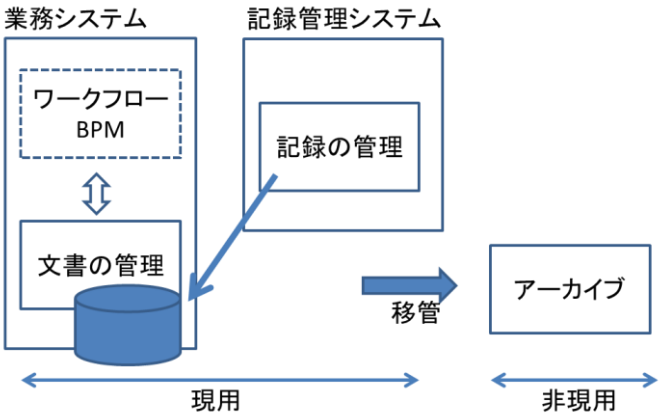
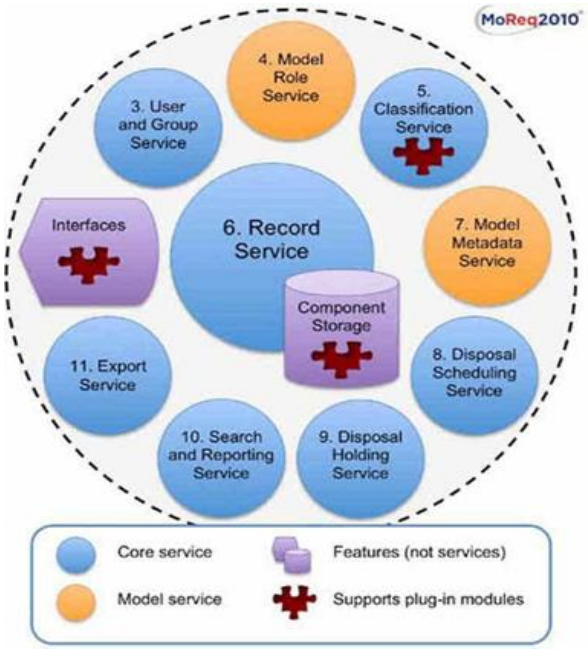


図 4-4　蓄積機能をもたない記録管理システム

この背景となっているのが、記録管理システムのアーキテクチャの進展である。図 4-5 は MoReq2010 で採用されているアーキテクチャである。図における 6. Record Service 以外は他のシステムとシェア可能となっている。



出典：MoReq2010

図 4-5　MoReq2010 における記録管理システムのアーキテクチャ

MoReq 統治委員会[5] は、更に、図 4-6 のような業務システム自身の中に記録管理システムを内包するアプローチの可能性を示唆している。個々の業務システムによって獲得あるいは発生した特定の記録を管理するだけであるが、実質的には同時に記録管理システムとなっている。

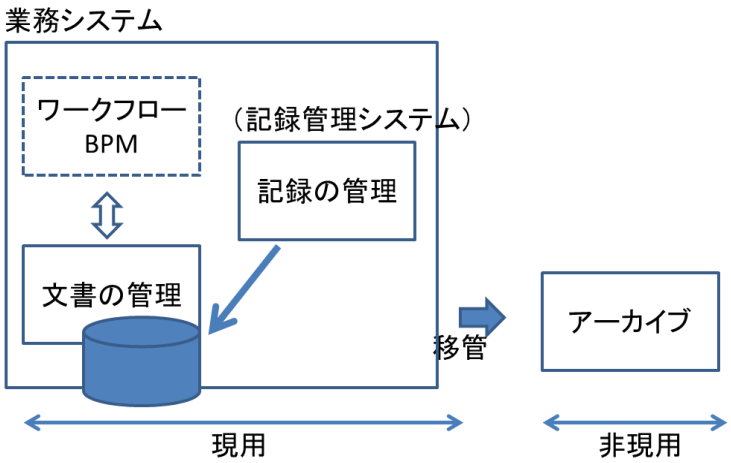


図 4-6　業務システムの中に埋め込まれた記録管理システム

(2) 記録のライフサイクル管理

記録管理標準として、ISO 15489-1(JIS X 0902-1) が世界各国で幅広く参照されている。この標準は、図 4-7 に模式化したように文書のキャプチャから廃棄・移管までのライフサイクル管理に視点が置かれている。

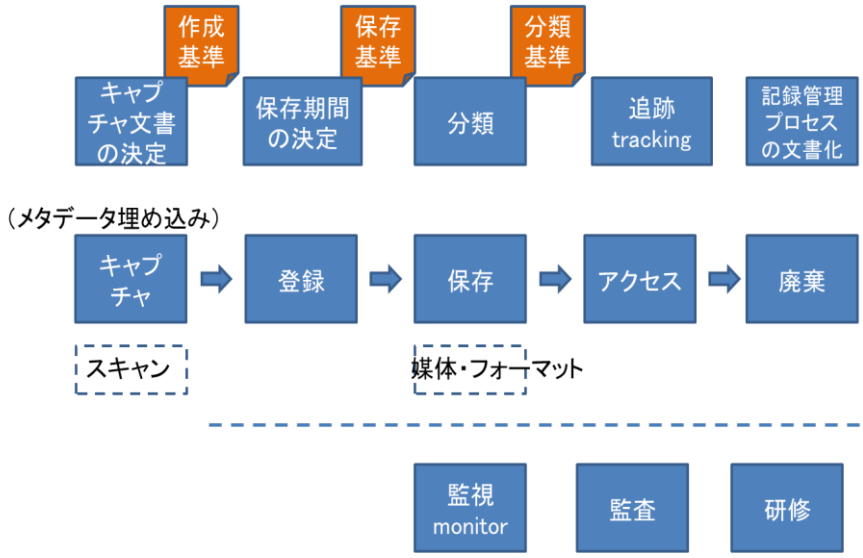


図 4-7　記録のライフサイクル管理

(3) 記録管理システム

記録管理システムやアーカイブシステムのモデルとしては、図 4-8 に示す ISO 14721(OAIS 参照モデル)[7] が世界各国で幅広く参照されている。例えば、韓国の公認電子文書保管所、米国の国立公文書館記録管理庁(NARA) のシステムなどが挙げられる。

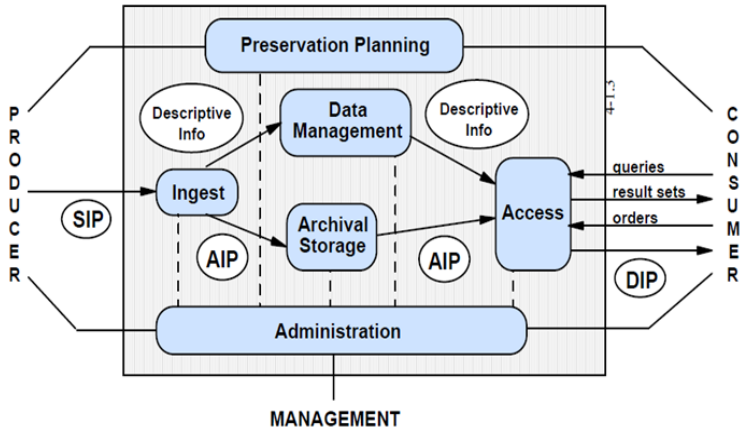


Figure 4-1: OAIS Functional Entities

Submission Information Package (SIP)
Archival Information Package (AIP)
Dissemination Information Package (DIP)

図 4-8　OAIS 参照モデル

図 4-9 は OAIS 参照モデルで用いられている情報パッケージ構造である。

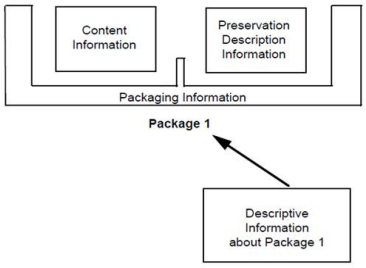


Figure 2-3: Information Package Concepts and Relationships

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

図 4-9　OAIS のパッケージモデル

(4) メタデータ

メタデータに関しては、ISO 23081-1 及び-2(記録のメタデータ)[8][9] が広く参照されている。

図 4-10 は、ISO 23081-1 のなかで述べられている、業務、人、記録の関係である。業務(タスク)定義の一環で作成や取得すべき記録が定義され、人がアサインされ、記録が作成、保存される関係を示している。

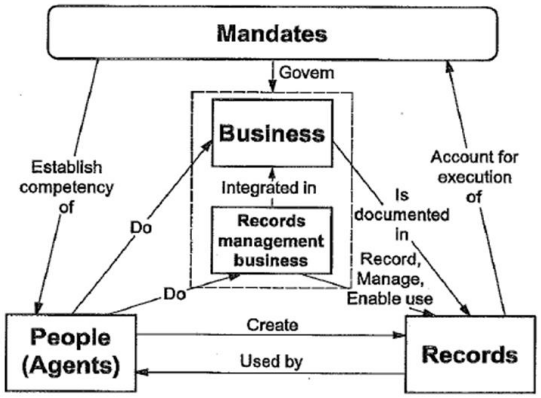


図 4-10　業務、人、記録の関係

図 4-11 はメタデータの汎用モデルである。メタデータにはその対象物のアイデンティティ、説明、計画、履歴、使用、他の対象との関係に関するメタデータがあることを示している。

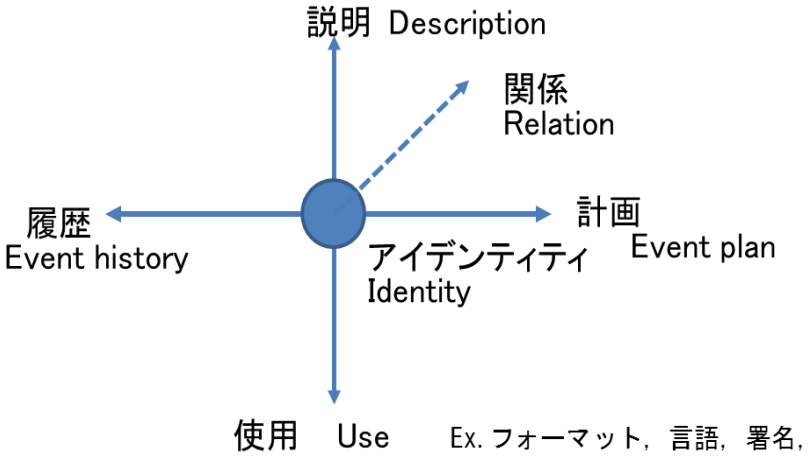


図 4-11　メタデータのモデル

図 4-12 はこのモデルをファイルと記録に適用した例である。図中、メタデータは、

ID　メタデータの名称　メタデータの値

で示されている。

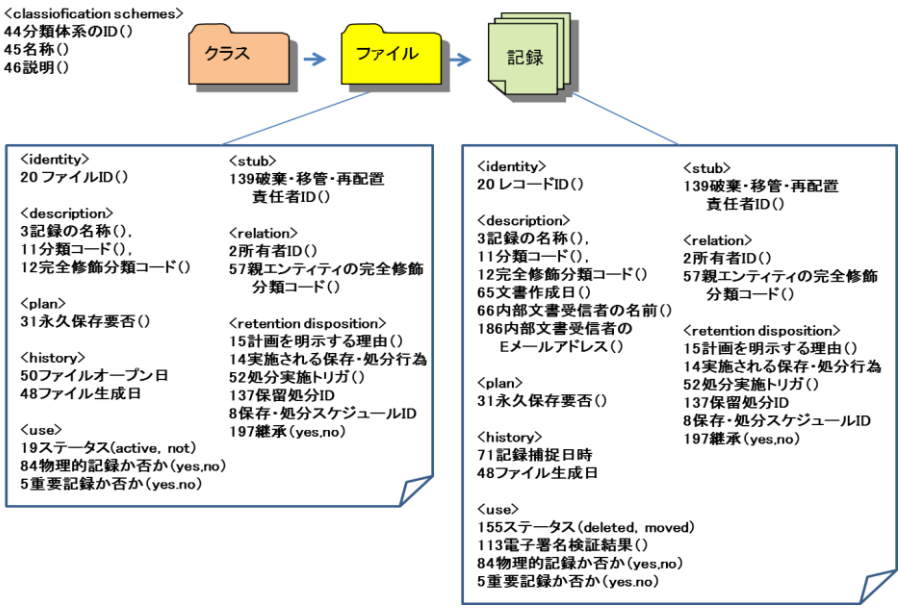


図 4-12　メタデータ例(MoReq2)

4.3　eRAP が提案する記録管理モデル

eRAP が提案する記録管理モデルを図 4-13 に示す。特徴は次の通りである。

・ケースと文書をパッケージの形でキャプチャする(取り込む)
・ケースと文書をパッケージの形で移管する
・業務分類のスナップショットも記録としてキャプチャする

なお、業務分類の管理とどのように連携するかは今後の課題である。

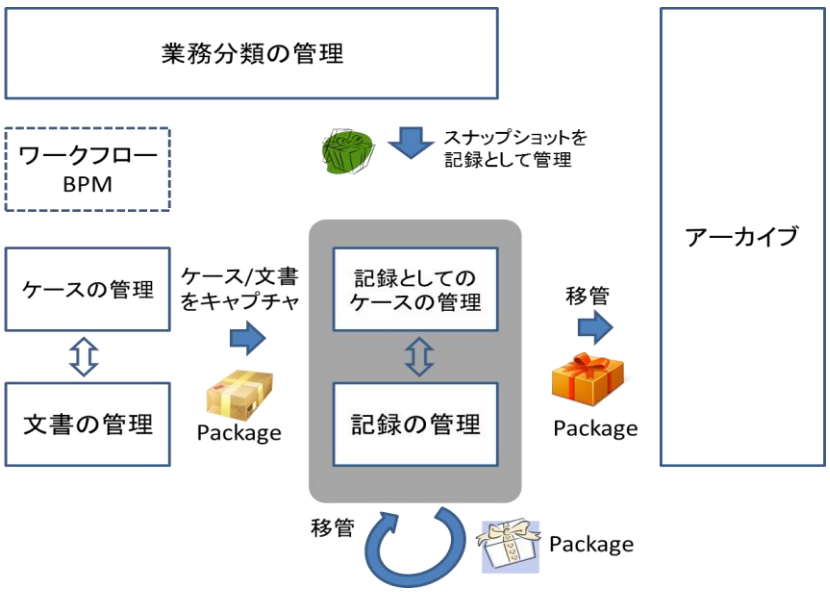


図 4-13　eRAP が提案する記録管理モデル

参考文献

[1] GARP (The Generally Accepted Recordkeeping Principles).
http://www.arma.org/garp/index.cfm

[2] ARMA International Maturity Model for Information Governance.
http://www.arma.org/garp/metrics.cfm

[3] HB-278:2009　Recordkeeping Compliance.　http://trove.nla.gov.au/version/38670495

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

[5] The Principles Assessment.　http://www.arma.org/garp/Assessment.cfm

[6] DLM Forum.
http://www.dlmforum.eu/index.php?option=com_content&view=article&id=17&Itemid=22&lang=en

[7] OAIS 参照モデル.
ISO 14721:2012 Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model

[8] ISO 23081-1:200.　Information and documentation -- Records management processes -- Metadata for records -- Part 1: Principles

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

第2部　IT共通基盤

まえがき

電子記録応用基盤フォーラム(以下“eRAP”とする)及びその前身である電子商取引推進協議会・次世代電子商取引推進協議会(以下“ECOM”とする)では、2000 年度より 13 年にわたって電子署名・認証に関わる活動に取り組んできた。特に電子署名に関しては各種関連ガイドラインの策定及び業界に向けた提案、海外との協力による相互運用性テストの実施、国内及び国際での長期署名プロファイルの標準化など、先駆的テーマを率先して手がけ、数多くの実績を残してきた。

これまでの活動の集大成というには充分とは言えない内容となってしまったが、関連活動の最終報告という意味も加味して、第 2 部では技術検討 WG における 2012 年度の関連活動成果を報告することに加え、これまでの 13 年にわたる成果を振り返り、まだ少なからず残る重要な課題について紹介することとしたい。

第 2 部の各章・節の内容は次の通りである。

第 1 章「電子署名の新しい可能性」では、ECOM 及び eRAP におけるこれまでの電子署名関連の成果、電子署名市場の現状認識、クラウドやモバイル環境といった新たな環境、または組込システムや制御系システムといった従来は電子署名とは無縁であった環境における可能性について述べ、最後にこれらの環境を想定したときに今後検討すべき課題をまとめる。

第 2 章「本人認証／属性認証についての考察」では、電子記録管理システムにおけるアクセスコントロールへの適用を目的とした ID 管理や属性管理のあり方について考察した結果と今後取組むべき課題を述べる。

第 3 章「署名・認証標準化動向」では、3.1 から 3.4 までの 4 つの節において電子署名の最新の標準化動向について述べる。

3.1 節「標準化活動報告」では、2012 年 9 月に ISO として発行するに至った長期署名(CAdES/XAdES)プロファイルにつき、標準化の経緯、JIS や ETSI プロファイルとの関係、最新の標準化動向を踏まえた検討課題について述べる。特に新出のため未着手であった PAdES プロファイルの標準化の必要性について説明する。

3.2 節「XAdES のプラグテスト」では、2012 年 3 月から 4 月にかけて欧州電気通信標準化機構(以下“ETSI”とする)主催により実施された XAdES のプラグテストへの参加報告を記す。プラグテストの概要に加え、今回のプラグテストで新たにテスト項目となった XAdES 1.4.1/1.4.2 につき、それ以前の仕様との相違を解説する。実装者にとって有益な情報となるであろう。

3.3 節「ASiC プラグテスト参加報告」では、2012 年 11 月から 12 月にかけて ETSI 主催によ

り実施されたASiCのプラグテストの参加報告を記す。ASiCはETSIにおいて2011年から2012年に策定化された新たな仕様であり、本仕様のプラグテストは今回が始めての試みである。プラグテストの概要に加え、ASiC仕様概要や技術課題等も解説する。

3.4節「ETSI/TC ESIの動向」では、欧州電気通信標準化機構／電子署名基盤技術委員会(ETSI/TC ESI)での最新の議論を紹介する。現在、同委員会ではEC電子署名指令460及びEC電子署名規制対応の取組みを行っており、その取組みの中からトラステッドリスト、適格証明書の失効タイミング、CAdESにおけるアーカイブタイムスタンプV3、署名検証プロセス、欧州以外の国の適格証明書発行、欧州標準承認プロセスの簡素化について取上げる。

本稿が、電子署名・認証に関するこれまでの成果の価値を改めて見直す契機を与え、またこの領域に残された課題に挑戦しようとする個人あるいはグループの参考となることを、そしてこれが通して電子署名・認証の本格的展開を促し、安全・安心なIT社会の実現へと結びつくことを切に希望する。

第１章　電子署名の新しい可能性

1.1　eRAP/ECOM におけるこれまでの取り組み

日本において電子署名の標準化と普及に向けた取り組みは ECOM によって 2000 年度に開始され、その活動が 2010 年度は eRAP に引き継がれてきた。以下に活動の概要を簡単にまとめる。この間に長期署名仕様の JIS プロファイル化や ISO 化など多くの実績が残った。

表 1-1　eRAP/ECOM における活動と報告書の一覧

ECOM 次世代電子商取引推進協議会	
2000 年度	電子署名文書長期保存に関する中間報告
2001 年度	電子署名文書長期保存に関するガイドライン
2002 年度	タイムスタンプサービス調査報告書 タイムスタンプサービスの利用ガイドライン タイムスタンプサービスの運用ガイドライン
2003 年度	署名ポリシ調査報告書 電子文書長期保存のための保存性・見読性調査検討報告書
2004 年度	電子文書の長期保存と見読性に関するガイドライン 電子署名法の在り方と電子文書長期保管に関する現状調査報告書(※PKI-J)
2005 年度	◆長期署名フォーマット相互運用性試験 長期署名フォーマットプロファイル 長期署名フォーマット相互運用性試験報告書
2006 年度	電子文書長期保存ハンドブック
2007 年度	◆ECOM CAdES/XAdES Plugtest 電子署名普及に向けた調査報告書
2008 年度	◆ETSI XAdES Remote Plugtest 電子署名普及に関する活動報告 2008 JIS X 5092 CMS 利用電子署名(CAdES)のプロファイル JIS X 5093 XML 署名利用電子署名(XAdES)のプロファイル
2009 年度	電子署名普及に関する活動報告 2009
eRAP 電子記録応用基盤フォーラム	
2010 年度	電子記録応用基盤に関する調査検討報告書 2010 [1] 電子データ保存システムに関する調査研究報告書 ◆2010 XAdES / CAdES Remote Plugtest (日欧合わせて XAdES に 16 カ国 27 組織が参加。うち日本からは 1 社が参加、CAdES が 10 カ国 17 組織が参加)
2011 年度	◆PAdES Remote Plugtest (日米欧合わせて 17 カ国 36 組織が参加、日本からは 6 社が参加) ◆XAdES Remote Plugtest (日欧とブラジル合わせて 14 カ国 23 組織が参加、日本からは 1 社が参加) 電子記録応用基盤に関する調査検討報告書 2011 [2]
2012 年度	◆ASiC Remote Plugtest (日欧合わせて 12 カ国 16 組織が参加、日本からは 1 社が参加) ○ISO 14533-1, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES) ○ISO 14533-2, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 2: Long term signature profiles for

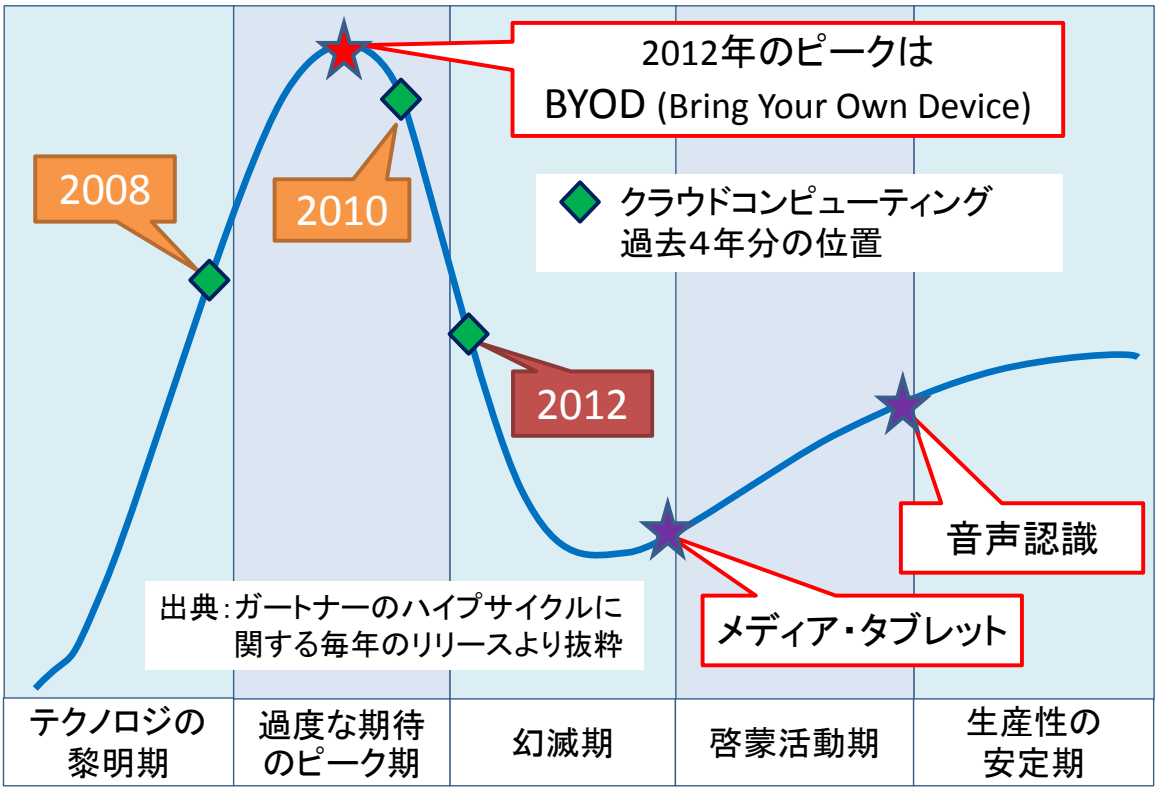
	XML Advanced Electronic Signatures (XAdES) ○ISO/DIS 32000-2：Document management -- Portable document format -- Part 2: PDF 2.0

※ PKI-J：日本 PKI フォーラム

1.2 電子署名マーケットの現況

電子署名マーケットの現状を考える為にまずは調査会社であるガートナーが毎年公開している「先進テクノロジのハイプ・サイクル」を見てみることにする。最新の 2012 年版でも多数の先進テクノロジがリストアップされているが残念ながら電子署名は入っていない。ハイプ・サイクルでは、先進テクノロジが普及するまでの流れを「黎明期」「過度な期待のピーク期」「幻滅期」「啓蒙活動期」「生産性の安定期」の 5 つのステージ(期)に分けている。もちろん途中で消えてしまう先進テクノロジもあるであろうし、何でもハイプ・サイクルを経るとは限らないが、多くの先進テクノロジが普及するにはハイプ・サイクルのステージを経験することが多い。ここではハイプ・サイクルを使って電子署名の現況を検討した。

先進テクノロジの例としてまずクラウドコンピューティングを見てみる。図 1-1 に過去の分も含めてガートナーのリリース[3][4][5]より抜粋した図を示す。クラウドコンピューティングの「黎明期」は 2008 年くらいであり、この頃に名前が出てくるようになっている。次に「過度な期待のピーク期」が 2010 年。2012 年現在では既に「幻滅期」に入っている。「幻滅期」とは良い面ばかりでは無く実際に使われるようになって問題点や悪い面が見える時期と考えられる。クラウドコンピューティングはほぼ 2 年毎にステージを移動しているようであり、このまま行けば 2014 年には「啓蒙活動期」に入り、2016 年には「生産性の安定期」に入り本格的に普及すると予想できる。なお 2012 年にピークを迎えているのは BYOD(Bring Your Own Device)である。BYOD はこれから幻滅期を迎えると予想される。また 2012 年にはメディア・タブレットが啓蒙活動期に入ろうとしており、音声認識は生産性の安定期に入っている。メディア・タブレットはこれから普及が期待され、音声認識は既に市場にて受け入れられている状況と言うことになる。ほぼ現状を表していると言えるだろう。



2012年リリース： http://www.gartner.co.jp/press/html/pr20120906-01.html

図 1-1　ガートナーの先進テクノロジのハイプ・サイクル（抜粋）

それでは次に電子署名をハイプ・サイクルで考えてみる。電子署名の「黎明期」は 2000 年頃に ECOM から「電子署名文書長期保存に関する中間報告」が出た辺りと考えられる。2001 年には電子署名法が施行されており、本格的な電子署名利用の検討が開始された時期である。次に「過度な期待のピーク期」は 2007 年頃の「ECOM CAdES/XAdES Plugtest」の時期であろう。日本国内だけで CAdES と XAdES を合わせて 22 社がこの 2007 年度の相互運用試験に参加している。この数は現在 ETSI で行われている国際プラグテストへの参加社数と比べても遜色が無い程多い。残念ながら近年では ETSI 国際プラグテストへの日本からの参加企業数は多くても 6 社程度となっている。

「過度な期待のピーク期」において、長期署名を実装するベンダは増えたものの実際の案件が増えることが無くだんだん幻滅し撤退企業も増える「幻滅期」が 2011 年頃まで続いていたが、2012 年からは内容は後述するが少し上向きになり「啓蒙活動期」に入っていると考えている。ここまでの電子署名の普及の動きをクラウドコンピューティングと比べると残念ながらかなり遅い。1 つのステージにクラウドコンピューティングの倍以上の 5～6 年程度かかっている。本当の電子署名が普及する「生産性の安定期」には「啓蒙活動期」に入った現在からまだ 5～6 年はかかると予想される。これからが本格的な普及に向けたステージでありしっかりと啓蒙活動して行くことが重要と考えている。

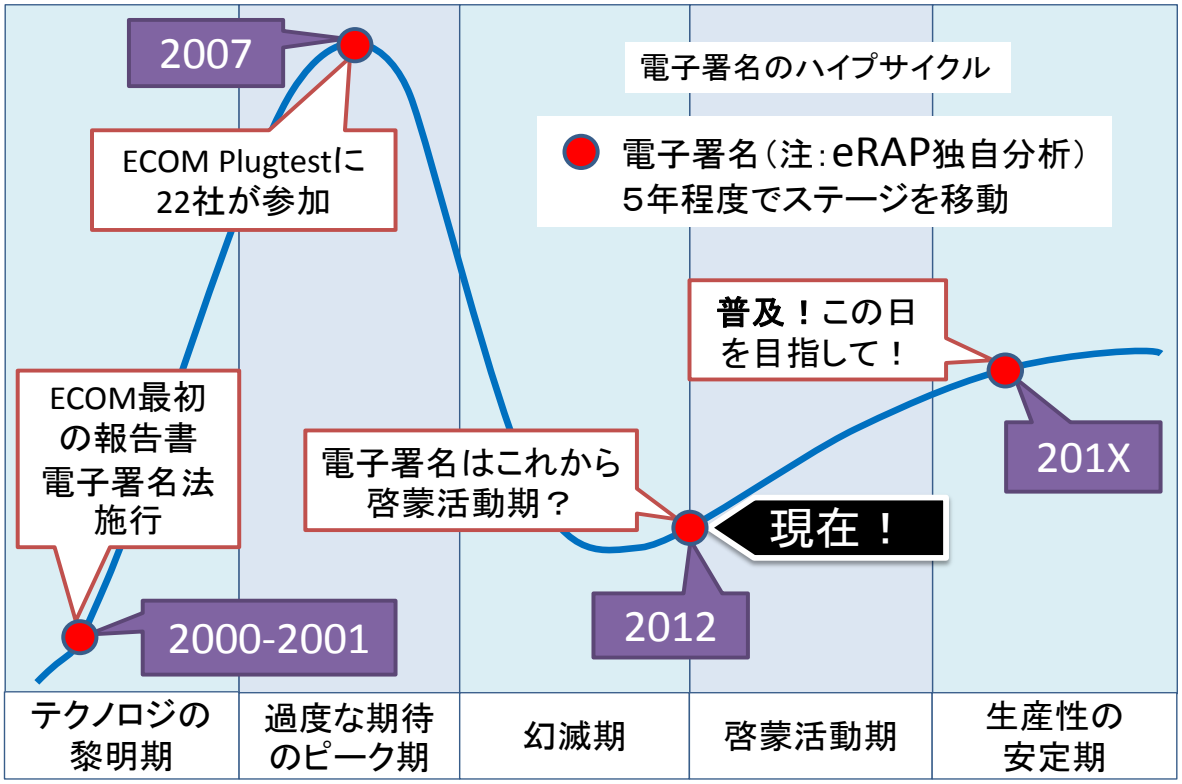


図 1-2 電子署名のハイプ・サイクル（eRAP 技術検討 WG の分析結果）

次に 2012 年現在において電子署名の何が上向きになっているかをまとめる。大きなポイントとして「長期署名が世間に認知されはじめた」ことだろうと考えている。ドキュメント利用アプリケーションである Microsoft Office(以下“MS-Office”とする)(OOXML)と Adobe Acrobat(PDF)が近年どちらも長期署名を採用した。Office(OOXML)では XAdES が、Acrobat(PDF)では PAdES が使われている。

OOXML に関しては MS-Office 2010 から署名フォーマットとして Xml 署名(XmlDsig)に替わって XAdES が採用された。PDF に関しては Adobe Acrobat-X から PAdES にも対応した。Microsoft と Adobe と言う一般にも良く知られたメジャー企業の製品に長期署名が採用されたことで、一般の利用者にも長期署名と言うキーワードが認知されはじめたようだ。

しかしながら MS-Office ではレジストリを修正しないと XAdES-T(署名タイムスタンプ)以上が利用できない上に、XAdES-A(アーカイブタイムスタンプ)も付与できない。また MS-Office も Acrobat も検証情報発行までの猶予期間の考慮がなされていない等、本格的に利用するにはまだまだ課題が残っている。いずれこれらはアプリケーションのバージョンアップにより改善されると期待される。既に MS-Office 2013 や Acrobat-XI が発表またはリリースされており、改善を期待したい。日本独自の事情もあるので可能であれば要望等をアプリケーションメーカーに上げて行けることが望ましい。例えば日本の商用タイムスタンプ局で必要となっている独自認証への対応や、GPKI/LGPKI 等の日本独自認証基盤への対応等があげられる。

PDF の長期署名である PAdES に関してはまだ JIS プロファイル化されておらず、仕様的にも自由度が高いことが相互運用性確保する場合に問題になる可能性が高いと懸念している。XAdES/CAdES の JIS プロファイルも見直しの時期にあることから、XAdES/CAdES/PAdES の

3 種類の長期署名フォーマットに関する JIS プロファイル標準化を整備することが、長期署名の本格普及の鍵になると考えている。

他にも内閣官房情報セキュリティセンター(以下“NISC”とする)において、公開 PDF 文書に電子署名を付与するようになった。詳しくはドキュメント「PDF ファイルの改ざんによるサイバー攻撃への対策について」[6] が公開されている。このドキュメントにも PDF 電子署名が付与されている。本件に関しては eRAP 代表メンバにて NISC の訪問と意見交換も行った。なお公開 PDF 文書の署名検証の為に、Adobe Reader/Acrobat では GPKI のルート証明書が標準搭載された。しかしながら GPKI では CRL の取得に GPKI のディレクトリサーバのホストを指定する必要があるが、ディレクトリサーバの設定は手動で行う必要がある。一般の検証者の手間が必要な点ではまだ課題が残っていると言える。

海外の政府系認証基盤にも長期署名が多く使われている。例えば欧州ではエストニアが、ラテンアメリカではブラジルの政府認証基盤にて、XAdES が使えるようになっている。PAdES 仕様ができたことで政府系公開文書にも PAdES を利用する動きも欧州等では広がりつつある。

eRAP メンバ企業のビジネスにおいても 2012 年度は案件数や成約数が増えたとの報告があった。このように利用者側から電子署名や特に長期署名について関心が高まりつつある。これから来るであろうハイプ・サイクルの「啓蒙活動期」を乗り越えて普及が進み「生産性の安定期」のステージ到来を期待して、その為の活動も業界として行っていくべきと考える。

1.3 これからの電子署名の可能性

1.3.1 クラウド・モバイルや認証との連携

2012 年度はこれまで以上にクラウドとモバイルによるパラダイムシフトが進んだ年であった。スマートフォンやタブレット等のモバイル端末による常時ネットワーク接続の環境は、クラウドによるサーバサイドを利用したサービス提供との相乗効果によって、コンシューマ市場における PC の利用を減らした。これに伴い電子署名もクラウド化や Web サービス対応が今後必須になると考えられる。eRAP ではこれまでクラウド上での電子署名の利用形態を考察してきた。

もう 1 つ大きなキーワードとしてソーシャルがある。例えば 2012 年度は、ソーシャル・ネットワーキング・サービス(以下“SNS”とする)やソーシャルゲーム等が本格的な普及した年でもあった。特に SNS ではクラウドや認証技術と結びつき ID の利用が進み、多数の ID を管理する ID プロバイダを生み出している。ID を使う為の技術以外に ID の信頼性も認証レベルやトラストフレームワークにより向上している。eRAP の 2011 年度の報告書では認証技術を中心に電子署名との連携の可能性をまとめた。

コンシューマ市場においては従来の Java やデータベースによるウェブサービスから、REST(REpresentational State Transfer)サービスによる軽量かつ簡単に構築できる仕組みに移行が進んでいる。電子署名サービスも API として提供することで既存ウェブサービスとの連携による利用の可能性が考えられる。その際に X.509 証明書と関連付いた秘密鍵をどのように利用運用するかを検討する必要がある。秘密鍵をサーバ側に置く鍵ローミングが実現すると、電子署名のクラウドや Web サービスにおける利用が進むと期待される。

ここで問題となるのは、利用者が安心してサーバ側に置かれた秘密鍵を使う為の技術や仕組み

をどう実現するかである。認証技術としては近年 OpenID Connect with OAuth 2.0 [7] 等の標準化や学術分野では Shibboleth/SAML 等の利用[8] が進みつつあるが、技術だけでは無く電子署名サービスを提供しているサービス提供事業者を確認する信頼の仕組みも必要となる。これには eRAP の 2011 年度の報告書にも書いたが、米国で進んでいるトラストフレームワークのような取り組みや、新しい信頼の仕組みを検討して行く必要があると考えている。信頼と言う意味では PKI の認証局と ID プロバイダの連携も新たな可能性があるように思える。このようにクラウドや認証等の新しい技術や仕組みと、電子署名や PKI の組み合せによる新しいビジネスモデルの構築と実現が期待される。

1.3.2 組込システムや制御系システムのセキュリティ

組込システムや制御系システムにおいてもセキュリティの要請は高まっている[9]。これらのシステムはインターネットとは接続しない閉じたネットワークのため安全性が高いとされてきた。しかし最近の自動車は 100 個近い ECU が搭載され、車内 LAN によってそれらが結ばれ、カーナビゲーションシステムなどを通じて外部とも接続し始めている。またビル管理や工場、発電所などのプラント、社会インフラやライフラインを制御する重要な制御システムも、近年はそれらをメンテナンスするシステムに Windows や Linux などの汎用 OS が用いられており、インターネット経由のサイバー攻撃[10] が現実のものとなっている(イランの核施設攻撃に用いられた Stuxnet は記憶に新しい)。そのためこれら組込システムや制御系システムにおいてもシステムのインテグリティ確保や監査証跡の保全、あるいは通信データや制御データの完全性確保のため電子署名を用いる動きがある。計算機リソースに制限があり、コスト競争の厳しいこれらの機器、システムにおいて利用しやすい電子署名や証明書とその検証について検討を進め利用指針を示すとともに技術者の教育を行う必要があるのではないだろうか。

1.3.3 これからの電子署名の課題

電子署名の普及の為には情報提供方法を、一般利用者とサービス開発者に分けて検討すべきと考える。利用者と開発者では要求が異なる点を理解した上で情報を整理して提供すべきである。これまでの電子署名は一部専門家だけが理解していると思われている点が、利用者や開発者から敬遠されている一因になっているのではないか。まず利用者と開発者に何が必要で何が必要ないかをまとめてみる。サービス提供者と言う区分もあるがここでは開発者にまとめた。

(1) 利用者は仕組みを知る必要はない - 望んでいること

※ 利用者は仕組みを知らなくても何をすれば何ができるのかを理解していればよい。

・電子データの保証の為にハンコを押印するように手軽な利用方法を望んでいる。
・手軽に電子証明書を取得と更新し、タイムスタンプを使える環境を望んでいる。
・既存のクラウドや Web サービスと連携した利用形態を望んでいる。
・非 PC 系のスマホ等のネットデバイスからの利用形態を望んでいる。

(2) 開発者(サービス提供者)は仕組みを知る必要がある - 必要な情報

※ 開発者は利用者にサービスを提供する為に情報を得て仕組みを理解する必要がある。

・利用者に電子署名をサービスとして提供するビジネスモデルを必要としている。
・サービスに使えるインフラ(認証局やタイムスタンプ局)を必要としている。
・運用する為の標準化や法的な対応に関する情報を必要としている。
・サービスの実装に必要となる技術情報を必要としている。

以上から考えて電子署名の普及の為に、主に開発者やサービス提供者へ提供すべき項目を列挙する。一部の項目は相反する面もあるが今後検討する材料となれば良いと考えている。

(a)利用者向け環境の整備
・初心者にも分かりやすい説明と電子署名を簡単に試せるポータル等の整備
・電子署名のサービス提供者を信頼する為の仕組みの提供
・公的証明書や認証局や ID プロバイダ等による用意な証明書の取得環境の整備
・既存サービスと連携して利用可能な電子署名やタイムスタンプのサービスの提供
・署名鍵をサーバに預ける為(鍵ローミング)の信頼と安全な認証の仕組みの提供

(b)開発者向け環境の整備
・電子署名に関する技術者コミュニティの実現による教育や情報交換の場の提供
・新技術や異分野と電子署名を組み合わせたビジネスモデルを構築して提供
・専門家の持つ知識を分かりやすく解説した技術書籍やガイドライン資料の提供
・フリーに利用して試せる長期署名等のオープンソース実装の提供
・高度に API 化された使いやすい商用の電子署名機能の提供
・相互運用性を確認する為のプラグテスト実施やポータルによる互換性情報の提供

(c)標準化による環境の整備
・電子署名のサービス提供者を信頼する為の仕組みの検討と標準化作業
・世界標準の技術を日本でうまく利用する為のプロファイル等の標準化作業
・日本の法律や実情に合ったシステム構築や運用手順のガイドライン化等の作業
・日本で検討した仕様を世界標準に反映する為の作業

「1.2 電子署名マーケットの現況」にて分析したように、利用者のニーズ自体は着実に高まりつつあると感じられる。更に新たな電子署名の利用方法を実現し提供することで市場は拡大すると期待できるのではないか。また eRAP/ECOM ではこれまで地道な標準化作業を続けてきたが、これは国際標準化の場においても一定の評価を得ており電子署名分野に関しては日本が国際的にも進んでいる分野と言える。日本で標準化された技術を逆に国際標準にすることができれば日本がこの分野のリーダーの立場も確立して先行者として有利になれる。今後も継続した標準化に関しての取り組みと、クラウドやモバイルを含めた新市場への取り組みによる情報の提供が重要であると考える。この 2 つはどちらも平行して進めて行く必要があるだろう。

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 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-．一般財団法人日本情報経済社会推進協会，2012 年 3 月

[2] 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-．一般財団法人日本情報経済社会推進協会，2011 年 5 月

[3] ガートナー ジャパン株式会社．“先進テクノロジのハイプ・サイクル(プレス・リリース) : 2012 年”．http://www.gartner.co.jp/press/html/pr20120906-01.html

[4] ガートナー ジャパン株式会社．“先進テクノロジのハイプ・サイクル(プレス・リリース) : 2010 年“．http://www.gartner.co.jp/press/html/pr20101019-01.html

[5] ガートナー ジャパン株式会社．“先進テクノロジのハイプ・サイクル(プレス・リリース) : 2008 年“．http://www.gartner.co.jp/press/html/pr20080827-01.html

[6] 内閣官房情報セキュリティセンター(NISC)．“PDF ファイルの改ざんによるサイバー攻撃への対策について”．http://www.nisc.go.jp/press/pdf/pdf_kaizan_press.pdf

[7] OpenID ファウンデーション・ジャパン．http://www.openid.or.jp/

[8] 学術認証フェデレーション(学認)．https://www.gakunin.jp/ja/

[9] 独立行政法人 情報処理推進機構．制御システムにおけるセキュリティマネジメントシステムの構築に向けて～ IEC62443-2-1 の活用のアプローチ ～．2012 年 10 月 http://www.ipa.go.jp/security/fy24/reports/ics_management/ics_management_manual2012.pdf

[10] 独立行政法人 情報処理推進機構．グローバルシンポジウム 2012 報告書　公演資料“制御システムの今あるセキュリティ脅威と対策について～制御システムは、セキュリティ脅威とは関係ないと思っていませんか～”．2012 年 5 月 http://www.ipa.go.jp/about/news/event/globalsympo2012/pdf/glosym2012_security2.pdf

第２章　本人認証／属性認証についての考察

電子記録の推進には、安全な保管とともに、その利活用を安全に行うことが重要な課題としてある。特に電子記録に対するアクセス制限を多様に行うためには、利用者の本人認証とともに、所属企業、役職、国家資格などの属性情報を用いて行うことが考えられる。

これまで、電子記録に対するアクセス制限に関する標準的なガイドラインがなかったことにより、極力リスクを避ける目的で電子記録の利用者を例えば部門内に限定するなど制限を強くしており、電子記録を広く利活用するには至っていなかった。

そこで、来年度以降に電子記録のアクセス制限に関する標準的なガイドラインを作成する準備として、本章では、まず本人認証及び属性認証分野の概要と動向について紹介し、次にネット上において信頼性の高い本人認証及び属性認証を実現するために今後検討すべき課題を整理する。

2.1　本人認証／属性認証技術の概要と動向

2.1.1　本人認証[1]

認証技術は技術、強度などの観点から様々な分類が考えられる。

一般に、本人認証技術は次の 3 つの要素に分類することができる。

・本人の記憶に基づくもの(パスワード、PIN など)
・本人の所持に基づくもの(eID カードなど)
・本人のバイオメトリクス情報に基づくもの(指紋、虹彩など)

(1)記憶

本人のみが記憶しているデータに基づいて利用者を認証する方法であり、パスワード、などがこれに当たる。この方法は記憶忘れの問題がある。これに対応するために、長期記憶(小学校の担任の先生の名前、など)を利用するものもある。

(2)所持

本人のみが所持している物によって利用者を認証する方法であり、eID カードやワンタイムパスワードのトークンなどがある。所持物は盗難の危険性がある。これに対応するため、バイオメトリクスである指紋認証や記憶要素である PIN と組み合わせで用いることが多い。

(3)バイオメトリクス情報

本人の生体に基づくデータにより利用者を認証する方法であり、本人の特性としての指紋、音声、虹彩、顔の形などを識別することによる。この方法は識別装置の性能により精度が左右される。より一般的な方法として、顔写真による方法がある。

2.1.2　属性認証[2]

属性(attribute)とは、本人(主体)に付属する情報(職責／資格／地位など)である 。属性には次のような例がある。

・申請等の代理人資格(社内代理人、行政書士、弁理士等)
・社員の所属、担当業務、職位
・医師資格など各種資格
・情報処理技術者試験などの試験の合格情報
・インターネットショップにおける会員資格

属性を利用するにあたっては、以下の観点で利用する属性を分類し、適切に取り扱う必要がある。

(1)時間の経過に伴い変化する属性情報かどうか

①先天的に変わらない情報：生年月日、バイオメトリクス情報など
②後天的に付加され変わらない情報：学歴・職歴などの経歴、賞罰など
③時間的にあまり変化しない情報：資格、免許、職業、住所など
④時間的に変化しやすい情報：所属、職責、権限、資産(預金残高等)など

(2)オープンな属性情報かどうか(信頼できる属性情報かどうか)

①オープンに通用する情報：住民基本情報、商業登記情報、免許(許認可)など
②コミュニティ内で通用する情報：所属部門、職責、ランク、会員資格など

(3)センシティブな属性情報かどうか

①知られてもよい(知らせたい)情報：氏名、会社名、資格、免許(許認可)、賞など
②知られたくない情報：戸籍情報、住所・TEL、経歴、罰、診療情報、成績、年収など

2.2　アイデンティティ管理技術の動向[3]

近年、アイデンティティ管理技術は、ユーザの識別子(ID)の管理技術にとどまらず、複数のサービスで利用することを前提としたものとなっていて複数の目的を持っている。例として、以下のものが上げられる。

・人々を本人であると認証すること
・人々の属性情報を交換すること
・人々の属性情報に基づいてアクセスを制御すること

これらの検討は米国を中心に進んでおり Liberty Alliance　以降 Concordia Project が立ち上がり、現在ではカンターラ・イニシアティブが中心に活動している。

(1)カンターラ・イニシアティブ[4]

カンターラ・イニシアティブは ID 管理技術を通じてオンラインサービスにおける「セキュリティ確保」「プライバシ保護」を促進することを目的として 2009 年に設立された。

この設立に参加した団体は以下のとおりである。なお、カンターラ・イニシアティブ設立に伴い、リバティ・アライアンス、コンコーディア・プロジェクト、openLiberty の 3 つのプロジェクトはカンターラ・イニシアティブに活動内容を移管したうえで解散した。

①Concordia Project：SAML、OpenID、OAuth、InfoCard 等、アイデンティティ管理技術間の相互運用方式検討を行う非営利団体

②Liberty Alliance：アイデンティティ管理技術に関する技術標準策定、セキュリティ評価、技術標準に基づく実装の相互運用性試験、等を実施する標準化団体

③openLiberty ：リバティ・アライアンス仕様に基づくオープンソースソフトウェアの実装を行うオープンコミュニティ

④DataPortability Project：インターネットにおけるユーザ情報のサービス間での相互利用方式を検討する非営利団体

⑤Information Card Foundation ：インターネットにおけるデジタル・アイデンティティ・カード(InfoCard)の普及を目指す非営利団体

⑥Internet Society：インターネットに関する標準化、教育、ポリシ策定等の活動を主導する非営利団体。Internet Society は下部組織には IETF(Internet Engineering Task Force)や IAB(Internet Architecture Board)を有している

⑦XDI.org/XDI Public Trust Organization：ネットワーク、プロトコル非依存のリソース識別子 XRI(eXtensible Resource Identifier)ベースの Identity が、個人・企業ともに長期的・安定的かつ安全に利用できるようにするための非営利の管理団体

(2)応用事例(学認システム概要)[5]

属性情報の交換を行うプロジェクトの例として、学認システムを紹介する。

平成 20 年度から実験がスタートし、現在数十の大学、ベンダが参加し活動を行っている。これらの傘下団体は、学術認証フェデレーションに参加する。

学術認証フェデレーションのホームページによれば、「学術認証フェデレーションとは、学術 e-リソースを利用する大学、学術 e-リソースを提供する機関・出版社等から構成された連合体のことです。各機関はフェデレーションが定めた規程(ポリシ)を信頼しあうことで、相互に認証連携を実現することが可能となります。」とある。

認証連携を実現することにより、学生が学内で ID/パスワードなどにより認証することにより、連携するサービスに対してもシングルサインオンすることができるようになる。

2.3 本人認証/属性認証展開のための課題

電子記録管理システムのアクセス制御について、図 2-1 に示す通り、組織内利用と組織間利用

についてその課題を整理する。業務及び保管(アーカイブ)についてのアクセス制御については、検討外とする。

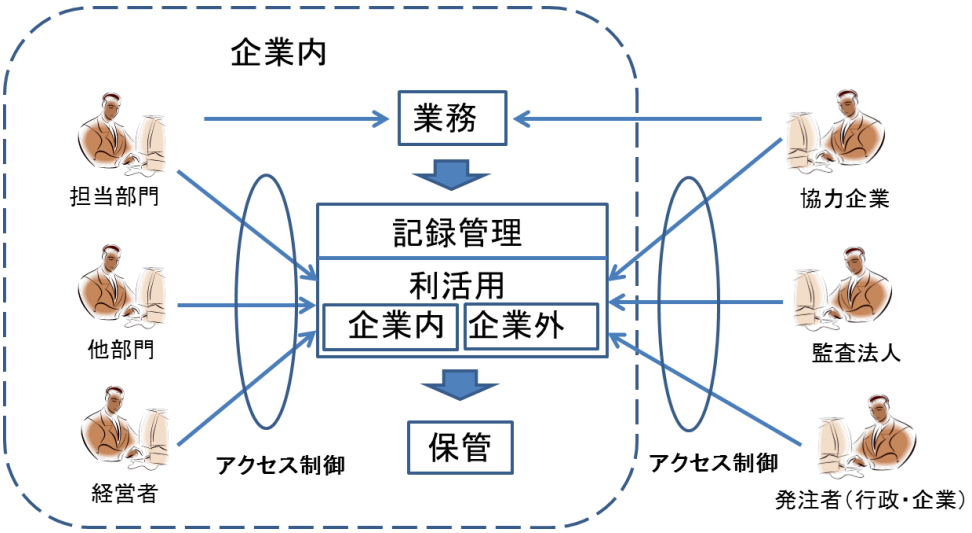


図 2-1　記録管理の組織内利用と組織間利用

(1) 組織内利用

組織内利用とは、電子記録の発生及び管理している組織内での利用で、一般的に社員番号とパスワードで本人確認ができ、人事システムと連携していることから以下の属性を社員番号から引き出すことも容易である。

- 所属組織/役職
- 経歴(社内履歴を含む)
- 基本 4 情報(住所、生年月日、性別、氏名)
- 顔写真
- 資格情報
- 国籍
- 病歴・活動歴(社秘密の可能性もある)

これらの情報を用いて、アクセス制御のバリエーションを検討することができる。

人事異動によるアクセス権の喪失時の対応については、考慮する必要がある。

(2) 組織間利用

組織間利用とは、1 つの企業が下請けなどと組んで 1 つの文書管理システムを利用する場合、監査法人に必要な記録を開示する場合、及び発注者側(官庁・企業等)と情報を共有する場合が考えられる。

(a)信頼の枠組み

アクセス権を社外の人に与える方法を検討する必要がある。

①仮の社員番号とパスワードを発行する場合

例えば、下請け会社の社員にアクセス権を与える場合は、本人確認及び必要な属性情報を確認したうえで仮の社員番号とパスワードを発行する場合が考えられる。

この場合は、社内システムを変更しないで利用することが可能であると考えられる。

②外部の会社/団体の本人確認/属性情報をそのまま利用する場合

・この場合は、カンターラ・イニシアティブが進めている ID 連携を検討する必要がある。ただし、政府機関とも情報連携していくためには、政府が認める独自の「(日本型)信頼の枠組み」について新たな検討が必要になる可能性もある。

・ID 連携において、政府が進めているマイナンバーをどのように民間 ID と連携して活用することにより信頼性を高めることができるかも、検討課題である。

・企業内では属性情報として電子的に管理されていない顔写真などの情報も必要になる可能性も高い。

③セキュリティの向上

セキュリティ確保のため、以下の項目も検討対象になる。

・データ送信時の暗号/秘密分散技術の利用

・アクセス記録の保管

④属性情報プロバイダ再考

アクセス制御のための本人確認及び属性認証を信頼できる第 3 者機関に依頼する方法が考えられる。これは、電子記録のアクセス制御だけではなく、本人確認及び属性認証を必要とされるサービスにも利用できる可能性がある。

また、この信頼できる第 3 者機関を法律で制度化することにより、政府が信頼する属性情報交換の枠組みを作ることが可能である。

一般財団法人日本情報経済社会推進協会(以下“JIPDEC”とする)では属性情報プロバイダとして、本人の了承を得たうえで属性情報を提供するシステムを検討した[2]。今後、電子記録の利活用をユースケースとして検討することも価値があると思われる。

そのイメージを図 2-2 に示す。

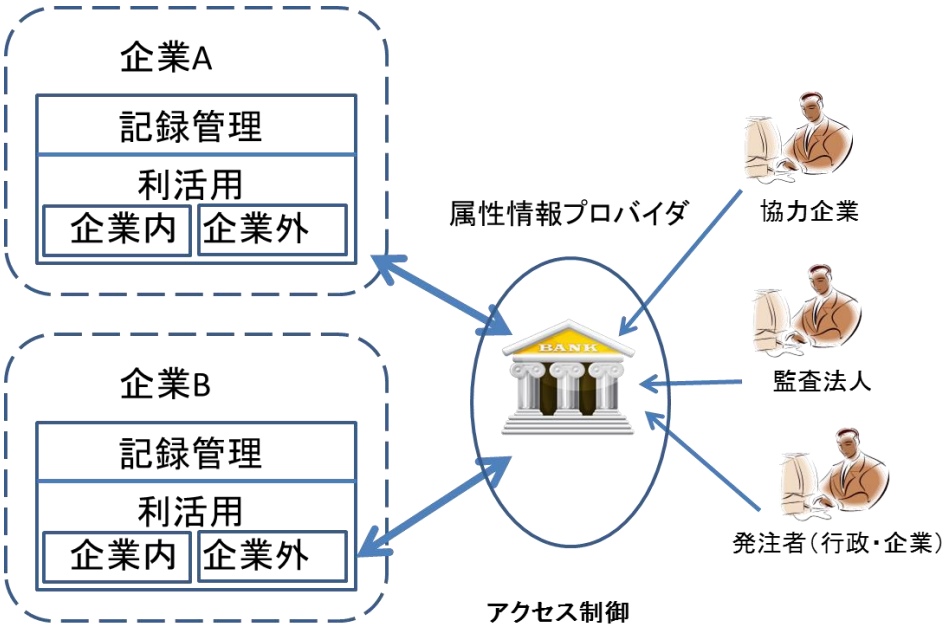


図 2-2　属性情報プロバイダによるアクセス制御

2.4　まとめ

電子記録に対するアクセス制御のガイドラインを作成するため、今後検討すべき検討課題を整理した。検討項目の中で、アクセス制御のための本人確認及び属性認証を行う信頼できる第 3 者機関である属性情報プロバイダの具体化による日本型の信頼の枠組みの構築についても取り上げた。今後、具体的なユースケースを想定して、検討を進めていく予定である。

参考文献

[1] 情報処理振興事業協会，本人認証技術の現状に関する調査報告書．2003 年 3 月．
[2] 財団法人日本情報処理開発協会．属性認証ハンドブック．2005 年 2 月．
[3] 公益財団法人 情報処理推進機構．アイデンティティ管理技術解説(ドラフト版)．2013 年 1 月．
[4] 伊藤宏樹．アイデンティティ管理技術に関する新団体「カンターラ・イニシアティブ」．NTT 技術ジャーナル，2009 年 11 月．
[5] 学術認証フェデレーション．https://www.gakunin.jp/ja/　2013 年 1 月 30 日取得．

第 3 章　署名・認証標準化動向

3.1　標準化活動報告

3.1.1　長期署名プロファイル ISO 標準化プロジェクト

2012 年 6 月に ISO ドラフト(FDIS)の最終投票が行われ、参加国(P メンバ)の大多数の賛同が得られ、2012 年 9 月についに ISO 標準として発行されることになった。ISO 標準のタイトルはドラフト版のタイトルから変更となり、最終的に以下のようになった。

- ISO 14533-1, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 1: Long term signature profiles for CMS Advanced Electronic　Signatures (CAdES)
- ISO 14533-2, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 2: Long term signature profiles for XML Advanced Electronic　Signatures (XAdES)

ISO 標準として発行されたことで、2009 年より進行してきた長期署名プロファイル ISO 標準化プロジェクトは無事に終了することとなった。

最終投票において、数カ国の投票国からいくつかコメントがあった。コメントの中には ETSI で検討中の新しいアーカイブタイムスタンプ仕様に関する記述を求めるものや、策定作業中に IETF より発行された XML 方式の ERS(Evidence Record Syntax)規格[1] についての記述を求めるものなどがあったが、最終投票の段階ではこのような技術的な修正は禁じられているため反映させることはできなかった。

なお、JAHIS(一般社団法人保健医療福祉情報システム工業会)において、医療分野向けの長期署名プロファイルの ISO 標準化作業が進められており、その草案では ISO 14533 の仕様をベースにしている。

3.1.2　ISO 14533 と JIS X 5092/5093 との関係

ISO 14533 プロファイルは JIS X 5092[2]や JIS X 5093[3]と同様に署名タイムスタンプ付き署名(ES-T)のプロファイルとアーカイブタイムスタンプ付き署名(ES-A)のプロファイルを定めている。長期署名フォーマットの各フィールドの規定は ES-T プロファイルに関しては ISO 14533-1(ISO 14533-2)と JIS X 5092(JIS X 5093)は同じ規定となっている。ES-A プロファイルにおいてアーカイブタイムスタンプの方式として IETF で公開されている ERS(RFC4998 Evidence Record Syntax)方式[4] も選択可能として言及している点が JIS プロファイルとは異なっている(図 3-1)。

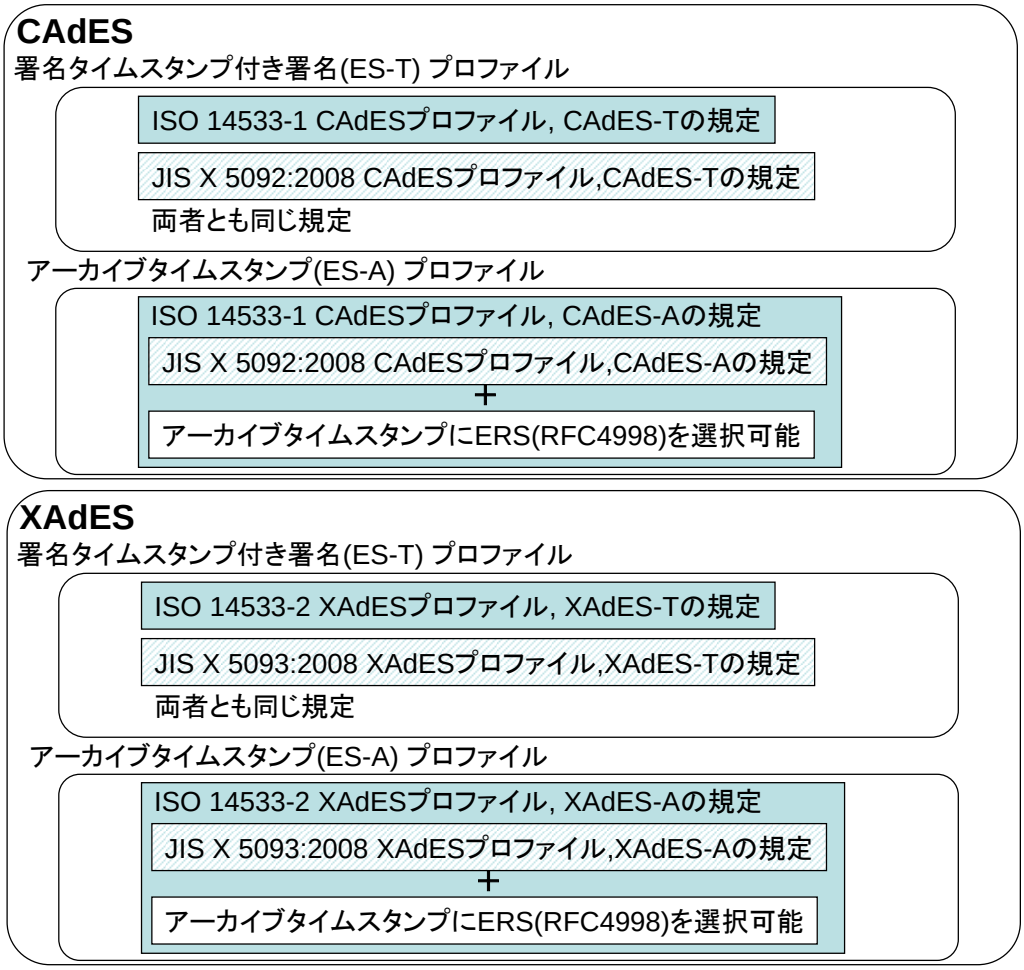


図 3-1　ISO 14533 と JIS X 5092/5093 の関係

従来の CAdES[5] や XAdES[6] の仕様では、1 つの署名データに対して 1 つ以上のアーカイブタイムスタンプが必要であったが、ERS 方式のタイムスタンプでは複数の署名データをまとめることで 1 つのアーカイブタイムスタンプを付与することができる。このアーカイブタイムスタンプの仕組みは、一緒にまとめた他の署名データがなくてもアーカイブタイムスタンプを検証できるようになっており、関係性のない署名データ群をまとめることができる。アーカイブタイムスタンプに関して JIS プロファイルよりも広い用途に適用できることから、JIS プロファイルは ISO プロファイルのサブセットとして考えることもできる。

3.1.3　ISO 14533 策定時の海外の動向

ISO 14533 の策定作業中にも海外において長期署名に関する新たな標準規格が公開された。以下にそれらの規格を簡単に紹介する。

(1)PAdES (PDF Advanced Electronic Signature)[7]

PDF に適用する長期署名フォーマット仕様。

ETSI TS 102 778 として公開されている。

現在策定作業中の PDF 規格 ISO 32000-2 にも同様の仕様が採用される予定である。

(2)ASiC (Associated Signature Container) [8]

関連する複数のデータを 1 つのファイルにまとめてパッケージングする仕様。まとめて署名を付与することもできる。

ETSI TS 102 918 として公開されている。

(3)ETSI ベースラインプロファイル

欧州の電子署名指令に基づく長期署名フォーマットのプロファイル。

ETSI TS 103 171 (XAdES プロファイル)[9] 、ETSI TS 103 172 (PAdES プロファイル)[10] 、ETSI TS 103 173 (CAdES プロファイル)[11] が公開されている。

(4)CAdES の新しいアーカイブタイムスタンプ仕様

ETSI ベースラインプロファイルの策定と共に CAdES の新しいアーカイブタイムスタンプ仕様である Long Term Validation 属性が検討され、同属性の定義が追記された ETSI TS 101 733 v2.1.1[5] が公開された。更に、同属性の仕様とは異なるアーカイブタイムスタンプ v3 が現在検討されている。

(5)長期署名の検証プロセス

ETSI TS 102 853[12] として公開されている。

(6)XML ERS

XML 方式の ERS タイムスタンプ。

IETF で RFC 6283[1] として公開されている。

これらの規格については、ISO 14533 の新規作業提案時に定めたスコープから外れるものや、ISO 14533 の最終投票段階で公開されたものなどがあり、今回の ISO 14533 には取り入れることができなかった。ETSI ベースラインプロファイルと ISO 14533 のプロファイルの関係については 3.1.4 項で、PAdES に関する考察は 3.1.5 項で説明する。

3.1.4 ISO 14533 と ETSI ベースラインプロファイルの関係

ETSI ベースラインプロファイルは主に EU での利用を想定した電子署名のプロファイルである。EU 指令により示された要求に基づき ETSI で規格化されている。ETSI ベースラインプロファイルは従来の CAdES や XAdES で定義されている ES-T(AdES-T)や ES-A(AdES-A)などのフォーマットの分類とは異なり、B-Level、T-Level、LT-Level、LTA-Level といったタイプで分類している。B-Level とは従来の BES や EPES に相当するタイムスタンプのない署名データであり、T-Level は ES-T のように署名タイムスタンプ付きの署名データ、LT-Level は検証に必要な証明書や失効情報を格納した形式、LTA-Level は更にアーカイブ目的のタイムスタンプを付与した形式である。XAdES、CAdES、PAdES について、それぞれのタイプに応じた各種フィールドに対する要件定義とともに、署名に用いるハッシュ関数や暗号アルゴリズムの要件についても言及している。

一方、ISO 14533 は CAdES や XAdES のオリジナル規格(ETSI TS 101 733、ETSI TS 101 903)

で定義されているフォーマットの分類やフィールドの規定に基づいて、長期保存のための利用方法を定めた国際標準であり、各国固有の要件は含まれていない。例えば、ETSI ベースラインプロファイルで言及されているような暗号アルゴリズムに関する要件は国や業界、用途などによって異なるため、ISO 14533 ではスコープ外としている。また、ETSI ベースラインプロファイルでは XAdES、CAdES、PAdES のオリジナルの規格ではオプション要素であった SigningTime 属性の利用を必須としている。SigningTime 属性はタイムスタンプのように第三者が保証する存在証明ではなく、署名者が自己申告で付与する署名時刻(例えば使用した PC 上の時刻など)である。SigningTime 属性の利用は EU での用途を想定したものであり、EU 以外の国にも適用できるものではない。ISO 14533 では SigningTime 属性はオリジナルの規格に従いオプションとして、その利用方法はアプリケーションに委ねている。

CAdES の ETSI ベースラインプロファイルでは従来のアーカイブタイムスタンプ(v1,v2)の利用については定めていないことについても注意が必要である。CAdES v2.1.1 では従来のアーカイブタイムスタンプとは異なる新たな仕様として Long Term Validation 属性を定義しており、CAdES の ETSI ベースラインプロファイルの LTA-Level ではその属性の利用を必須としている。Long Term Validation 属性の導入については一度アーカイブを作成した後に、失効情報などを署名データに追加したいという EU 指令からの要求が背景にあるようである。ISO 14533 では Long Term Validation 属性が新たに定義される前に技術仕様を作成していたため、この属性については直接言及していないが、アーカイブタイムスタンプの新たな仕様についてはその仕様を利用者が入手可能であるならば適用してもよいと定めており、ISO 14533 と CAdES v2.1.1 の仕様を合わせて参照することで Long Term Validation 属性も適用可能と考えることができる。

ISO 14533 と ETSI ベースラインプロファイル、オリジナルの規格(CAdES, XAdES, PAdES)の関係の概略を図 3-2 に示す。

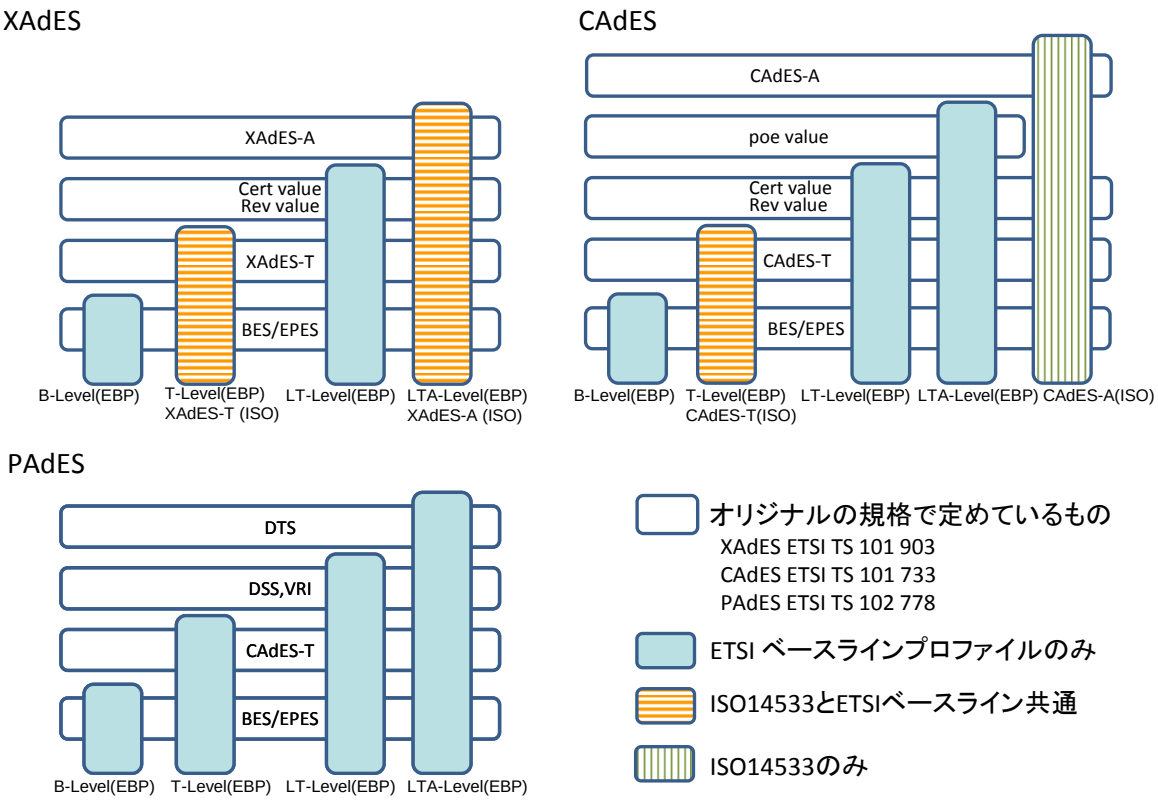


図 3-2　ISO 14533 と ETSI ベースラインプロファイルの関係

3.1.5　PAdES プロファイルについて

PAdES の規格は ETSI で標準化され、ETSI TS 102 778 として公開されている。CAdES や XAdES の規格では電子署名フォーマットの各要素や利用方法、要件などが 1 つの文書として構成されていたが、PAdES ではそれらの文書とは異なり、目的の異なるパートごとに分けて異なる文書として構成し、各パートごとに必要な要素の定義や要件などを記している。現在、公開されているパートは Part.1 (PAdES 規格の概要)、Part.2 (ISO 32000-1 に基づくプロファイル)、Part.3 (PAdES Enhanced ,BES/EPES)、Part.4 (PAdES Long Term)、Part.5 (XAdES に対するプロファイル)、Part.6 (署名の可視表現)となっている。しかし、これらの各パートは独立性が高く、それぞれをどのように組み合わせて利用すべきか、組み合わせた場合にはどのように検証すべきか、などの要件やルールなどが示されていない。PAdES の開発者毎に様々な署名フォーマットのデータが生成され、相互に正しく検証できなくなるといった相互運用性の問題が懸念される(図 3-3)。1 つの文書で要素の定義や利用方法、フォーマットのタイプと要素の関係なども記されていた CAdES や XAdES よりも相互運用性の問題を引き起こしやすい内容であると考えられる。

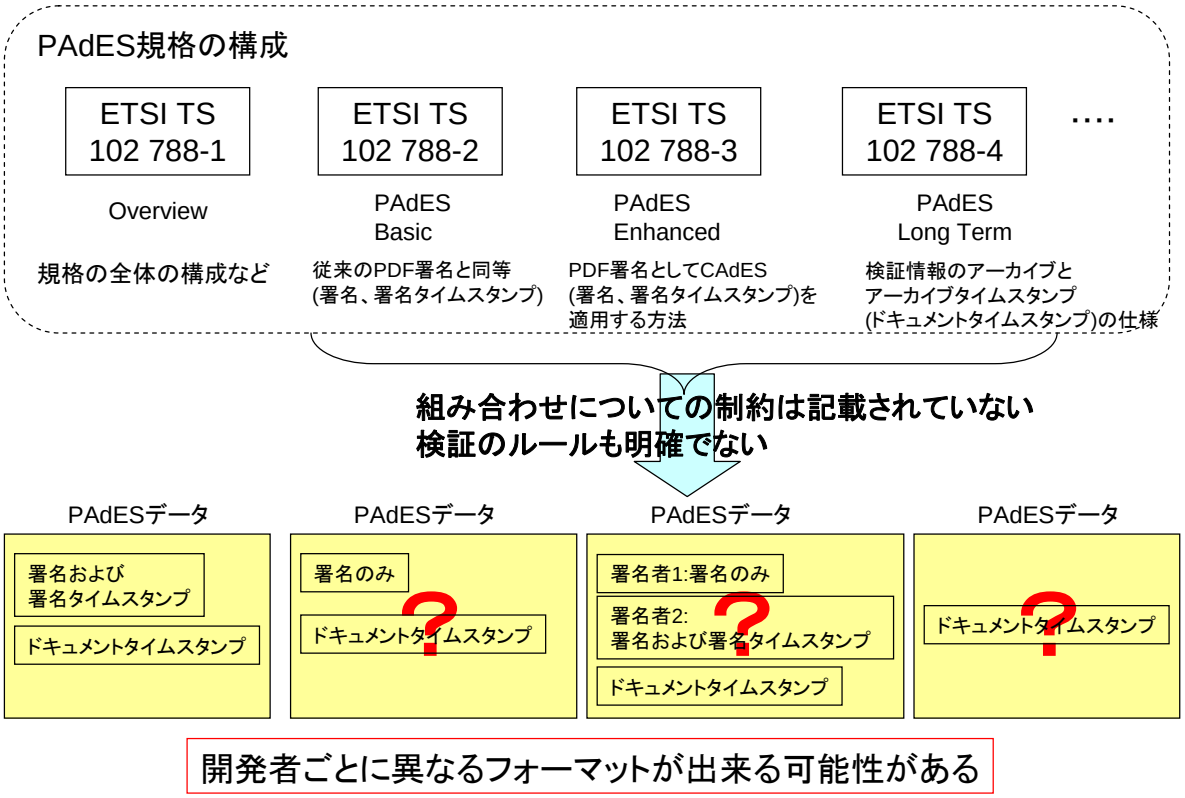


図 3-3　PAdES 規格の構成と問題点

前項で説明した ETSI ベースラインプロファイルではドキュメントタイムスタンプの利用方法については簡単に触れているものの、検証方法などの記述が不足しており、相互運用性の問題は依然として残っている状態にある。

今回の ISO 14533 の新規提案時には PAdES の仕様がまだ公開されていない状況にあり、CAdES と XAdES に関するプロファイルを規定するとスコープを限定していたため、残念ながら PAdES については取り組むことができなかった。ISO 14533 策定の過程においても、海外から PAdES に関するプロファイル策定を切望するコメントが寄せられていた。PAdES は PDF 製品のデファクトスタンダードである Acrobat/Adobe Reader X よりサポートされており、今後もますます活用が広がり、海外だけでなく日本においても PAdES をサポートしていくベンダが増えていくことが予想される。PAdES の相互運用性の問題に取り組むことへの重要性が高まっており、プラグテストの実施、PAdES の利用方法を定めたプロファイルの提案や PAdES 規格そのものの問題点を修正する提案など、日本も積極的に進めていくことが必要である。

3.1.6　まとめ

欧州電子署名指令や日本の電子署名法が成立した 2000 年頃より ECOM において電子文書の長期保存や電子署名、タイムスタンプ、長期署名に関する調査やガイドライン作成などの活動を行っており、2010 年より eRAP にその活動が引き継がれた。

2005 年頃には業界標準となる長期署名プロファイルである ECOM プロファイルを作成し、そのプロファイルに基づく ECOM プラグテストを実施した。この ECOM プラグテストには国内の 14 社のベンダが参加し、ECOM プロファイルや参照規格である CAdES や XAdES の問題点を明

らかにした。この ECOM プラグテストで得られた知見は ETSI へ要望と共に伝えられ、CAdES や XAdES 規格の改訂につながり、また、後の JIS 規格を作成するうえでのベースにもなった。更に、この ECOM プラグテストは、ETSI では初となる非対面のオンラインによる長期署名のプラグテストを実施する際のリファレンスとなり、現在も ETSI で同様のスタイルによるプラグテストが継続して実施されている。

2008 年には ECOM プロファイルと ECOM プラグテストによって得られた知見を元に作成した JIS X 5092:2008 (CAdES プロファイル)と JIS X 5093:2008 (XAdES プロファイル)が成立し発行された。長期署名プロファイルが業界標準から日本国内標準となり、e-文書法に基づく電子文書保存などの分野において利用促進の原動力となった。更に、この規格を国際的にも矛盾がないものにするため、長期署名プロファイルの ISO 標準化プロジェクトを発足し、2012 年に晴れて ISO 14533 の成立に至った。ISO 14533 は JIS 標準を元に ISO 標準を作成したケース(fast track ではない)であり、あまり一般的なケースとは言えないが、規格の内容も JIS と矛盾なく完成することができた。それを可能にした理由としては、ECOM プロファイルや JIS プロファイル作成時より情報交換を行っている ETSI とのリエゾン関係を結んだことにあると考えられる。これまで規格作成やプラグテストの実施などで協力関係を強めてきた賜物といえる。

様々な調査報告やガイドラインの作成、標準規格策定やプラグテストの実施など様々な成果を出してきた ECOM/eRAP の標準化活動は、ISO 14533 が発行されたことで 1 つの節目を迎えることになった。しかし、長期署名に関する分野は取り組むべき課題がまだ残されており、海外においても動きが活発であるため、今後も目を離すことができない。特に欧州の最近の動向では、欧州内の特別な事情を標準規格に取り入れる傾向があり、その標準規格を参照している欧州以外の国にも影響を及ぼす問題がある。日本国内での利用方法に適合しなくなる恐れもある。国際的な標準をただ利用すればよいというだけではなく、どのように国際的な標準に関わっていくのかという戦略的な視点が今後も重要である。

3.2 XAdES のプラグテスト

3.2.1 ETSI XAdES Remote Plugtest 2012 概要

2012 年 3 月 14 日から 2012 年 4 月 3 日(当初予定は 3 月 28 日までだったが延長された)にかけて ETSI 主催の XAdES Remote Plugtest 2012 [13] が開催された。XAdES Remote Plugtest 2012 は XAdES 規格(ETSI TS 102 903)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。欧州から 12 カ国と日本及びブラジルからの合計 14 カ国 23 組織(うち日本からは有限会社ラング・エッジの 1 社)が参加した。XAdES のプラグテストは毎年のように行われているが今年は欧州の標準となる Baseline Profile があった為か参加者が多かった。

表 3-1 ETSI XAdES Remote Plugtest 2012 参加登録数

登録数	国名	テスト参加数	未参加数	参加比率
5	フランス	5	0	21.70 %
6	スペイン	4	2	17.40 %
2	ハンガリ	2	0	8.70 %

登録数	国名	テスト参加数	未参加数	参加比率
2	ポーランド	2	0	8.70 %
1	**日本**	**1**	**0**	**4.35 %**
1	ドイツ	1	0	4.35 %
1	リトアニア	1	0	4.35 %
1	ベルギー	1	0	4.35 %
1	ルクセンブルク	1	0	4.35 %
1	スウェーデン	1	0	4.35 %
1	スロバキア	1	0	4.35 %
1	トルコ	1	0	4.35 %
1	英国	1	0	4.35 %
1	ブラジル	1	0	4.35 %
1	スロベニア	0	1	---
1	イタリア	0	1	---
1	オーストリア	0	1	---
合計 28	全 17 カ国 (参加 14 カ国)	合計 23 組織	合計 5 組織	---

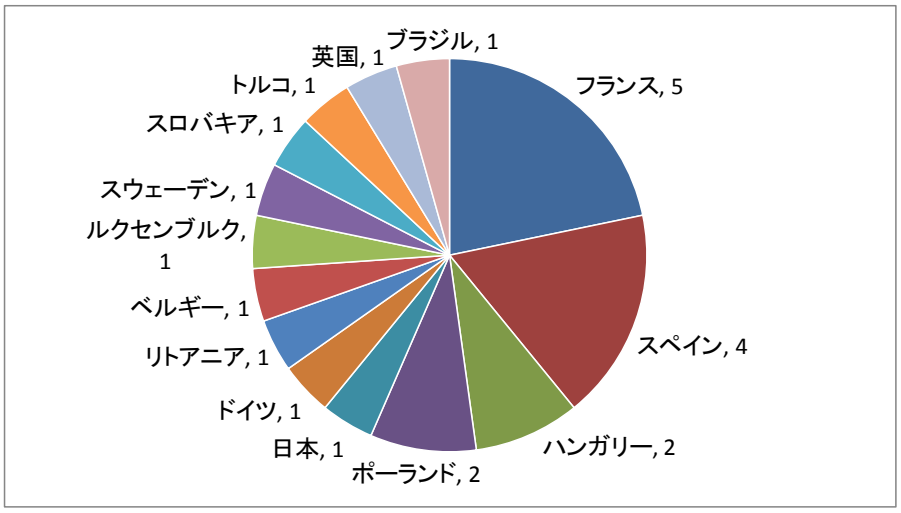


図 3-4　ETSI XAdES Remote Plugtest 2012 参加者(国別)

テストの内容は従来通りのポジティブテストとネガティブテストに加えて、新しい試みとしてアーカイブタイムスタンプを他社の XAdES に付与する署名更新(ポジティブ)テストもあった。しかし署名更新テストは、署名と検証の数が膨大になり一部参加者のみが実施したと言う状況であった。

(1)署名生成及びクロス検証テスト(ポジティブテスト)

Generation and cross-verification (a.k.a. Positive) tests.

各参加者は指定された仕様の署名ファイルを生成し、それを他の参加者がダウンロードして検証をするテスト。ポジティブテストであり正常に相互検証できることを確認する。XAdES の v1.3.2 [14](38 パターン)と v1.4.1 [15](10 パターン)と Baseline Profile(16 パターン)の大きく 3 つのケースが用意された。

(2) 検証のみのテスト（ネガティブテスト）

Only-verification (a.k.a. Negative) tests.

事前に ETSI により用意された検証に問題があるケースの署名ファイルを、各参加者がダウンロードして検証をするテスト。問題点を正しく見つけることができなければいけないネガティブテスト。XAdES の v1.3.2(26 パターン)と Baseline Profile(5 パターン)の大きく 2 つのケースが用意された。

(3) 署名更新テスト（ポジティブテスト）

Signatures Upgrade and Arbitration (a.k.a. Positive) tests.

他の参加者が生成した署名ファイルに対してタイムスタンプを付与する等の更新を行い、それを他の参加者が更にダウンロードして検証するテスト。ポジティブテストであり正常に相互検証できることを確認する。他社の署名を更新する必要があり難易度が高い。これまでは無かった新しく追加されたテストである。ケース数は参加者数の掛け算になるので膨大になるが、残念ながら参加者はそれ程多くは無かった。このテストを行なうにはもっとテスト期間を延ばさないと難しいように感じた。

XAdES は現在 JIS プロファイル(JIS X5093:2008)にも使われている v1.3.2 仕様に加えて、新しく v1.4.1/1.4.2 の仕様がある。v1.4.1/1.4.2 のテストが目的の参加者も多かったようだ。

更に今回は新しい仕様として XAdES Baseline Profile(ETSI TS 103 171)に関して力が入っていたようだ。ポジティブテスト以外にテストポータルには Baseline Profile 用のオンライン検証テスト(XAdES Baseline Profile Conformance Checker)が使えるようになっていた。Baseline Profile は今後欧州の基本プロファイルになるとのことであり、JIS プロファイルとの整合性や差異を今後明確にする必要があるだろう。

2011 年末に行われた PAdES Remote Plugtest 2011 にて日本から電話カンファレンスへの参加が難しいとの要望を出していたが、今回は Web 会議のシステム GoToWebinar[10]によりプレゼン画面の共有と PC による双方向の音声が実現された。手軽に参加できて非常に良いと感じた。

テスト結果についてはさすがに XAdES 仕様自体に関しては細かいミスがあった程度で大きな問題は無かった。ただし相変わらず参加者のレベルの違いはあり、初歩的な質問も見られた。また採用している仕様も相変わらずバラエティに富んでおり大変参考になった。その中で 1 つだけ JIS プロファイルとの差異で以下の問題があった。

・XAdES v1.3.2 におけるアーカイブタイムスタンプの検証情報保管場所

XAdES v1.3.2 ではアーカイブタイムスタンプの証明書群と検証情報群を保管する場所が XML 要素として用意されていない問題があった。この為に JIS プロファイル[16][17][18][19] ではアーカイブタイムスタンプ自体に証明書と検証情報を埋め込むことになっており ECOM 相互運用性テスト[20] に参加した日本ベンダは皆サポートしていた。今回参加した欧州の多くの実装においてアーカイブタイムスタンプの証明書群と検証情報群は署名タイムスタンプと同じ RevocationValues 要素にあるので良いとの意見があった。日本の参加者はアーカイブタイムスタ

[10] http://www.gotomeeting.com/fec/webinar

ンプへ検証情報を埋め込んでいたが欧州の参加者では 1 社のみが同様の仕様であった。この問題自体は欧州側も認識しており XAdES v1.4.1 の TimeStampValidationData 要素で解決しておりこの問題は生じない。また Baseline Profile では JIS プロファイルと同様とのことでありあくまで XAdES v1.3.2 だからとのことであった。

今回のプラグテストも従来同様事前に NDA(守秘契約)を交わした上で行われており、結果や利用したテストケースは公開されない。プラグテスト毎に日本から要望していることだが、電子署名実装普及の為にテストケース等は公開されることが望まれる。現在は公開目的よりも、仕様の確認や、参加者同士での問題が無いことの確認が主な目的になっているように思える。もちろんそれはそれで意義があることではある。特に欧州のように実装者が多様な場合には有効ではあろう。

3.2.2 XAdES v1.4.1/v1.4.2 仕様概要

(1)概要と名前空間

XML の長期署名フォーマットである XAdES の仕様は ETSI が中心となって策定している。日本では ECOM また現在は eRAP が中心となって JIS プロファイルを策定してきた。現在の JIS プロファイル(JIS X 5093:2008)は XAdES 1.3.2 をベースにしているが、XAdES 1.4.1 が既にリリースされており、更に更新された XAdES 1.4.2 も 2010 年 12 月にリリースされている。この為に JIS プロファイルもそろそろ XAdES 1.4.1/1.4.2 ベースに移行する必要がある。なお ETSI の Baseline Profile も昨年リリースされ欧州では標準化作業が進展している。ここまでの XAdES 仕様の流れを以下にまとめる。

- (2005) ETSI XAdES 1.3.1 Draft
- (2006-03) ETSI XAdES 1.3.2
- (2008-05) JIS X 5093:2008 – XAdES 1.3.2 ベース
- (2009-06) ETSI XAdES 1.4.1
- (2010-12) ETSI XAdES 1.4.2
- (2011-09) ETSI XAdES Baseline Profile

XAdES 1.3.1 の前にも仕様が存在するがほとんど使われていない為に、ここでは説明しない。また XAdES はベース仕様として XmlDsig(XML 署名)を使っているが、XAdES 1.4.1/1.4.2 においての変更は無いので説明を省略する。本章では ETSI の XAdES 1.4.1/1.4.2 仕様を簡単にまとめる。

まず XAdES 1.4.2 は仕様としては基本的に XAdES 1.4.1 と同じであると言える。XAdES 1.4.1 にあった Schema の間違いを正す等のマイナーな変更のみである。仕様書としては XAdES 1.4.2 だけを参照して問題ない。以後 XAdES 1.4.1 と書いた場合には XAdES 1.4.2 も含む。

XAdES 1.4.1 では新しい名前空間の下に XAdESv141:TimeStampValidationData と XAdESv141:ArchiveTimeStamp の 2 つの XML 要素が追加された。2 つの新要素はそれぞれ、タイムスタンプの証明書/検証情報の格納用の要素と、新しいアーカイブタイムスタンプ形式であ

る。

・名前空間　http://uri.etsi.org/01903/v1.4.1#
・新要素１　XAdESv141:TimeStampValidationData
・新要素２　XAdESv141:ArchiveTimeStamp

まず名前空間について簡単にまとめる。XAdES 1.3.2 までの仕様ではマイナーバージョンアップも含めて全ての要素の名前空間が更新されてきた。例えば XAdES 1.3.2 と 1.3.1 では以下のようになっていた。

・1.3.1 名前空間　http://uri.etsi.org/01903/v1.3.1#
・1.3.2 名前空間　http://uri.etsi.org/01903/v1.3.2#

1.3.1 と 1.3.2 の名前空間が混在することはアーカイブタイムスタンプを除き基本的にはない。それに対して 1.4.1 では新規追加された要素以外は全て 1.3.2 の名前空間をそのまま利用している。つまり 1.4.1 対応にするには XAdES 1.3.2 と 1.4.1 の両方の仕様を参照する必要がある。

・1.3.1 と 1.3.2 は全く別の名前空間
・1.4.1 の名前空間は 1.3.2 をベースに 1.4.1 を追加

これに関してはどちらのやり方が良いかと言うのはその人の立場や考え方次第と言える。実装者から見た場合には 1.4.1 のやり方が楽かもしれない。それは 1.3.2 仕様の実装部分はそのままにして、1.4.1 仕様の実装部分を追加すれば良いからだが、将来的な仕様を考えると別にしたほうが良いと言う見方もある。なお ArchiveTimeStamp 要素に関しては名前空間が異なり同じ要素名で 1.3.2 と 1.4.1 が存在しそれぞれ計算方法も異なる。少し紛らわしいので注意が必要である。

(2)XAdESv141:TimeStampValidationData

XAdES 1.4.1 で新しく追加されたタイムスタンプの検証情報を保管する XAdESv141:TimeStampValidationData について説明する。XAdES をはじめとする長期署名は基本的には「署名」＋「タイムスタンプ」(これが ES-T 形式)となる。PDF 長期署名の PAdES では「(文書)タイムスタンプ」だけで「署名」無しの仕様も可能だが、XAdES/CAdES では署名抜きでタイムスタンプだけの仕様は存在しない。

タイムスタンプの RFC3161 仕様とは「署名」の一種と言える。つまり「署名」＋「タイムスタンプ」では 2 つの「署名」があることになる。それぞれの「署名」について EE(署名者)証明書が存在(署名証明書とタイムスタンプ証明書)しており、かつトラストアンカーとなるルート証明書までの認証パス(証明書チェーン)が存在する。もし「署名」と「タイムスタンプ」で同じトラストアンカーのルート証明書を使うのであれば同じ証明書群と CRL/OCSP 等の検証情報群で良いので認証パスは 1 つだけですむ。過去の ETSI プラグテストにおいても署名証明書とタイムスタンプ証明書は同じトラストアンカーを利用していた。欧州等ではどうもこのような運用が一般

的だったようである。

一方日本においては、認証局とタイムスタンプ局が別々に認定されている経緯もあり、「署名」と「タイムスタンプ」ではトラストアンカーとなるルート証明書が通常異なる。この場合に認証パスは「署名」と「タイムスタンプ」の異なる 2 つが必要となる。この為に少なくとも日本では認証パス(と正確には認証パスに必要な検証情報群)は 2 つ格納する必要がある。ところが XAdES 1.3.2 の仕様では証明書群は CertificateValues 要素下に格納し、検証情報群は RevocationValues 要素下に格納できるだけである。かつ CertificateValues 要素と RevocationValues 要素は 1 つだけしか認められない。つまり認証パスの情報を格納する場所は 1 ヶ所しか無い。本来 CertificateValues 要素と RevocationValues 要素には「署名」に関する証明書パスと検証情報を格納することになっている。このままでは「タイムスタンプ」の証明書群と検証情報群を XML 要素として格納することができない。そこで JIS 化する際に以下のルールが定義された。

・署名タイムスタンプ(SigTS)の証明書群と検証情報群：
1)タイムスタンプトークン自身に埋め込む
2)CertificateValues 要素と RevocationValues 要素に入れる

・アーカイブタイムスタンプ(ArcTS)の証明書群と検証情報群：
1)タイムスタンプトークン自身に埋め込む

正確にはタイムスタンプトークンのどこに証明書群と検証情報群を埋め込むかによって更に種類は分かれるが、ここの本題では無いので省略する。JIS プロファイルでは署名タイムスタンプについては、CertificateValues 要素と RevocationValues 要素に関しては意味を広義にとり利用しても良いことになっている。一方でアーカイブタイムスタンプはその時刻が常に RevocationValues 要素に埋め込まれた検証情報群の発行日よりも後になるのでポリシ次第ではあるが通常利用することが難しいのでタイムスタンプトークン自身に埋め込むしかなかった。JIS においてはこの仕様で問題はなくなったが、証明書群や検証情報群を「タイムスタンプトークン自身に埋め込む」ことについては以下の意見があった。

1)XML だけでなく ASN.1/DER(BER)の操作が必要になり難しい
2)取得したタイムスタンプトークンはそのまま利用すべき
3)XML の利点である可読性の面から望ましくない
4)CertificateValues/RevocationValues は署名証明書のみにすべき

この為に「タイムスタンプ」専用の証明書群や検証情報群の保存場所として XAdESv141:TimeStampValidationData が新たに導入されたと考えられる。TimeStampValidationData 要素の下に XAdES 1.3.2 の CertificateValues 要素と RevocationValues 要素を持ち、タイムスタンプ用の証明書群と検証情報群を格納することができる。新たに導入された TimeStampValidationData 要素を利用できるのは SignatureTimeStamp 要素、RefsOnlyTimeStamp 要素、SigAndRefsTimeStamp 要素、ArchiveTimeStamp 要素の各

タイムスタンプとなっている。TimeStampValidationData 要素は URI 属性で情報を保持しているタイムスタンプ要素の指定が可能(オプション)となっている。なお XAdES 1.4.1 の Schema ではこの URI 属性が"UR"と間違って書かれていた為に XAdES 1.4.2 で正しく訂正されている。なお UnsignedSignatureProperties 要素の下にはもともと任意の要素を入れて構わない仕様になっていた。

(3)XAdESv141:ArchiveTimeStamp

XAdESv141:ArchiveTimeStamp 要素は XAdES 1.3.2 と同じくアーカイブタイムスタンプであるが、計算方法が XAdES 1.3.2 とは異なる為に互換性がない。この為に名前空間で区別して利用する必要がある。

XAdESv132:ArchiveTimeStamp の計算時では UnsignedSignatureProperties 要素の下の「決められた要素を順番に取得して連結して行く仕様」となっていた。この決められた要素とは全て XAdES 1.3.2 で定義された SignatureTimeStamp 要素や CertificateValues 要素等であり、XAdES 1.4.1 で追加された XAdESv141:TimeStampValidationData 要素が含まれていない。この仕様では XAdESv141:TimeStampValidationData 要素の下が保護できない。XAdES 1.4.1 で追加された XAdESv141:ArchiveTimeStamp の計算方法では「UnsignedSignatureProperties 要素の下を全て対象とする仕様」となっている。

XAdESv141:ArchiveTimeStamp ではもう 1 点 ds:Object の扱いについても変更があった。XAdESv132:ArchiveTimeStamp の仕様では「Reference 要素で参照されていない ds:Object」が対象だったが、XAdESv141:ArchiveTimeStamp の仕様では「全ての ds:Object」が対象となっている。正確には「XAdES の要素である QualifyingProperties を持つ ds:Object は除外する」と言うルールがあるがこれは XAdES 1.3.2 と XAdES 1.4.1 では共通であり変更は無い。差異部分のみリストアップすると以下のようになる。

1：XAdES 1.3.2 におけるアーカイブタイムスタンプ仕様(一部)
　1－1：UnsignedSignatureProperties 要素の下の決められた要素を連結
　1－2：Reference 参照されていない全ての ds:Objecct を連結 ※

2：XAdES 1.4.1/1.4.2 におけるアーカイブタイムスタンプ仕様(一部)
　2－1：UnsignedSignatureProperties 要素の下の全ての要素を連結
　2－2：Reference 参照有無に関係無く全ての ds:Objecct を連結 ※
　※ ただし XAdES の QualifyingProperties を持つ ds:Object は除外する。

計算方法が 2 箇所異なるので、当然計算結果のハッシュ値も XAdES 1.3.2 と XAdES 1.4.1 では異なり一致しない。なお XAdES 1.4.1 の Schema では XAdESv141:ArchiveTimeStampV2 と書かれていたがこれは誤りであり、V2 が無い XAdESv141:ArchiveTimeStamp が正しい要素名となっている。これは XAdES 1.4.2 で訂正された。

表 3-2 XAdES 1.4.1/1.4.2 の構造例

<ds:Signature>	
<ds:SignedInfo /> <ds:SignatureValue /> <ds:KeyInfo />	
<ds:Object> <xa:QualifyingProperties>	
<xa:SignedProperties>...</xa:SignedProperties>	署名対象プロパティ領域
<xa:UnsignedProperties> <xa:UnsignedSignatureProperties>	非署名プロパティ領域開始
<xa:SignatureTimeStamp ID="SigTS" />	署名タイムスタンプ
<xa141:TimeStampValidationData RI="#SigTS"> <xa:CertificateValues> SigTS の TSA 証明書の認証パス証明書群用 </xa:CertificateValues> <xa:RevocationValues> SigTS の TSA 証明書の検証情報群用 </xa:RevocationValues> </xa141:TimeStampValidationData>	署名タイムスタンプの認証パス用の証明書群と検証情報群の格納(XAdES 1.4.1)
<xa:CertificateValues> 署名証明書の認証パス証明書群用 </xa:CertificateValues> <xa:RevocationValues> 署名証明書の検証情報用 </xa:RevocationValues>	署名証明書の認証パス用の証明書群と検証情報群の格納
<xa141:ArchiveTimeStamp ID="ArcTS1" />	アーカイブタイムスタンプ 1
<xa141:TimeStampValidationData URI="#ArcTS1"> <xa:CertificateValues> ArcTS1 の TSA 証明書の認証パス証明書群用 </xa:CertificateValues> <xa:RevocationValues> ArcTS1 の TSA 証明書の検証情報用 </xa:RevocationValues> </xa141:TimeStampValidationData>	アーカイブタイムスタンプの認証パス用の証明書群と検証情報群の格納(XAdES 1.4.1)
<xa141:ArchiveTimeStamp ID="ArcTS2" />	アーカイブタイムスタンプ 2
</xa:UnsignedSignatureProperties> </xa:UnsignedProperties>	非署名プロパティ領域終了
</xa:QualifyingProperties> </ds:Object>	
</ds:Signature>	

3.2.3 まとめ

XAdES仕様もv1.4.1/1.4.2によりタイムスタンプの認証パスの証明書群と検証情報群の保管場所の問題もクリアされ、長期署名として大きな問題は解決されたと考えられる。JIS プロファイルも XAdES v1.4.1/1.4.2 に対応した仕様の更新が期待される。また複数署名や複数署名対象等、日本国内における実際の運用面に係る仕様の標準化やガイドライン作成(一部では作成されているが[21]、拡充が必要)も、今後の普及の為に必要だろう。

ETSI プラグテストは、NDA・料金支払い手順・英語での情報交換等で事務的技術的なハード

ルが高い。今後日本国内向けに XAdES v1.4.1/1.4.2 に対応した JIS プロファイルを前提としたプラグテストの実施が期待される。しかしながら日本国内で長期署名のプラグテストを行うには以下の問題点や課題がある。

①試験用 PKI 環境(認証局と証明書発行/タイムスタンプサーバ/OCSP サーバ)が必要。
②結果更新と管理用ポータルサイトやメーリングリスト等インフラの用意も必要。
③試験データの検討と用意の為に仕様に詳しい技術ボランティアが必要。

これらの問題点や課題は XAdES に限らず CAdES や PAdES のプラグテストを行う場合でも同じである。①と②に関しては XAdES/CAdES/PAdES 共通に利用ができるので今後整備が期待される。特に①の試験用 PKI 環境を整備運用して公開することができれば新たな実装者にとっても役立つ環境となるだろう。

プラグテストによる異なるベンダ間の相互運用性を確認することは、長期署名の利用者や運用者の安心にも繋がる。今後 XAdES 仕様に関しても、ETSI のプラグテストへの紹介や参加はもちろん、日本国内のプラグテストの実施もベンダから強く期待されている。

3.3 ASiC プラグテスト参加報告

2012 年 11 月 19 日から 2012 年 12 月 21 日まで、ETSI 主催の ASiC プラグテストに参加したので状況等について報告する。

3.3.1 ASiC プラグテストの目的

ASiC[8] は、電子記録等のコンテンツと、そのコンテンツを保護する署名等のデータ及びこれらの管理を容易にするためのメタデータ等を一体化するパッケージ構造に関する署名フォーマットの仕様であり、ETSI により 2011 年 4 月に仕様化され、その後、2012 年 2 月に改定が行われた。今回のプラグテストは、この ASiC 技術仕様(ETSI TS 102 918 V1.2.1)に関する相互運用性評価の場として設けられた。

ETSI はこれまで、CAdES、XAdES、PAdES 等の、長期署名プロファイルに関する相互運用性評価としてプラグテストを進めてきた。ASiC は、その内部に電子署名やタイムスタンプを含むものの、検証すべき観点については従来とは大きく異なっている。これまでは、署名データの生成・検証が主な試験項目とされたが、ASiC ではパッケージ構造のフォーマット要件に関する相互運用性が重視された。

ASiC の仕様制定とプラグテストの実施に至る背景としては以下が考えられる。

・コンテンツ流通に耐える、安全かつ簡便な手段の確立に対するニーズの高まり
・ODF[22] 等の標準ドキュメントフォーマットの普及

欧州では、各国政府・自治体の発行するドキュメントを他国・他自治体においても受け入れ可能にする相互運用性確保のニーズが高く、ドキュメント交換を安全に行うための技術確立が切望

されている。ASiC は電子署名やタイムスタンプがもたらす否認防止、改ざん検知、存在証明等により、ドキュメント交換時の成りすましや改ざん等の不正リスクを抑止する。また、ASiC のコンテナフォーマットの原型である OCF[23] は、ODF 等、既に幾つかの欧州の政府・自治体等の公共機関において採用されているため[24][25] 、ASiC はこれらのドキュメントフォーマットとの親和性が高く、最小のインパクトで署名等による安全性を提供できる。

3.3.2 ASiC 仕様概要

ASiC の技術仕様である、ETSI TS 102 918 V1.2.1 について概説する。

(1) コンテナ構造

ASiC は、いくつかの署名対象データと電子署名やタイムスタンプを関連付けし、これを ZIP ファイル[26]にして格納する。(図 3-5)

ASiC に格納できる電子署名やタイムスタンプについては以下に限られる。

・CAdES [5]
・XAdES [6]
・タイムスタンプトークン[27]

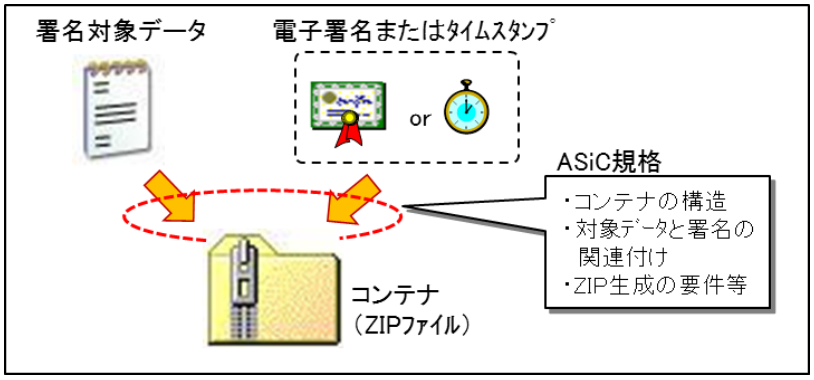


図 3-5 ASiC よるコンテナ化のイメージ

なお、今回のプラグテストでは CAdES 及び XAdES については、-BES 及び-EPES プロファイルのみが評価対象とされた。長期保管向けへの適用については今後の課題となっている。

ASiC 自体はジェネリックな規定であり、ドキュメントデータ、XML 構造化データ、スプレッドシート、マルチメディアコンテンツ等の多様なデータを署名対象として扱うことができる。更に、特定アプリケーションへの対応として、OCF、ODF、UCF[28] 等の既存ドキュメントフォーマットとの互換性維持のための個別規定が設けられている。

(2) コンテナタイプ

ASiC のコンテナ構造については、大別して以下の 2 種類がある。(図 3-6)

(a) ASiC-S (simple form)

1 つの署名対象データオブジェクトと、それに関連付けられる署名構造データを格納するコンテナフォーマット。格納できる署名は、CAdES、XAdES 及びタイムスタンプトークンのうちの 1 種類のみで、更に、CAdES またはタイムスタンプトークンの場合は、格納可能な署名やタイムスタンプは 1 個に限られる。

(b) ASiC-E (extended form)

複数の署名対象データを格納できるコンテナフォーマットで、その各署名対象データに対し、1 つまたは複数の署名が関連付けられているもの。署名やタイムスタンプの格納数の制約はない。CAdES やタイムスタンプトークンの適用において、複数の署名対象データを纏めて扱えるようにするため、XML 署名の Manifest 要素に類似の "ASiCManifest" と呼ばれる XML データを導入している。この他に、メタデータのオブジェクトも署名対象と含めることができる。更に、ASiC コンテナ生成後の、新たな署名対象データと署名の追加格納もできる。このほか、XAdES の適用に関しては OCF、ODF、UCF との整合性が考慮されている。

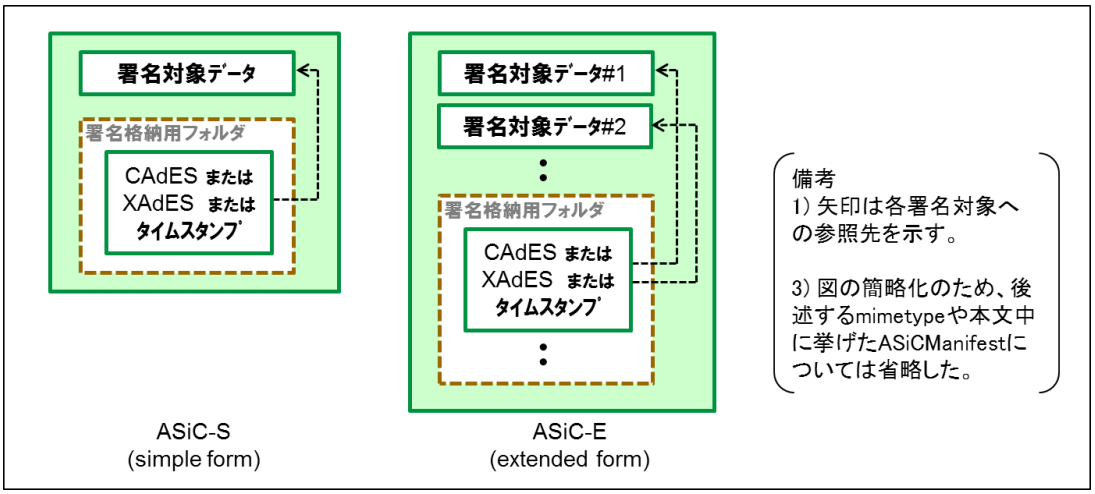


図 3-6　ASiC のコンテナタイプのイメージ図

(3) ASiC の基本構成要素

コンテナを構成する主要なフォルダやオブジェクトには以下がある。(ASiC-S,-E 共通)

(a) "root" フォルダ

ZIP 化の対象となる、コンテナ全体を表す親フォルダ。

(b) "META-INF" フォルダ

"root" フォルダ直下に置かれる、コンテンツのメタデータ格納用フォルダ。ASiC では署名やその管理データの格納に用いられる。

(c) "mimetype" オブジェクト

"root" フォルダ直下に置かれる、そのコンテナの mime タイプ情報を示すオブジェクト。実体は拡張子の付かないプレーンテキストのファイルで、ASiC のジェネリックな用法として、コンテナタイプを特定する以下の文字列が格納される。

・"application/vnd.etsi.asic-s+zip" (ASiC-S の場合)
・"application/vnd.etsi.asic-e+zip" (ASiC-E の場合)

なお、ASiC-E の拡張として OCF、 ODF、 UCF を扱う場合は、それらの元の mime タイプが引き継がれる。

(4) その他 ASiC 実装上の規定

(a) ZIP の適用

ZIP 適用上の要求事項は以下のとおり。

・上記(3)(c)の mimetype オブジェクトは ZIP 格納順の第一番目に置かれること。
・ZIP の拡張フィールドは使用しないこと。
・mimetype オブジェクトはプレーンテキストであり、圧縮しないこと。
(コンテナ全体を解凍しなくても、mime タイプを参照できる必要があるため)
・ZIP の先頭からの 4 オクテットの値は、"50 4B 03 04" (ローカルヘッダを表すシグネチャ値)とすること。
・ZIP ヘッダのコメントフィールドにメディアタイプ(コンテナタイプを特定する mime タイプ)を格納すること。(オプション)

(b) ASiC コンテナファイルの拡張子

ジェネリックな用法として、コンテナファイルの拡張子は以下とすること。

・".asics" (ASiC-S の場合)
・".asice" (ASiC-E の場合)

なお、上記のほか、".scs"、".sce" 等の短縮形式や ".zip" の使用が許容されている。更に、OCF、UCF、ODF 等を扱う場合は、元のドキュメントの拡張子を用いることも規定されている。

(c) 署名及びタイムスタンプのファイル名や格納方法

CAdES、XAdES 及びタイムスタンプトークンは、"META-INF"フォルダ直下に置くこと。ジェネリックな用法として、ファイル名は以下の命名規則に従うこと。

【ASiC-S の場合】

・"META-INF/signature.p7s" （CAdES の場合）

・"META-INF/signatures.xml" （XAdES の場合）

・"META-INF/timestamp.tst" （タイムスタンプトークンの場合）

【ASiC-E の場合】

・"META-INF/*signature*.p7s" （CAdES の場合）

・"META-INF/*signatures*.xml" （XAdES の場合）

・"META/INF/*timestamp*.tst" （タイムスタンプトークンの場合）

("*" の部分には識別のための任意の文字列を付加することができる。)

なお、CAdES やタイムスタンプトークンを ASiC-E に適用する場合は、署名対象データと署名との関連付けを定義するための以下のオブジェクトを置くこと。

・"META-INF/ASiCManifest*.xml"

("*"の部分には識別のための任意の文字列を付加することができる。)

(d) XAdES の XML データ構造のルートの要素名

ASiC に XAdES を適用する場合、XAdES を包含する XML データ構造のルート要素名については以下とすること。

・<asic:XAdESSignatures>要素 （ASiC のジェネリックな用法の場合）

・<document-signatures>要素 （ODF の場合）

・<signatures>要素 （OCF の場合）

(e) META-INF ディレクトリ配下への署名データ以外のオブジェクトの格納

ODF 等への拡張利用として、META-INF ディレクトリ配下に以下のオブジェクトを格納することができる。

・"META-INF/container.xml"及び"META-INF/metadata.xml" （OCF の場合）

・"META-INF/manifest.xml" （ODF の場合）

(5) ASiC のデータ構造のサンプル

以下に、ASiC-S 及び ASiC-E のコンテナ構造と、その実装イメージの例を図示する。

【ASiC-S の例】

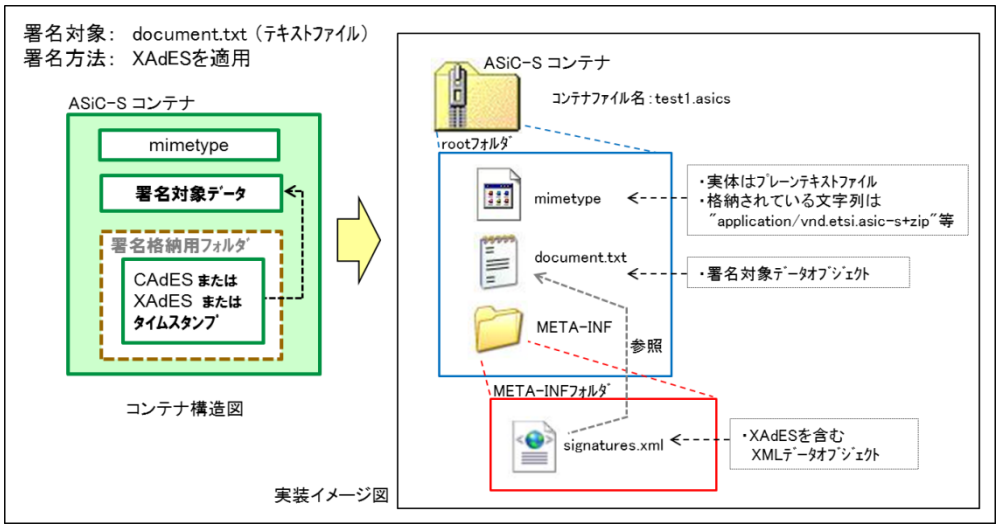


図 3-7　ASiC-S（XAdES 適用）の実装例

【ASiC-E の例】

(a) CAdES またはタイムスタンプを用いる場合

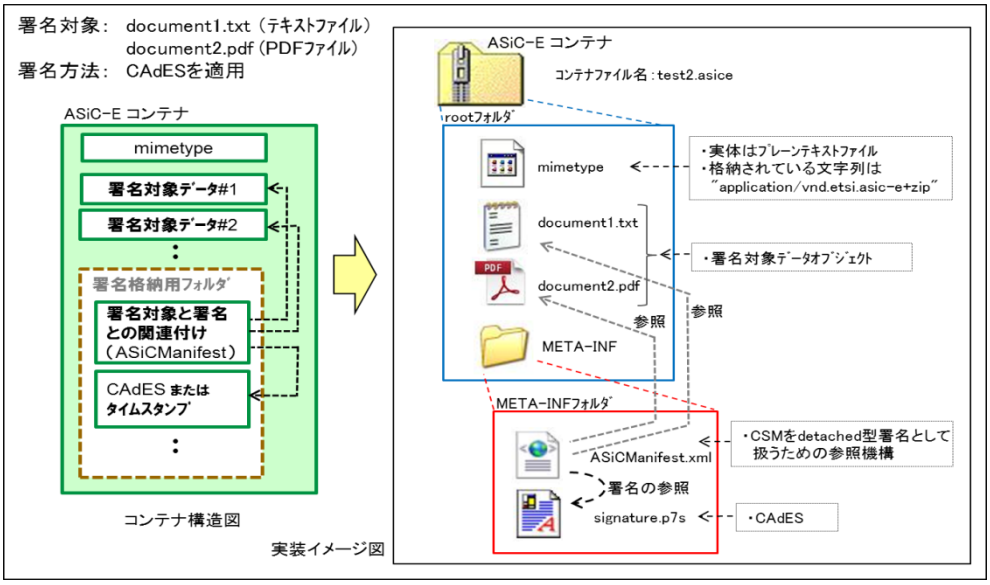


図 3-8　ASiC-E（CAdES 適用）実装例

(b)XAdES を用いる場合

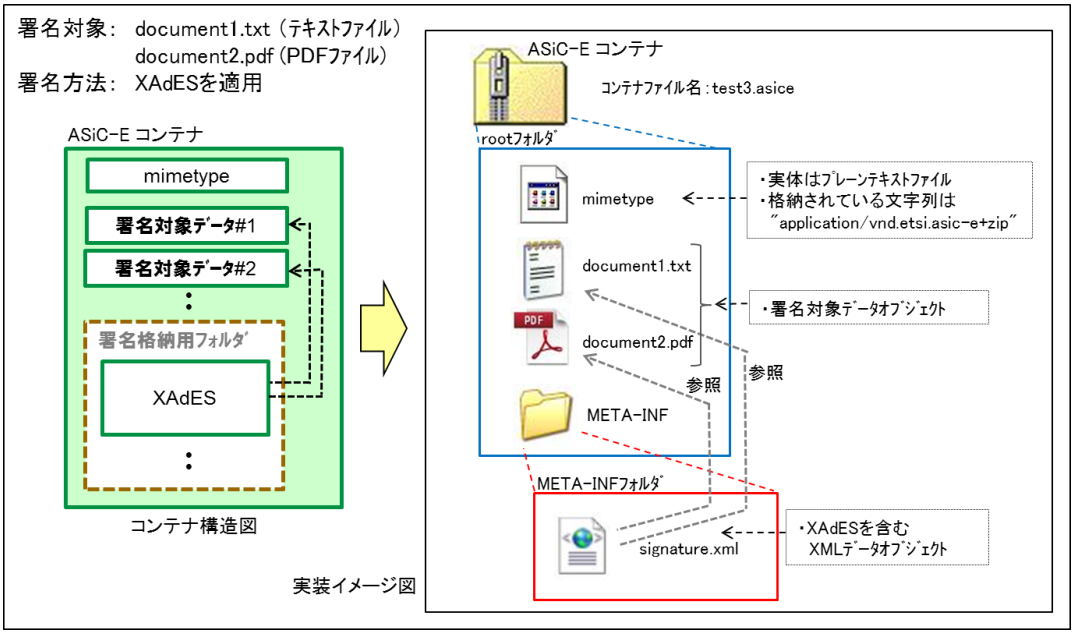


図 3-9　ASiC-E(XAdES 適用)実装例

3.3.3　ASiC プラグテスト状況

今回参加した ASiC プラグテストの実施状況等について以下に記す。

(1) 試験内容

ASiC の相互運用性評価項目に関しては、ETSI が定めるテストケースの規定がある[29]。今回は、この中から主要なテストケースが実施された。検証の観点は以下の 3 つであった。

- 形式検証(CS: Container Structure)：フォーマットの正しさを検証
- 意味検証(SC: Syntactical Conformance)：主に META-INF フォルダの用法に関する検証
- 署名検証(STV: Signature Time-stamp token Value)：署名とタイムスタンプの検証

試験は、これまで同様リモートにより行われた。試験の種類については、従来同様、「ポジティブテスト」と「ネガティブテスト」(後述)の 2 種類が設けられた。ただし、従来のプラグテストが、長期署名プロファイルの仕様に準拠するよう各社が開発した「署名エンジン」に対する試験であったのに対し、今回は、ETSI 側から指示されたコンテナ生成条件に従って ASiC 準拠のコンテナを生成し、またこれを検証する、「コンテナ生成・検証エンジン」に対する試験であった点が大きく異なる。以下にこれら 2 種類の試験内容について示す。

(a) Generation and cross-verification tests. (通称：ポジティブテスト)

ETSI が署名対象データ及び、コンテナ内に格納すべきオブジェクト項目を出題し、各参加者はその要件に応える ASiC データを生成する。生成した ASiC データは他の参加者によって有効性が検証される。(試験項目数：53 件)

本試験での主なフォーマットのバリエーション項目を以下に示す。

表 3-3　生成フォーマットの主なバリエーション項目

観点	パターン
ASiC タイプ	ASiC-S 及び ASiC-E
署名構造	CAdES、XAdES、タイムスタンプ(RFC3161 準拠)
mime タイプ設定方法	mimetype オブジェクト利用、ZIP ヘッダー利用
署名数	1 個の場合 及び 複数の場合
署名対象データ数	1 個の場合 及び 複数の場合(ASiCManifest の適用)
ASiC-E の拡張利用	ODF、OCF、UCF 等

参考として、今回出題された試験項目の一例(簡約)を下図に示す。

テストケース #A は　以下のプロパティを含む

・AsicDataObject

・AsicMimeType

・AsicAssociatedXades

本テストケースは、そのコンテナフォーマットが mimetype によって特定できる場合(TS 119 164-2 TC/ASiC-S/CS/2)についての試験である。

具体的なコンテンツとその署名要件は以下のとおり。

```
<SignatureRequest>
    <AsicSimpleContainer>
        <AsicFileExt>.zip</AsicFileExt>
        <AsicDataObject File="../../Data/document.txt"/>
        <AsicMimeType Value="application/vnd.etsi.asic-s+zip"/>
        <AsicAssociatedXades File="../../Data/signatures.xml"/>
    </AsicSimpleContainer>
    <Documentation>
        This test case tests if the container if the container format is identifiable
        using mimetype (TS 119 164-2 TC/ASiC-S/CS/2)
    </Documentation>
</SignatureRequest>
```

図 3-10　ポジティブテストの試験項目例

一般に、プラグテストでの検証失敗の要因については、生成側実装、検証側実装及び仕様上の問題の 3 つが考えられるが、それらについては、検証結果に添付されるエラー情報のほか、参加メンバとのメーリングリスト上での情報交換により原因分析が図られる。仕様やその解釈に問題がある場合は、メーリングリストや、期間内に開催されるミーティングで問題提起することで議論がなされ、期間内に解決できる場合は、仕様変更やその解釈の再定義がなされた暫定解に従いプラグテストが継続される。一方、期間内での解決が難しい問題は課題として棚上

げされ、プラグテスト終了後に ETSI メンバで検討される。

(b) Only-verification tests. (通称：ネガティブテスト)

ETSI が作成した ASiC データに対し、各参加者の検証ツールでそのコンテナの仕様適合の成否を検証する。参加者にはその検証成否の要因を正しく検出することが求められる。今回は、署名の正当性と証明書の有効性確認に関する項目のみが実施された。(試験項目数：15 件)

(2) 参加状況

今回のプラグテストには、ETSI を除き 16 団体(企業、大学、政府機関等)が参加した。日本からは NTT セキュアプラットフォーム研究所が参加した。国別参加状況を以下に示す。

表 3-4　署名フォーマット別参加団体数

登録数	国名	テスト参加数				参加比率 (全体比較)
		全体	署名フォーマット別			
			CAdES	TST	XAdES	
2	フランス	2	2	0	2	14.29 %
2	イタリア	2	1	1	1	14.29 %
2	ハンガリ	2	1	1	1	14.29 %
1	チェコ	1	1	1	1	7.14 %
1	ポーランド	1	1	1	1	7.14 %
1	リトアニア	1	1	1	1	7.14 %
1	スペイン	1	1	0	1	7.14 %
1	スロバキア	1	1	1	0	7.14 %
1	日本	1	0	1	1	7.14 %
1	その他(連合体)	1	1	0	1	7.14 %
1	エストニア	1	0	0	1	7.14 %
1	オーストリア	0	0	0	0	---
1	トルコ	0	0	0	0	---
合計 16	全 12 カ国 (うち参加 10 カ国)	合計 14 組織	10 組織	7 組織	11 組織	---

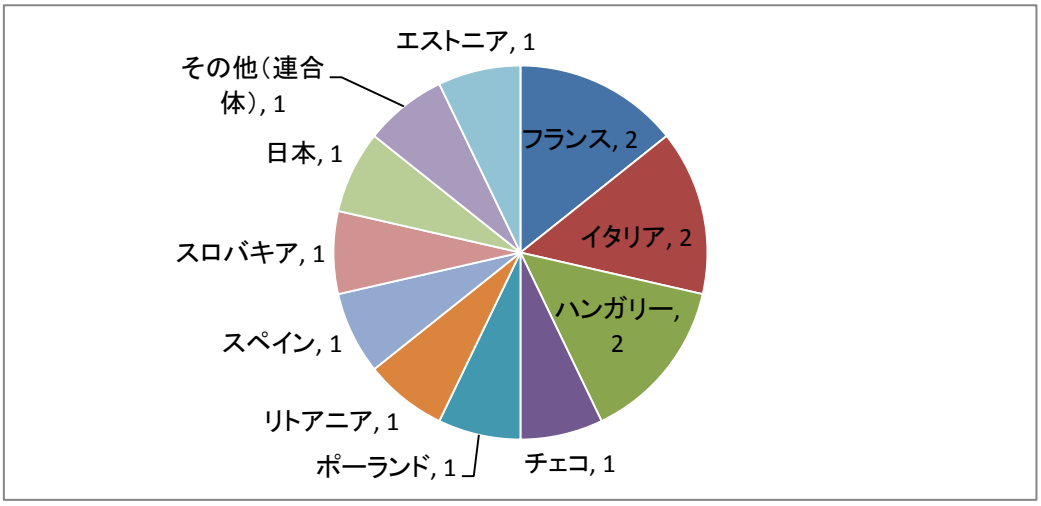


図 3-11　全体参加状況

(3) 相互運用性評価結果

本プラグテストでの試験項目(大分類別)の結果を下表に示す。ポジティブテストでは、全ての大分類において、80%を超える試験成功率を達成した。ASiC-S、-E を纏めた ASiC 全体での試験成功率は 92.9%であった。ネガティブテストについては検証実施件数が少ないものの、100%の検出率となった。なお、試験項目単位での結果については別途 ETSI から報告書として公開されると思われるので、そちらを参照願いたい。

表 3-5　ASiC-S 評価結果

			署名別			全体
			CAdES	TST	XAdES	
ポジティブテスト (25 項目)	形式検証＋意味検証	試験項目数	6	6	6	18
		登録数	42	36	47	125
		検証実施数	257	196	310	763
		検証成功数	242	196	279	717
		成功率	**94.2%**	**100.0%**	**90.0%**	**94.0%**
	署名試験	試験項目数	3	1	3	7
		登録数	15	6	19	40
		検証実施数	80	32	115	227
		検証成功数	74	32	93	199
		成功率	**92.5%**	**100.0%**	**80.9%**	**87.7%**
ネガティブテスト (7 項目)		試験項目数	3	1	3	7
		検証実施数	10	5	15	30
		検証成功数	10	5	15	30
		成功率	**100.0%**	**100.0%**	**100.0%**	**100.0%**

(ネガティブテストについては、検証の失敗をもって成功とみなす。)

表 3-6　ASiC-E 評価結果

			署名別			全体
			CAdES	TST	XAdES	
ポジティブテスト (28 項目)	形式検証＋意味検証	試験項目数	6	6	9	21
		登録数	30	25	49	104
		検証実施数	141	125	274	540
		検証成功数	132	118	264	514
		成功率	**93.6%**	**94.4%**	**96.4%**	**95.2%**
	署名試験	試験項目数	3	1	3	7
		登録数	10	4	12	26
		検証実施数	36	20	53	109
		検証成功数	31	17	45	93
		成功率	**86.1%**	**85.0%**	**84.9%**	**85.3%**
ネガティブテスト (8 項目)		試験項目数	4	1	3	8
		検証実施数	10	4	11	25
		検証成功数	10	4	11	25
		成功率	**100.0%**	**100.0%**	**100.0%**	**100.0%**

(ネガティブテストについては、検証の失敗をもって成功とみなす。)

(4) 技術課題等

本プラグテストで指摘された課題項目のうち、主なものを下表に示す。なお、幾つかの項目については、仕様改定としてフィードバックされる可能性がある。(表中のフィードバック案は、プラグテスト期間内に参加者及び ETSI メンバ等から示された意見の集約であり、標準化会議等で正式に提案されたものではない。またその規格の改定を保証するものではない。)

表 3-7　ASiC プラグテストで指摘された課題項目

項番	課題内容	フィードバック案
1	META-INF のファイル名表記について、フォルダ名の"META-INF" 、ファイル名の "manifest.xml"、"container.xml"、"metadata.xml" の大文字小文字の用法が不明確。	"META-INF" は全部大文字で、"manifest.xml"、"container.xml"、"metadata.xml" は全部小文字と明示的に規定する。
2	XAdES 署名での ds:Reference の URI 表記について、現状の Annex 6 の記述があいまい。	A.6 は、ODF に対する整合性確保を目的として書かれたもの。A.6 の ODF への直接参照の用法ルールの修正と、ASiCManifest のための互換性ルールの追記を行う。
3	XAdES 署名を root の子要素として生成した場合の、正規化での namespace 問題 【意見 1】: 署名は、署名対象データやその利用についてのコンテキストを考慮したものになっているべき。 【意見 2】: ZIP の解凍は署名の検証後にされるべきで、解凍処理と個々の署名検証が独立して行える自由度を確保すべき。	exclusive canonicalization 適用の利点について追記する。(推奨とする可能性あり)

項番	課題内容	フィードバック案
4	ZIP コメントフィールドについて、6.2.1 の 3)の "the type of content within the container" の表現が 混乱を招くので修正が必要。(関連として、7.2.4 も要修正) 現行の 6.2.1 の 3) 3) The comment field in the ZIP header may be used to identify the type of content within the container. If this field is present, it should be set with "mimetype=" followed by the mime type defined above.	6.2.1 修正案： 3) The comment field in the ZIP header may be used to identify the type of content within the container as a hint for the application. If this field is present, it should be set with "mimetype=" followed by the appropriate mime type defined above. 4) When the file extension is set according to point 1) above and the container format complies with an external specification the Mime type should be set accordingly, as applicable, instead of the Mime type specified in point 2). (上記 3)は修正、4)は追加)
5	ASiC-E(CAdES またはタイムスタンプの場合)の mimetype オブジェクトの内容について、対象となるデータの mime タイプ(例 "text/plain" 等)を設定すべきか、あるいは、仕様に規定の、"application/vnd.etsi.asic-e+zip"とすべきか? 仕様(6.3.1 の 2))も、"should" とあり、自由度が認められているようにも解釈できるのも問題。 mimetype は、コンテナの中身ではなく、そのコンテナのフォーマットを識別する目的で用いるべきである。(メーリングリスト上の議論では、mimetype には、コンテナに格納される中身のファイルの mime タイプではなく、 ASIC-E コンテナの mime タイプを設定するべき、との案に各社賛成となった。)	6.3.1 修正案： 6.3 Detailed format for ASiC-E with CAdES and Time Stamp Tokens 6.3.1 Media type identification 2) Mime type "application/vnd.etsi.asic-e+zip" mime type shall be used to identify the format of this container. 今回は、CAdES またはタイムスタンプの ASiC-E についてのみ修正。(XAdES については、ODF 等の個別の規定があるため、一律に定められない。)ODF 等の拡張型との整合性確保については、今後検討される可能性がある。

3.3.4 ASiC に関する取り組みと今後の予定

(1) 長期保管対応

プラグテスト期間中、参加者から ASiC の長期保管に向けた仕様制定を求める意見が多く寄せられた。これに対し ETSI からは、①ASiC-S 及び ASiC-E のコンテナタイプを踏襲し、-BES, -EPES のみの署名プロファイルの制限を廃して、-T, -A 等を許容する方式と、②長期保管用のコンテナタイプを新たに設ける方式(“ASiC-A”と呼ばれる)の 2 案について、現在検討が進められているとの回答があった。

(2) e-Invoicing Profile 関連項目

ETSI 及び CEN(European Committee for Standardisation) の電子署名に関する工程表[30]によれば、2013 年内に e-Invoicing Profile に関する要件が他の長期署名フォーマットと同様に制定される予定になっている。仕様への直接的な影響は不明であるが、署名対象データ及び署名の追加や、その際のカウンタ署名や並列署名の生成・検証処理に関する相互運用性評価が試験項目として必要になると考えられる。

(3) ケース管理用基本データ構造としての活用

本報告書「第 1 部第 3 章　パッケージ構造」で報告したように、ASiC はケース管理の基本データ構造として活用できる可能性が高い。しかしながら、多段のコンテナ構造の取扱いや、保全

対象データの追加変更と、それに伴う署名の追加や、上記(1)の長期保管対応等、解決すべき多くの課題が残されており、今後も継続的な検討が必要となる。

3.4 ETSI/TC ESI の動向

現在、ETSI /電子署名基盤技術委員会(TC ESI)は EC 電子署名指令 460(M/460)[31] 及び新たな EC 電子署名規制[32] 対応の取り組みを行っている。以下、委員会活動の概要を報告する。

EC 電子署名指令 460 対応のフェーズ 1(2010～2012 年)は新たな枠組みの策定とこれまでの懸案事項の解決、フェーズ 2(2012 年～)は新たな枠組みに従った標準の策定と実装を行う。フェーズ 2 は ETSI と欧州標準化委員会(以下“CEN”とする)の役割分担を考慮して次のように分けられた。

・フェーズ 2a　新たな枠組みに関する ETSI と CEN の調整領域(特に暗号関係が重複している)
・フェーズ 2b　主として CEN が扱う領域(署名生成デバイスなど)
・フェーズ 2c　主として ETSI が扱う領域。パート A とパート B に分けられる。
　パート A　優先度の高いテーマ(署名生成・検証、TSP(Trusted Service Provider))
　パート B　それ例外のテーマ(REM(電子書留)等のトラステッドアプリケーションサービス、適合性試験・相互運用性試験(Plugtest))

一方、EC 電子署名規制(電子識別(electronic identification)及び欧州内市場における電子取引の信頼サービス(trust services for electronic transactions)の規制)に関する提案が 2012 年 6 月 4 日に欧州議会で採択された。これに伴う電子識別及び信頼サービスのための新しいフレームワークの要点は次の通りである。

・国境を越えた相互認識と電子識別の受け入れを確認する。
・法的効果と電子署名で強化した現在の規則を含む、電子シール、タイムスタンプ、電子文書の受入れ、電子納品、ウェブサイトの認証のための法的枠組みを提供するサービスを信頼するよう相互承認を与える。

この背景には、実際問題として国を超えて ID や電子文書が流通していないという現実があった。

3.4.1 適格電子シール

電子シールはいわゆる職印に相当するものであり、新たな EC 電子署名規制の第 28 条から第 31 条では、法人(regal person)を対象とした適格電子シール (qualified electronic seals)の法的効力(真正な成立の推定)、電子シール用適格証明書の要件、適格署名生成デバイスの要件、保証及び保証付きデバイスのリスト公開、並びに適格電子シールの検証と保存について定めている。

3.4.2 適格タイムスタンプ

新たなEC電子署名規制33条では、適格タイムスタンプ（qualified electronic time stamps）の法的効力(時刻の確実性の推定)及び適格タイムスタンプの要件について定めている。

3.4.3 電子文書の受け入れ

更に、新たな EC 電子署名規制 34 条では、適格電子署名または適格電子シールを使用して署名された自動変更できない電子文書について真正な成立が推定されるとし、公共サービスにおいて元の文書または謄本の提供が必要とされる場合、加盟国の国内法に従って認定されたオリジナルまたはコピーの電子文書は、追加要件なしで、他の加盟国に受け入れなければならないとしている。

3.4.4 トラストリスト

トラストリストは、各国の管理(スーパーバイズ)機関が各々発行する信頼できる認証局等のサービスのリストである。現時点での主な論点を以下に述べる。

(a)マルチトラストモデル

2012 年 2 月に開催された EU-US 電子署名ワークショップで課題として挙げられた EU の TSL(Trusted Service Provider List)と米国製品(Adobe、Microsoft)に組み込まれているトラステトリスト[33][34] との整合化課題を受けて、トラストリストの構成は、それぞれ既に実績があることから、当面は、EU、Microsoft、Adobe の、マルチトラストモデルで考えて行くこととなった。

(b)TSL の長期保存

TSL の長期保存問題に関して議論となったが、TSL に限らず、長期保存におけるトラストアンカー問題は存在するので、TSL 固有の検証要件と、長期保存問題は分けて考えることになり、Trusted List Lifecycle model の策定が必要との結論になった。

(c)トラストリスト署名検証の関係

署名検証のモデルとして図 3-12 に示すモデルを想定することとなった。ここで、SVA は DA からの制約(constraint)に従って動作し、SVA にどのような制約を与えるかは、ローカル環境、法的要件、署名の特性等によって異なる。文書の種類や国によっても異なる。この制約には次のようなものがある。

－証明書パス検証に関する制約(検証方針に合致しているか、パス長は制限以下かなど)
－証明書のメタ情報に関する制約(適格証明書か否かなど)
－暗号アルゴリズムの制約(鍵長など)
－署名要素に関する情報(signing time のチェックなど)
－信頼点(TSL など)

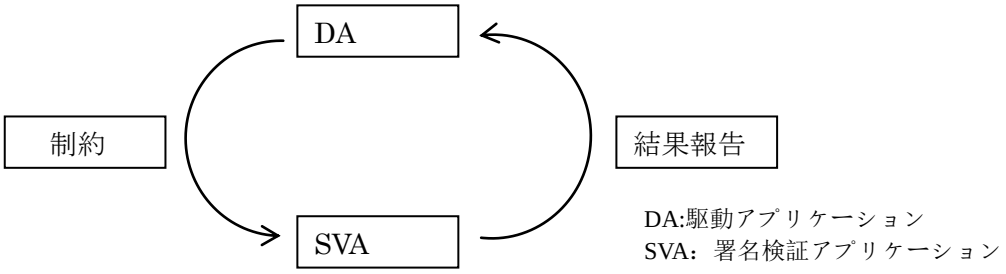


図 3-12　署名検証モデル

(d)トラストリスト更新の把握

利用者が各国のリストの更新を把握する方法として、コミッションがトラストリストのリスト(list of list)を作成しこれを自動的にメンテナンスする方向で決着した。更新は、リストのハッシュ値、または最終更新日、またはシーケンス番号で把握する。

(e)リストに対する署名の危殆化対策

危殆化で運用に空白が生じないようマルチ(2、または 3)証明書で対応する。

なお、トラストリストに関しは、ETSI の活動とは独立に、2012 年 9 月 15 日付けでトラストリストに関するドラフトが公開されている。

Trust models of the Web PKI“draft-moses-webpki-trustmodel-01”

3.4.5　適格証明書の失効

新たな EC 電子署名規制の 19 条 3 で、適格証明書の失効は 10 分以内の対応が求められている。この解釈について議論となり、結果は失効と判断された時点から DB に反映するまでとすることで決着した。失効と判断されてから CRL または OCSP により通知されるまでの期間については、即時から数時間まで様々な意見がでたがまとまらず、可能な限り早く(ASAP)で収束がはかられた。従って、失効報告から失効判断迄が 1 日以内、DB に反映するまでが 10 分以内、失効判断から通知までは ASAP となった。

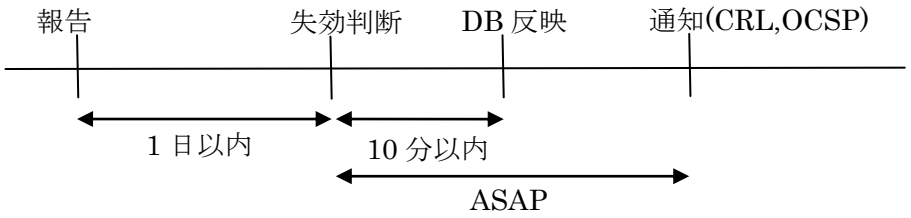


図 3-13　適格証明書の失効処理時間

3.4.6　アーカイブタイムスタンプ v3

アーカイブタイムスタンプ付与後の追加署名を可能とするアーカイブタイムスタンプ

v3(ATSv3)が CAdES 仕様に追加されることになった。ATSv3 の要否については、ETSI メンバの間でも賛否両論があったが、土地の権利証などは長期経過後に移転が発生し、新たな署名(所有者と受付機関の署名)を付与する場合などが適用例として挙げられている。

3.4.7 署名生成/検証

現状の署名生成検証仕様である TS 102 853 (Signature verification procedures and policies)は、コミッション決定の影響を強く受けており、このままでは、欧州以外では使えないことから次の内容を骨子とする改定を行うこととなった。

・汎用的な仕様とコミッション決定を反映するためのプロファイル仕様に分ける
・要求機能、制約(Validation constraint)を明確に定義する
・検証結果の詳細通知(Associated validation report data)はオプションとする
・タイムスタンプやトラストアンカーに関する不足要件を追加する

なお、コミッション指示[35] により、署名時刻(signing time)の扱いがオプションから必須になったが、汎用的な仕様として signing time をオプションとするか否かは保留となっている。signing time の扱いについては各国の解釈や方針は必ずしも一致している訳ではなく、①設定はオプションでも検証は必須なので影響はないという考えや、②必須でも制約(Validation constraint)で無視するようにすればよいという考えなど様々であり、今調整が必要である。

3.4.8 欧州以外の国の適格証明書発行

ディレクティブの変更に伴い、欧州域内に設置された欧州以外の国の CA 局が適格証明書を発行できなくなると解釈できる問題に端を発し、議論が行われた結果、欧州以外の国が適格証明書を発行するには次の 3 つの選択肢があるという結果になった。

・欧州域内に現地法人を設定
・欧州域内の国と全く同じスキームを設ける
・コミッションと直接交渉(bilateral)

このうち、第 2 案と第 3 案は国としての対応が必要となる。

3.4.9 EN(欧州標準)承認プロセスの簡素化

標準には、TS(技術仕様)、ES(ETSI 標準)、EN(欧州標準)の 3 レベルがあり、それぞれ、TC(技術委員会)、ETSI 加入メンバ、欧州メンバ国の承認プロセスがある。このうち、EN(欧州標準)に関して、現在の 2 段階承認(公聴会後にメンバ国投票)から 1 段階(公聴会とメンバ国等投票を同時に実施)承認に簡素化される。

また、ドラフトは、http://docbox.etsi.org/ESI/Open/Latest_Drafts/ で公開される。

参考文献

[1] RFC 6283, A. Jerman Blazic, Extensible Markup Language Evidence Record Syntax (XMLERS)

[2] JIS X 5092:2008, CMS 利用電子署名(CAdES)の長期署名プロファイル

[3] JIS X 5093:2008, XML 署名利用電子署名(XAdES)の長期署名プロファイル

[4] RFC 4998, T. Gondrom, Evidence Record Syntax (ERS)

[5] ETSI TS 101 733 v2.1.1, CMS Advanced Electronic Signatures (CAdES)

[6] ETSI TS 101 903 v1.4.2, XML Advanced Electronic Signatures (XAdES)

[7] ETS TS 102 778-1 v1.1.1, PDF Advanced Electronic Signature Profiles

[8] ETSI TS 102 918 v1.2.1, Associated Signature Containers (ASiC)

[9] ETSI TS 103 171 v2.1.1, XAdES Baseline Profile

[10] ETSI TS 103 172 v2.1.1, PAdES Baseline Profile

[11] ETSI TS 103 173 v2.1.1, CAdES Baseline Profile

[12] ETSI TS 102 853 v1.1.2, Signature validation procedures and policies

[13] XAdES Remote Plugtest 2012. http://www.etsi.org/plugtests/XAdES2012/Home.htm

[14] ETSI TS 101 903 XAdES 1.3.2. 2006 年 3 月.
http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=21353

[15] ETSI TS 101 903 XAdES 1.4.2. 2010 年 12 月.
http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?WKI_ID=35243

[16] 次世代電子商取引推進協議会(ECOM). 電子文書長期保存ハンドブック. 平成 19 年 3 月.
http://www.jipdec.or.jp/archives/ecom/results/h18seika/h18results-17.pdf.

[17] 次世代電子商取引推進協議会(ECOM). 電子署名の普及に関する活動報告. 平成 20 年 3 月. http://www.jipdec.or.jp/archives/ecom/results/h19seika/h19results-14.pdf

[18] 次世代電子商取引推進協議会(ECOM). XML 署名利用電子署名 (XAdES) の長期署名プロファイル JIS 案.
http://www.jipdec.or.jp/archives/ecom/LongTermStorage/data/jis/Long_term_signature_profiles_for_XAdES%28jp%29.pdf

[19] 木村道弘、前田陽二、宮崎一哉. 電子文書保存のしくみと実務　第 2 版. 中央経済社. 平成 20 年 5 月. http://www.jipdec.or.jp/archives/ecom/Publication/publication1.html

[20] 次世代電子商取引推進協議会(ECOM). 長期署名フォーマット相互運用性テストプロジェクト. http://www.jipdec.or.jp/archives/ecom/LongTermStorage/download.html

[21] 電子認証局会議. 電子署名活用ガイド. 平成 21 年.
http://www.c-a-c.jp/pdf/download/digital_signature_guidebook_CAC.pdf

[22] OASIS "Open Document Format for Office Applications (OpenDocument) Version 1.2. Part 3: Packages", Committee Specification 01.

[23] IDPF "OEBPS Container Format (OCF)".

[24] “ORDER ON THE CONFIRMATION OF THE SPECIFICATION ADOC-V1.0 OF THE ELECTRONIC DOCUMENT SIGNED BY THE ELECTRONIC SIGNATUREADOC

specification", September 7, 2009.
[25] EESTI STANDARD ESV 821:2009, "BDOC Format for Digital Signatures".
[26] PKWARE ".ZIP Application Note".
http://www.pkware.com/support/zip-application-note.
[27] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".
[28] Adobe "Universal Container Format (UCF)".
[29] ETSI TS 119 164-2, "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC) Testing Compliance & Interoperability; Part 2: Test Suite for ASiC interoperability test events)".
[30] ETSI SR 001 604 V1.1.1, "Rationalised Framework for Electronic Signature Standardisation".
[31] EC 電子署名指令 460(M/460)
STANDARDISATION MANDATE TO THE EUROPEAN STANDARDISATION ORGANISATIONS CEN, CENELEC AND ETSI IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES APPLIED TO ELECTRONIC SIGNATURES
[32] EC 電子署名規制
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market
[33] Adobe Approved Trust List
http://helpx.adobe.com/acrobat/kb/approved-trust-list2.html
[34] Windows and Windows Phone 8 SSL Root Certificate Program (Member CAs)
http://social.technet.microsoft.com/wiki/contents/articles/14215.windows-and-windows-phone-8-ssl-root-certificate-program-member-cas.aspx
[35] COMMISSION DECISION of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (2011/130/EU)

付録１　秘密分散技術標準化関連市場調査

1.　市場調査の目的

秘密分散技術を用いたサービスは、中・長期間の電子データの安全・安心な運用管理を目的として導入されることが多く、サービス主体または利用者が万が一存在しなくなったとしても、利用者は異なる環境で適切に必要な情報を利活用できなければならない。また、当該技術の市場供給に関する留意事項として、当該技術や関連ノウハウの反社会的利用の未然防止と健全な利用モデルでの市場普及といった観点も踏まえながら、特定ベンダに依存するなど限定された利用環境だけではなく、正当権限者は柔軟な利用環境下でも安心して利用できるようにするためには技術標準化が必要である。今後、技術や商品サービス等の提供や運営のあり方等に関しても広く考察を加えた結果を技術標準化し、当該技術を健全に市場普及させていかなければならない。

まず、秘密分散技術の標準化を行うに先立ち、広く現状調査を行うこととした。①既公開ガイドライン[1] のメンテナンスの必要性の確認、②ケーススタディ(秘密分散技術の利用事例調査)及び、③秘密分散技術の利用に関する有識者等に対するヒアリングを行った。

今年度は調査、検討を開始した段階であり、まだ詳細な技術標準化に関する内容(原案等)の報告は含まれないが、そのベースとなる現状調査活動内容を紹介するとともに、技術標準化を行う際に考慮すべき事項を報告する。

2.　技術標準化に向けた事前調査内容

2.1　意見書に基づくガイドラインの再検討

電子記録応用基盤フォーラム(以下“eRAP”とする)の顧問である東海大学　辻秀一教授より、「「秘密分散技術(電子割符)」の市場先行事例調査への意見書」を受け取り、その課題への対応について検討した。

2.1.1　課題

意見書で指摘された課題は以下のとおりである。

① 参考文献[1] における「秘密分散に関する技術ガイドラインおよび秘密分散技術利活用に関するガイドライン」の「３．秘密分散技術を実現するソフトウェアプロダクトにおける必須要件」、「４．秘密分散技術を実現するソフトウェアプロダクトにおける任意要件」と「５．秘密分散技術を利活用するシステムにおいて考慮すべき必須要件」が記載されているが、記述が定性的で断片的で不十分な内容となっている。これらについては、定量的で網羅的な検討と整理が必要である。

② 参考文献[1] における「情報分散管理技術(電子割符技術を利用した情報管理)に関する法的意見書」の「第１　技術と運用に関する基本的視点」に「－－－　②その技術を運用する運用者側の運用ルールや、運用実態、リスク分析などを踏まえた運用の評価、－－－②は実用を評価対象とするものではないため、問題点の指摘にとどめ、今後の電子割符技術の

利活用に資する問題点を指摘し、－－－　」と記述されており、運用時における様々な検討が必要であることが指摘されている。この指摘にあるように、具体的で詳細な運用管理や実装の方法を検討・整備し、更に運用時におけるリスク分析や脅威分析などにより安全性レベルを評価することが必要である。

2.1.2　対応

課題に対しては、当該技術に関する先駆者からノウハウ等の開示協力を得て検討を進める必要がある。この件に関しては、、既公開ガイドラインで代表的秘密分散技術の供給者と記載されたグローバルフレンドシップ株式会社より、社会安全保障上懸念される情報部分の開示はできないが、技術開発に関し既公表情報等と未公開情報も含めた社内情報の開示に関する内諾を受けた。

2.2　事例概要と事例調査先概要

ベンダごとに異なる秘密分散技術を用いたシステムを相互利用する可能性の検討のため、3 つのユースケースについて検討を行った。

① 広域災害を前提とした DNA 情報を含む本人特定情報(ID)と本人から家族等に宛てたメッセージ等を当該技術を用いて本人、配偶者、掛かり付け医とで割符を保有し、安全に運用管理する。
② 電子証明書や暗号鍵を当該技術で処理し端末と外部記憶メディアとで分散して運用管理する。
③ 小規模医療機関(整骨院)の院内情報管理。
ここでは「小規模医療機関(整骨院)の院内情報管理」を選択し報告する。
選択基準としては、個人情報管理を要求される分野で、厳密な患者個人情報等の管理義務が存在し、組織規模を問わず同一法令等が適用される最小規模の組織の取り組みを報告し、それを超える規模の組織でも、共通または類似課題となり易い項目を拾い上げることとした。

この事例の特徴は、下記のとおりである。

・e-文書法に対応
・個人情報保護法に対応
・BCP 対策を実施
　業務効率化。最小規模の組織による無理の無い目標達成、副次的効果等

2.2.1　事例調査先概要

(1)導入の動機

事例調査先である整骨院(東京都渋谷区)では、本取り組み以前から患者に対する真摯な医療サービスのあり方を検討していた。昨今の個人情報保護への関心や、東日本大震災における電子カルテや本人を特定する ID を含む情報、更には行政情報の消滅による初動の遅れが人命の危機を

招く結果も生じた現実を見据えた結果、本件取り組みを 2012 年 06 月より開始した。

(2) IT 導入環境

現場の最大の課題は、ほぼ一人で切り盛りする現場でありながら患者情報の保護には大規模医療機関と同様の業界義務が課せられていることであった。通常この規模の医療施設の場合は大手 IT 企業等が支援に来ることは無く、自ら法律やガイドラインを通読し必要な対策等を実施していかなければならない。これは現場の実情を考えると非常に難しい要求事項であり大きな負荷が様々な面でかかっている事実は否定できない。

(3) 担当者スキル

同院院長は、技術習得に必要な学習期間や研修先等で早期から電子カルテやレセプトの仕組みを利用していた経験があり自らの院内でも利用していた。業務上来院患者から、同意書や他の医療機関からの紹介状を受領するので、電子と紙の両方の個人情報を完璧に管理しなければならない。零細規模の医療施設には、適切な e-文書法対応したカルテやレセプトの仕組みを提供する会社も少なく、診療時間後に院内の清掃を行った後に患者情報を紙に出力し原本管理している。

(4) まとめ

施術時間と、診療後の自分自身の時間を紙原本管理の為に費やしていることであり、e-文書法を制定してもなお我が国の方針が現場レベルでは実現できていないことの 1 つの事例である。事例の現場取り組みシステム概要図を図 1 に示す。

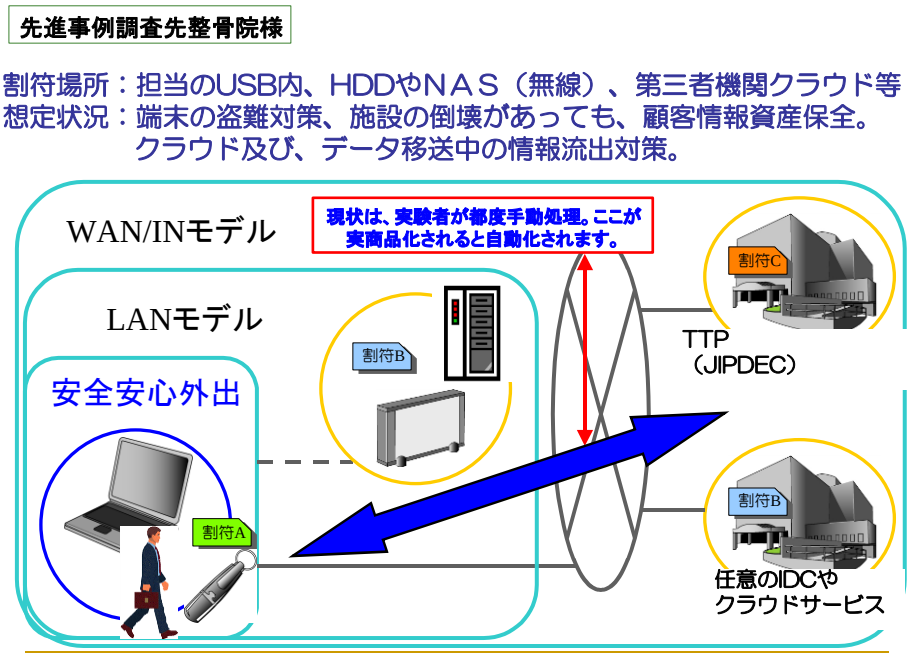


図 1　先進事例システム概要図

2.2.2 所感

今回の取り組みでは、タイムスタンプ・署名を行なうだけでは患者情報が見えていることと、院長の懸念事項である広域災害等でも患者情報を消失させない対策にはならないことも大きな課題であったので、秘密分散技術を用いて個人情報保護を実現した。

今回の現場取り組みの主要ポイントは、既存 IT ソリューションと秘密分散技術(電子割符)を合理的に組み合わせ、

① e-文書法対応した実務環境の整備
② 紙ベースの個人情報を手軽に e-文書法対応できる環境整備
③ e-文書法対応した電子的な個人情報保護の実現
④ 首都直下型の大規模震災等を想定とした BCP 対応の具体化

であった。この eRAP 報告書で報告されている既存 PKI 暗号技術を活用したタイムスタンプ署名やケース管理を、この現場では具体化や実装のレベルの違いこそあれ、原理的には市場先進事例現場では事実上実施していたことは興味深い。

我が国の産業構造上、最下層や中層に位置する組織の事業所数が我が国で絶対多数であることや、そのような層が経済全体を支えている事実も鑑み、大手 IT 企業等が対処協力できない組織・事業主体等の IT 化は、我が国全体の効率化や合法化を推進するに非常に大きな課題であり、今回の取り組み成果や、次年度も継続される高度化の取り組みは、非常に重要なものと考える。

ユースケースの検討に協力していただいた企業は以下のとおりである。

協力企業/団体(50 音順、敬称略):

株式会社アイ・オー・データ機器、エヌシーアイ株式会社、グローバルフレンドシップ株式会社、セイコーインスツル株式会社、ソフトバンクテレコム株式会社、凸版印刷株式会社、日商エレクトロニクス株式会社、特定非営利活動法人日本セキュリティ監査協会(JASA)、株式会社日本電子公証機構、株式会社ひろせ保険&L、マキシー株式会社、牧野総合法律事務所、めぐみ整骨院、他

2.3 ヒアリング結果

2.3.1 ヒアリング方法

広く事例先や有識者意見等を回収すべく、敢えて特段の質問項目等を設定せず対話形式でご意見等を頂戴した。事例先の場合は、特に広範な事業上の悩みから IT 導入を検討する経営者目線からの声も上がった。有識者には、事例先の声と取り組みの概要説明資料(前掲の「図 1 先進事例システム概要図」や、技術概要解説を含む)を持参し、特定の意見交換項目を敢えて設定せず、幅広くご意見を頂戴した。

2.3.2 事例先の主な声

今回の取り組みを通じて法的対応と同時に、IT 化により本来得られるはずのメリットを享受しやすくなった。特に e-文書法対応とプライバシ保護、更に BCP 対策も実現できることは、経営上も大きなメリットがある。昨年は、原理的な実験だったので、今年は一連の院内システムとし

て動くようなレベルへとステップアップしてもらえると更に良い。

2.3.3 有識者の主な声

- これまでの電子割符(秘密分散技術)の特性に関する法律家としての認識や過去の官庁等での実証実験成果や個別相談結果を踏まえた現場実験であり、個々の割符ファイルを適切に運用管理をしているのであれば問題ない。
- 残存リスクに対する利用者への明確な説明を誤解なくできるようにすることが大事である。利用者の導入ハードルをいかにして下げつつ安全性を確保するか。
- 保証内容をどのレベルにするかが市場普及の際の大事なポイント。
- 県内の同様な医療施設での応用等を検討したい。震災時は直接の被害は発生しなかったが、仮にスプリンクラーが誤作動してしまえばサーバのデータが消滅していた可能性もあり、BCP とは直接被害だけではないことを痛感。
- 運用管理の重用性を無視して秘密分散技術で処理するだけで、絶対安心というような誤解を招かない啓蒙普及も必要。
- 当該技術やサービスを利用する側と、そのサービスを提供する主体や商品等の評価等を行なう組織への外部監査や評価といった仕組みも必要となるであろう。
- ISMS の観点からも、今回の取り組み成果は応用できる可能性がある。

2.3.4 類型化及び評価(事例現場で確認したメリット・デメリット)

(1)実務面

非常に嬉しい効果が見えているが、実験用なので個々の仕組みを自らコントロールする必要があり、そこが現場実務としては軽くなると更に良い。ただし、あまり簡単な仕組みになると、自ら意識して大事な情報を管理している感覚が無くなることが怖い。

(2)経営面

非常に期待できる結果。早期に導入できる価格帯での正式な商用化を望む。損害賠償保険の料率算定にも好影響を与えるような形等で連携できると経営全般に対し更に良いと考える。もしも導入に対し公的補助があれば、更に助かる。

(3)社会面(法解釈、行政認識、学術等)

過去の公的実証実験や既公開の調査報告書記載の法的意見書に沿った内容で、特段の問題点は見受けられない。理論上完全秘匿できる暗号の仕組みは、安易に一般市場に流通させることができない。

世界的にも一定レベル以上の暗号に関しての輸出規制等が存在し、社会安全保障上の留意事項が存在することは周知の事実である。

今後、秘密分散技術が技術標準化と市場普及を両立させていくには、実社会で流通可能な技術として何らかの形で適切に社会が受容できる技術としての市場啓蒙と同時に技術標準化を行なう際に、第三者機関等による技術等の認定や登録といった制度も必要であろう。

早期に技術標準化のドラフトができることを望む。実社会で利用できる技術として、関連する

運用管理手法の正しい周知も必要である。

この成果を国民・個人の情報管理基盤へと応用することで、巨大災害への迅速な対応基盤へと発展させられないか。健全な形で市場普及が進むことを望む。

(4) 業界認識

これまでの啓蒙段階での実証実験や報告書等に記載された成果を組み合わせ現場実証したモデルである。

経営資源に厳しい現場でもクラウド等既存 IT 環境を有効活用できる成果で今後の可能性を感じる。現在電子割符・秘密分散技術の標準化は実現できていないが、日本発の世界標準化の可能性がある取り組みと考えられる。

既存暗号技術と合理的に組み合わせた成果。技術標準化の際に、既存暗号技術との棲み分けや相互補完等の具体的な利用法等が明確にできると更に良いだろう。

理論の世界の秘密分散法なのか、それとも市場流通する秘密分散技術なのか、現場で混乱する可能性もあるので早期の用語定義等が必要だろう。

2.3.5 ヒアリングの結果

- 市場性(技術的特性を踏まえたニーズ)はある。
- 社会的有用性(法解釈・行政解釈)に関しては、過去の公的実証実験等も含め、広く認知されてはいないが存在する。但し、広く社会に認知されている状況ではないので、正しく市場啓発する必要がある。
- 技術、商品サービス供給体制に関しては、先駆的企業が複数市場に技術や商品を提供しており、市場ニーズは確実に増加している。今後供給者は増えるものと考えられる。
- 消費者保護の観点からは、当技術が適切に開発、供給され、更に適切な商品化が行なわれることが必要。現時点では、技術供給者と商品供給者のモラルによって品質や保証が維持されている。これは社会的な仕組みとして中・長期間の利用を求める利用者の期待に相応しい状況ではなく、早期に中・長期的な利用を前提とした社会的な安全安心を担保する技術標準化が望まれる。
- 社会安全保障に関しては、既公開ガイドラインで代表的秘密分散技術の供給者の 1 社が当該技術の市場供給開始前後に行なった、情報政策官庁との当該技術の市場普及に関する協議結果(要点は、当該技術や関連ノウハウの反社会的利用の未然防止と健全な利用モデルでの市場普及)は、現時点では踏襲すべきである。
- 波及効果に関しては、当該技術の効用が世界的に見て IT 共通の課題に対応するものであることから、日本発の世界標準化の可能性を秘めた裾野の広い経済波及効果等を期待できる。

3. 来年度活動への提案

前述のヒアリング結果を受け、今後の活動を以下のように考えている。

① 市場啓発活動を本格的に開始する。
② 市場啓発活動を行なう組織は、秘密分散技術のサプライヤーや、その技術を用いた商品・サービス供給会社及び外部有識者、一部利用者等広く参加を可能とした場を準備する。
③ 今後も先駆的事例に関し､市場啓発を行う組織内だけではなく広く社会にも情報を供給し、正しい知識と利用の普及を促進する。
④ 本報告のような先進事例調査を継続し、市場啓発活動と技術標準化検討の場に情報提供する。
⑤ 既公開ガイドラインのメンテナンス作業は、新たな活動の場を準備して行なうことを検討する。

なお、技術標準化に関しては当該技術全般に関する標準化を一括して行わず、標準化に向けた作業の優先順位を付け活動していくこととした。
現状想定している技術標準化ステップは、以下のとおりである。

Part1－用語定義
Part2－フレームワーク(秘密分散技術概念定義)
Part3―中・長期の運用管理のあり方とプロファイル定義(ファイル定義やサービス実現のプロトコルから中・長期間の運用に耐える互換性確保も視野)
Part4－評価方法、等々と当該技術応用や利活用も含めた部分も今後標準化の対象となる可能性はある。

意見書でも記載されている現場での実運用管理面の安全性確保に関して次年度も現場事例の運用管理の高度化等の取り組みを行い、成果を技術標準化に反映させていく。
また現在までに評価されている当該技術の基本的な技術概念を踏み越えないものは既公開ガイドライン記載のように当該技術範疇に入るものとして、秘密分散法等の数学理論を背景にした技術も登録認定できる仕組みを構築することも検討対象としている。
但し、当該技術はあくまで実社会が受容できる技術として市場に供給されるため、社会安全保障上の観点から情報理論の世界で言う完全秘匿を実現した技術は今回の対象としない。
ここは既公開ガイドライン[1] を踏襲する。
なお Part2 で当該技術として認められる技術方式は、例えば A 社方式、B 社方式といった形で書き加えられていくことを想定。今後の活動は上記当該技術標準化準備に並行し、別添の意見書指摘事項等に対し実社会で有効となる具体策等を見出していく活動等も組み込まれ、既公開ガイドライン[1] 全体に反映される。
ポイントは以下のとおり。

① セキュリティ 3 要素のうち、特に中・長期間の電子情報運用管理において、完全性と可用性に資する基礎技術としての標準化を進めていく。
② 技術標準化の範囲には、既公開ガイドラインで示した機密性部分である原本情報を実際に分割することに起因する部分と、適切な割符管理で原本情報全体に対するアクセスコント

ロールに資する部分も含まれる。

③ 秘密分散技術の利活用の際には、利用者の割符の運用管理も機密性維持等における重要なファクターである。

④ 社会安全保障上の観点を十分考慮し、完全秘匿を可能とした技術は対象とせず、あくまで健全な利用モデルでの市場普及を推進する。

⑤ 当該技術標準化は、今後その用語定義から段階的に進められる。

⑥ 当該技術への既評価の根底を成す基本的な技術概要を満たす技術方式であれば、順次認定・登録ができるような組織の準備も含めた技術標準化を進める。

⑦ 当該技術標準化の内容が実社会との乖離を生じないよう、市場先進事例調査等を今後も継続し成果を技術標準化に反映させていく。

⑧ 現時点の反映点は、今後の社会情勢等の変化により適宜見直し等が行われる。

4. あとがき

今回の秘密分散技術の標準化に向けた市場調査報告では、多数の有識者様(行政、大学、企業、個人)のご意見を頂戴(2012 年 10 月～2013 年 1 月 29 日現在、ご意見頂戴先打ち合わせ総数 95 回)したにもかかわらず、それら内容やご意見頂戴先の一覧も紙面の都合上全てを掲載することができないことをお詫びしたい。

今回の報告に向けた関係各位の深いご理解とご支援に心より感謝すると同時に、今後の当該技術標準化に向けた一連の活動に対する更なるご協力等を申し上げる次第である。

解説　秘密分散技術

「秘密分散技術」は、高度な数学理論を熟知していなくても基本的安全性を理解・納得できる電子情報の簡明な安全確保技術である。内閣官房情報セキュリティセンター(以下“NISC”とする)公開「政府機関の情報セキュリティ対策のための統一管理規準」解説書等に明確に暗号とは異なる「技術」として明記され、官民問わず利活用事例や商品・サービス等が市場に複数提供されてきている。

(1)秘密分散技術の現状

当該技術に関しては、前記 NISC 解説書記載の秘密分散技術に対する技術ガイドラインの必要性もあり、次世代電子商取引推進協議会(ECOM)で既公開の「EC における情報セキュリティに関する活動報告書 2009(情報セキュリティ WG：SWG1・SWG2・TF の各報告書)中の、「秘密分散技術利活用検討における活動成果報告書 2009(TF1)」報告部分(以下“既公開ガイドライン”とする)において「秘密分散技術」の原理、定義、利用方法、社会安全保障上の留意事項、あるべき姿、代表的秘密分散技術、法的解釈等の基本的内容を公的に報告した。

http://www.jipdec.or.jp/archives/ecom/results/h21seika/H21results-10.pdfTF

近年、公共入札等でも「秘密分散技術」や「電子割符」の文言が明記された事例が散見される状況となってきた。後述の市場先進事例の調査現場においても、既公開ガイドラインで報告

されている代表的秘密分散技術を用いており、前述のように今後増加傾向と考えられる技術である。今回の市場調査でも意見が寄せられたが、その利活用の効用を踏まえ正式導入する為にも技術標準化の実現を望む声が多く上がった。

(2)秘密分散技術の技術等の概要

代表的秘密分散技術の概要は、電子的原本情報をビットレベルで分割し、指定した個数の割符ファイル(以下“割符”とする)にそれらのビットを都度ランダムに割り振ることにより、割符単体だけでは個人情報等に該当する原本情報文字列等を導き出せないが、必要な割符を揃えることで原本に統合・復元できる基本的特性を持つ基礎技術を指す。この割符単体は集合論で言うところの部分集合に相当し、欠落した未知の部分が入手できない限りは原本情報全体は保護されるので、そこに冗長部分を持たせたとしても原本情報全体は保護されたままで且つ、BCP 対策にも役立つ。また生成した割符を適切に管理することで攻撃者に都合の良い原本情報に対する改竄等が極めて困難な原本情報管理ができ、仮に割符のひとつに改竄等があったとしても復元に必要な他の割符と統合できない為、復元前に改竄が発生していたこともチェックできる。このような集合論的な特徴は、一般的なセキュリティ手法とは原理的背景が異なることから生じる興味深い特徴である。また盗難等の場合に備え、統合・復元に必要な残りの割符が容易に照合できない仕組みを具体化することで、簡便に個人情報等に対する有効性が確保できるという法解釈(後述、既公開ガイドライン参照)等も成立することから評価注目されている。例えば USB をはじめとする外部記憶メディアや外部クラウド等の利活用時に漏洩や紛失・盗難等が発生したとする。その際に紛失等の対象となった情報が単体の割符だけで、統合・復元に必要な他の割符を容易に照合できなければ取得者はその割符単体からは本人特定できる個人情報や原本情報全体は得られない。なお、秘密分散技術の技術実装の中で、生成される個々の割符に関し理論上の完全秘匿も実現する高度な機密性を持たせることも可能であるが、個別の当該技術供給者のアルゴリズム実装や、その技術に関する外部評価や実証結果等に依存する部分なので、関心のある向きは個々の当該技術供給者に確認されたい。前述のような基本特性を持つ電子割符のイメージを図 2 に示す。今回の活動では、この秘密分散技術・電子割符の特性を利活用した。

図 2　利活用した秘密分散技術（電子割符）の特色

前述のように生成される個々の割符に関し更に高度な機密性を考慮しない場合の秘密分散技術の持つ基本的な機密性は原本情報を実際にビットレベルで分割してしまうことを基礎とする機密性と、原本情報全体に対するアクセスコントロールが可能になる機密性を持つことによるもので、情報理論の世界で言うような完全秘匿を実現する暗号や、一般市場に流通する暗号技術・商品の保証する機密性とは少々異なる性質のものである。特に、原本情報を分割した割符を適切に管理することで原本情報全体へのアクセスをコントロールさせることができるという点は、自己情報コントロール権等の観点からも重要である。そこで当該技術の概要としては、既公開ガイドラインに記載されているような機密性に関する内容に加え、集合論的な性質による原本情報全体へのアクセスコントロールに資する点、更に BCP 対策にも有効な点を踏まえ、それら特長を活かし原本情報の中・長期的な運用管理にも資する技術として原本性(完全性)と可用性部分を担うべく技術標準化の検討等を進めていく。なお、一般の暗号が提供するような機密性を要求する情報管理場面でも、必要な強度の暗号化を施してから秘密分散技術を利用するといった高度な利用方法も下記 NISC ドキュメントに記載されている。

「政府機関の情報セキュリティ対策のための統一管理基準(平成 24 年度版)」解説書
http://www.nisc.go.jp/active/general/pdf/K304-111C.pdf

「政府機関の情報セキュリティ対策のための統一技術基準(平成 24 年度版)」解説書
http://www.nisc.go.jp/active/general/pdf/K305-111C.pdf

前述のような基本特性を持つ電子割符のイメージを図 2 に示す。今回の活動では、この秘密分散技術・電子割符の特性を利活用した。

前述の解説書で「秘密分散技術」を検索すると「要機密情報」や、先般の東日本大震災等で問題となったサーバーデータのバックアップも視野に入った「要安定情報」への措置の方法の

1 つとして記載されている箇所が確認できる。これらのドキュメントは、NISC 公開の(http://www.nisc.go.jp/materials/index.html)主要公表資料の中に存在しており、その根拠(http://www.nisc.go.jp/active/general/pdf/kihan24.pdf)となる政府機関の情報セキュリティ対策のための統一規範も、同様に NISC により公開されており、その定義では、機密性では、機密性 2 情報及び機密性 3 情報を「要機密情報」、完全性では、完全性 2 情報を「要保全情報」、可用性では、可用性 2 情報を「要安定情報」としている。上記の各要件から重要な情報であると認められる情報をまとめる名称として、要機密情報、要保全情報及び要安定情報を「要保護情報」とすることが明記されており、まだまだ適用箇所は少ないものの、当該技術が利用できる場面の記載が存在する。

なお、今回の活動発足の経緯が、東日本大震災発生以降、情報資産の中・長期間の運用管理に対する社会的認識の変化が顕著になったことと、既公開ガイドラインのその 3 部構成第一部の８．終わりに、の記述「今後は、今回記載から漏れた技術の調査や秘密分散技術の規格を ISO に登録するような動きをしていくことで秘密分散技術、ならびに情報セキュリティ技術の発展に寄与できるものと考えている。」の記述も受けたものである。また、このような基礎技術の場合、そのシステムへの実装方法や最終サービス等の提供や運用面の整備も重要である。関連する既公開の資料としては、電子商取引実証推進協議会(ECOM）の平成 12 年 3 月暗号利用技術ハンドブック 6.4 暗号利用とそのコスト 6.4.1(2)に、個々のアルゴリズムの安全性よりもシステムとしての安全性に対する配慮することの重要性が説かれており、既公開ガイドラインの法的意見書にも符合する。

参考文献

[1] 次世代電子商取引推進協議会．EC における情報セキュリティに関する活動報告書 2009(情報セキュリティ WG:SWG1・SWG2・TF の各報告書)／秘密分散技術利活用検討における活動成果報告書 2009(TF1)．平成 22 年 3 月

[2] 一般財団法人日本情報経済社会推進協会　電子記録応用基盤フォーラム　eRAP 中間報告会　保倉豊. 秘密分散技術(電子割符)を用いた先進事例の調査～技術標準化のための事前市場調査～．2012 年 10 月

メンバリスト

事務局

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、所属五十音順)

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
技術検討 WG 副主査	佐藤　雅史	セコム株式会社
有識者委員	柿崎　淑郎	東京理科大学
委員	石本　英隆	日本電信電話株式会社
ビジネス・システム検討 WG 主査	溝上　卓也	株式会社日立ソリューションズ
委員	三原　　真	富士ゼロックス株式会社
技術検討 WG 主査	宮崎　一哉	三菱電機株式会社
委員	杉崎　　元	三菱電機株式会社
技術検討 WG 副主査	宮地　直人	有限会社ラング･エッジ

上記以外のメンバ

役　割	氏　名	所　属
委員	宍倉　勝仁	シヤチハタ株式会社
委員	能勢健一朗	東芝ソリューション株式会社
委員	石原　達也	東芝ソリューション株式会社
委員	塩川　淳史	株式会社フォーク
委員	児玉　　剛	株式会社フォーク
委員	棚沢　優介	株式会社フォーク
委員	小野　成志	株式会社フォーク
委員	染野進之介	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	小池　正通	富士ゼロックス株式会社
有識者委員	西川　康男	ARMA　International 東京支部
有識者委員	佐藤　　均	東京医療保健大学
有識者委員	佐藤　伸一	株式会社 PFU
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	柳原　孝志	日本ガードタイム株式会社
オブザーバ	小林　大樹	三菱電機株式会社

電子記録応用基盤に関する調査検討報告書 2012

-ケース指向電子記録管理及び電子署名の新たなパラダイム-

電子記録応用基盤フォーラム（eRAP）

平成 25 年 3 月 29 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　東京都港区六本木一丁目 9 番 9 号　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

ISBN978-4-89078-030-3
C3004