証拠性確保を重視したケース指向電子記録管理のための パッケージ構造の業務適用評価

宮崎一哉[†1]　木村道弘[†2]　前田陽二[†2]　辻秀一[†3]

パッケージとは記録とメタデータを一体化するためのデータ構造である．パッケージは記録とメタデータの関係を維持した状態で流通あるいは移管されるときに用いられる．我々は電子記録管理において最も重視される要件を証拠性の確保であると捉え，更に，個々の電子記録のみでなく複数の電子記録が含まれる"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．提案形式をソフトウェアシステム請負製作業務に適用し，既存技術との比較による机上評価を行った結果，提案形式の定性的な有効性が確認できた．

Package Structure for Case Oriented Electronic Records Management Considering Evidence Preservation and its Evaluation

KAZUYA MIYAZAKI[†1]　MICHIHIRO KIMURA[†2]　YOJI MAEDA[†2]
and　SHUICHI TSUJI[†3]

1. はじめに

検索･共有･流用の容易性や多重化による耐災害性など，紙文書と比較して電子文書が多くの利点を持つことには疑問の余地が無い．一方で，改ざんの容易性や媒体劣化等による見読性喪失等の電子文書の種々の欠点にも技術や運用による解決策が与えられつつあり，また e-文書法等の文書を電子で扱うための法制度やデジタルデータの証拠性確保のために必要となるタイムスタンプサービスや関連の認定制度などの社会インフラも整備され始めており，電子化はますます進展している．ところが，文書等を電子記録として組織的に管理していくことは充分なされていない[1][3].

電子記録管理とは，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，それを長期間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実践である．電子記録管理では，特に権利保護や説明責任などを目的とする場合，電子記録の証拠性が重視される．

筆者らは電子記録管理を効果的に実現するためのシステムである電子記録管理システム上での個々の電子記録の取扱の単位となるパッケージの構造を提案した．そのパッケージ構造は，証拠性確保を重視し，欧州電気通信標準化機構が電子データと分離型電子署名を一体化するために提案している ASiC（Associated Signature Containers）に基づく構造とした[2].

†1 三菱電機株式会社
Mitsubishi Electric Corporation
†2 一般財団法人日本情報経済社会推進協会
Japan Institute for Promotion of Digital Economy And Community
†3 東海大学
Toukai University

また電子記録管理においては，決定過程を含めた記録の管理が重要であり，そのために筆者らはケース管理の概念を導入した．ケース管理に基づいて決定過程を含めて記録を管理するためには，複数組織に跨る案件毎に，対応する一連の業務と関連付けて記録を管理する仕組み，即ちケース指向電子記録管理システムが必要となる．筆者らはケース指向電子記録管理システムに対応させるために，個々の記録を対象コンテンツとするに対応するパッケージ構造を拡張し，個々の記録だけではなく一連の記録が互いに関連付けられた「ケース」を対象としたパッケージ構造を提案した[4].

本稿では，ケース指向電子記録管理システム対応のパッケージ構造の詳細を示すとともに，ソフトウェアシステム請負製作業務への適用例を通して既存技術との比較評価を行った結果を示す.

2. ケース指向電子記録管理システム

企業や行政組織等にとって電子記録管理の重要性は欧米では既に広く認知されている状況である．特に先進的な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，電子記録管理，ケース管理，及びケース指向電子記録管理システムについて説明する.

2.1 電子記録

本稿での電子記録の定義は ISO 15489-1[5]に準じることとする. 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及び情報として作成，受領，維持する，全形式の記録された情報」と定

義される．

電子記録は形式を問わないあらゆる電子データであり，その証拠性が最も重要な要件となる．

2.2 電子記録管理と電子記録管理システム

電子記録管理とは，組織による事業継続／発展，リスク回避，権利保護，説明責任などを達成し，それを長期にわたって維持することを目的とした，電子記録の取得，維持，活用等の仕組みであり，その実践である．

この定義もやはり ISO 15489-1[5]に準じるものである．文献[1][3]では，MoReq2(Model Requirements for the management of electronic records)に示された電子記録管理システムに対する要件より抽出し整理した「電子記録管理システムの主要 100 要件」を策定している．

電子記録管理システムは、電子記録管理システムの主要 100 要件に沿って電子記録管理を実現する基盤(プラットフォーム)である[1][2]。

電子記録管理システムの構造を図 1 に示す。

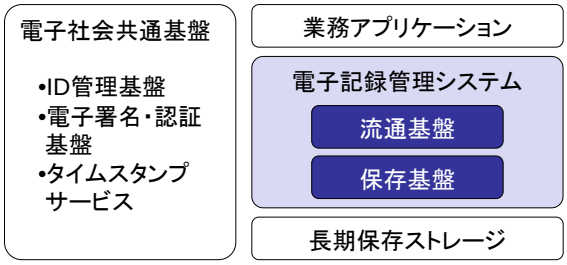

図 1 電子記録管理システムの構造

図 1 にあるように，電子記録管理システムは、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管理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管理システムの構成要素である．

電子記録管理システムは複数存在でき，1 つの電子記録管理システムより他の電子記録管理システム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．

2.3 ケース管理とケース指向電子記録管理システム

我々の想定する電子記録管理システムには，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[1][2][3][4][6]．この概念の導入目的は，決定過程を含めた記録の管理である．

決定過程を含めた記録管理のためには，複数組織に跨る案件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．この仕組みをケース指向電子記録管理システムと呼ぶ．

図 2 に業務とケース管理の関係を示す．一つの案件が発生すると，ケース指向電子記録管理システムは案件に対応するケースファイル（以降ケースと呼ぶ）を生成する．案件に含まれる業務は 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指向電子記録管理システムがそのケースに蓄積していく．ただしケース内に記録の実体を含む必要はなく，記録の実体への参照のみを含む場合もある．またケースはサブケースを含む場合も考えられ，その場合はケースにサブケースが格納される．つまり，ケースは入れ子状態になる場合がある．ただしサブケースについてもその実体を含まず，サブケースへの参照のみを含む場合もある．

こうして 1 つの案件の開始から終了までに発生した全ての記録及び属性は，最終的に 1 つのケースに関連付けられる．

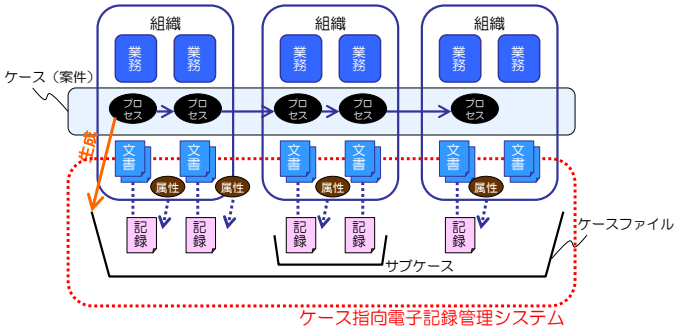

図 2 業務とケース指向電子記録管理システムの関係

一つの案件に対して生成される一つのケースは，図 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発生の順序や時刻を伴って関連付けられる．個々の記録には，それぞれ各種属性が添付される．

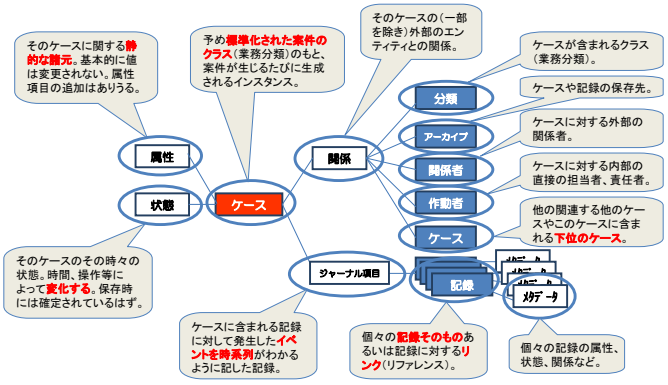

図 3 ケースの構造

3. ケースにおけるパッケージ

パッケージとは，電子記録管理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．本稿では，個々の電子記録をメタデータと一体化するだけではなく，ケー

スに関連する複数の電子記録やメタデータを一体化するためのパッケージを検討対象とする．

パッケージの参照モデルが ISO 14721:2003[7]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 4 に示す．

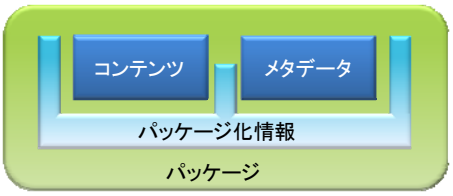

図 4　OAIS 参照モデル—パッケージの構造

このモデルでは単一のコンテンツに対するパッケージの構造しか示されておらず，複数の記録を含むケースに対応することができない．

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．ドイツのパッケージ[8]及びハンガリのパッケージ[9]はほぼ同様の構造を持つ．図 5 にハンガリのパッケージである e-Dossier の構造を示す．

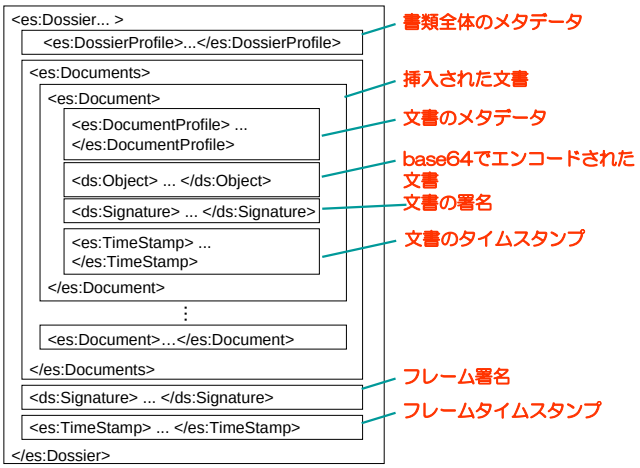

図 5　e-Dossier の構造

e-Dossier は次の特徴を持つ．

- 複数の文書を含めることができる．
- 個々の文書にメタデータ及び証拠性を確保するための電子署名及びタイムスタンプを付与できる．
- パッケージそのものに対してメタデータ及び証拠性を確保するための電子署名及びタイムスタンプを付与できる．

e-Dossier において，書類全体をケースに，文書を記録にあてはめられそうであるが，ケース対応とするためには，次に挙げる課題が残る．

[課題 1] 電子署名及びタイムスタンプが長期署名[11][12]に対応していないため，長期にわたって証拠性を確保できない．

[課題 2] ケース内にサブケースを含めることができない．

[課題 3] 実体を必ずパッケージに含まなければならない．

このうち最初の課題 1 に対応することを視野に入れたパッケージ構造として，欧州電気通信標準化機構(ETSI)が，コンテンツと長期署名を一体化する Associated Signature Containers (ASiC)[10]を提案している．

ASiC の基本構造は次の通りである．

- フォルダにより階層化されたファイルを zip 圧縮したファイルである．
- コンテンツのメタデータ(署名を含む)を格納する META-INF サブフォルダを持つ．

パッケージのタイプには大きく分けて次の 2 種類がある．

- ASiC-S(簡易型 ASiC)：単一のデータオブジェクトと 1 つ以上の署名やタイムスタンプを含むパッケージ(図 6)
- 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パッケージ

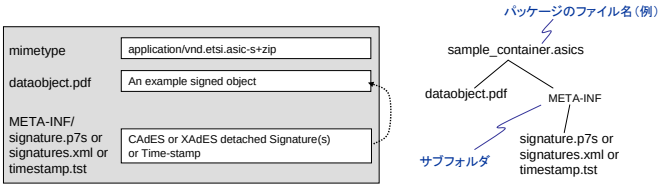

図 6　ASiC-S の構造とフォルダ構造の例

ASiC-E には，XML 型の長期署名(XAdES)[11]を含むものと CMS 型の長期署名(CAdES)[12]またはタイムスタンプを含むものがある．それぞれを図 7，図 8 に示す．

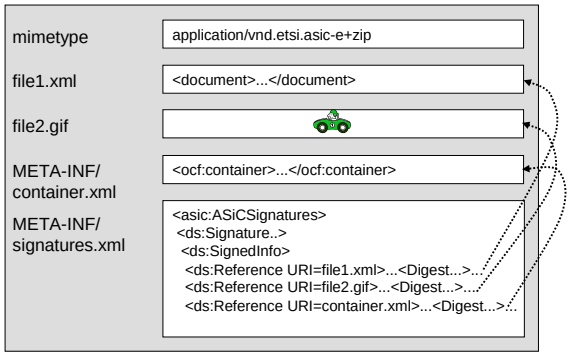

図 7　ASiC-E[XAdES を含む形式]の構造例

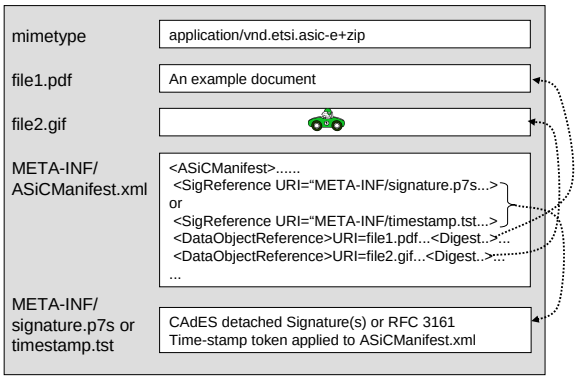

図 8　ASiC-E[CAdES／タイムスタンプを含む形式]の構造例

ASiC を利用して課題 1 を解決するケース対応のパッケージを構成できる可能性はあるが，その適切な構成と課題 2 及び課題 3 への対処方法は定義されていない．

4. パッケージ構造の提案

ASiC に基づき，複数存在する形式から適切な構成を選ぶことにより前章で示した課題 1 を解決することができる．本章では，まず課題 1 の解決のために最も適した ASiC の構成を示した後，更に課題 2 及び課題 3 を解決するためのパッケージの構成方法を示す．

まず，課題 1 に対応するためには署名やタイムスタンプの有効性を延長できなければならない．ASiC には前章で示した複数の異なる形式がある．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でそれが可能となる．

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．この場合，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 8 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．

なお，長期署名以外のメタデータは，ASiC の基礎となる形式である OEBPS Container Format(OCF)1.0[13] 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．

次に課題 2 及び課題 3 を考える．

ケースはケースのメタデータと複数の記録を含む場合がある．個々の記録自体もメタデータを伴う．また，ケースに格納される個々の記録は個別に証拠性を確保する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を確保のために長期署名を付せばよい場合が考えられ，更に，ケースのメータデータを含むケース全体の証拠性を確保する必要もある．

ケースに対応するパッケージを構築する場合，記録毎のパッケージとサブケースが存在する場合はそこに含まれる記録に対するパッケージを更にパッケージ化し，それらケース内の記録及びサブケースのパッケージを集め，ケースのメタデータ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 10 に示す．

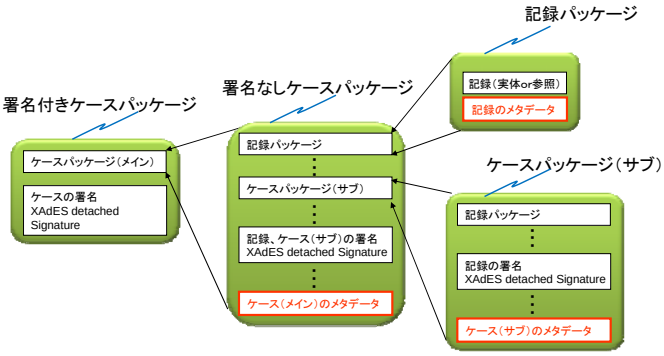

図 10 ケース対応のパッケージ構造

上記のようにケースに対するパッケージを構成すると，記録の容量や数によってはパッケージの容量が膨大となることが考えられる．ケースのパッケージでは主にメタデータやそこ に含まれる記録の包含関係のみを格納し，記録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記録に関する情報としては，URI やユニーク ID 等の記録への参照情報と記録のハッシュ値のみを格納することが考えられる(図 11)．ハッシュ値を格納することにより，参照先の記録やサブケース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が重要である．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して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．

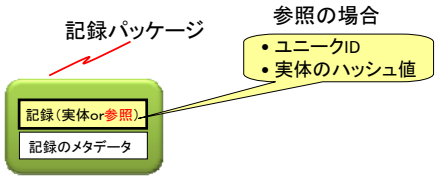

図 11 記録／ケースの格納方法

5. 評価

文献[14]を参考に，ソフトウェアシステムの請負製作業務を題材として評価を試みる．

文献[14]では，ソフトウェアシステムの請負製作における商談から運用終了までの業務フェーズの集合をプロジェ

クトの全体と捉え，その間に発生する全ての記録を一つの案件（ケース）として管理する例を示している．発生する記録及び所管部門は多種多様である（表 1）．

表 1　発生する記録及び所管部門

フェーズ	発生する記録	所管部門
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
	社内見積もり資料	営業
	社内審査記録	営業
	顧客提示見積書、提案書	営業
	契約書	営業
開発	設計書	開発、品証
	実装コード	開発、品証
	試験	開発、品証
	取扱説明書	開発、品証
	協力会社への発注仕様	開発、調達
	協力会社への契約内容	調達
	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
	メンバーの勤怠記録	開発、人事
	旅費、経費等	開発、経理
	メール	多岐
引渡し	検収資料	営業、顧客
保守	保守契約	営業、顧客
	保守状況報告	保守
	障害管理	保守、開発
運用終了	—	—

また，プロジェクト全体に相当するケース（キーケース）に対して 3 つのサブケース（商談，開発，運用・保守）を設けている．この状況を図 12 に示すように簡易化してモデル化し，モデル化された構造をパッケージ構造にどこまで反映可能であるかで評価を行う．

図 12 において，ソフトウェアシステム請負開発プロジェクトの全体をキーケース：プロジェクトとする．この下に商談，開発，保守・運用の 3 つのサブケースが位置付けられる．キーケース及びサブケースのそれぞれにはメタデータが関連付けられる．サブケース：商談及びサブケース：保守・運用には要求仕様書及び保守契約書の実体が記録として直接関連付けられ，それぞれの記録に対してメタデータが関連付けられる．サブケース：開発には設計書に対する参照情報が関連付けられる．設計書の実体はプロジェクト管理ツールによる集中管理を要するなどの運用上の事情により，ケース指向電子記録管理システムとは別管理されるような状況においてこのような構造となる．ただし設計書に関するメタデータはケース指向電子記録管理システムで直接管理される．

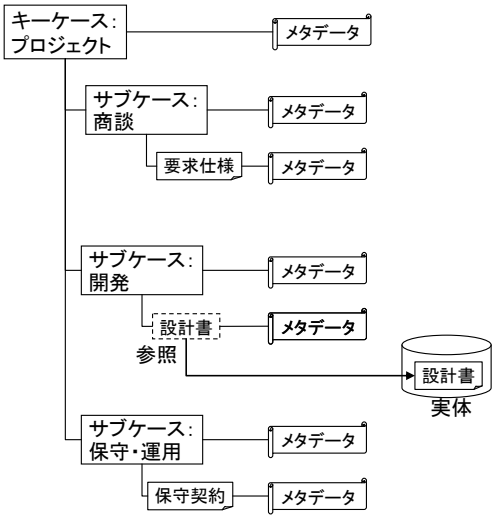

図 12　簡易ケースモデル

図 12 で示したソフトウェアシステム請負開発プロジェクトの簡易ケースモデルを提案するパッケージ構造で示すと図 13 のように表すことができる．

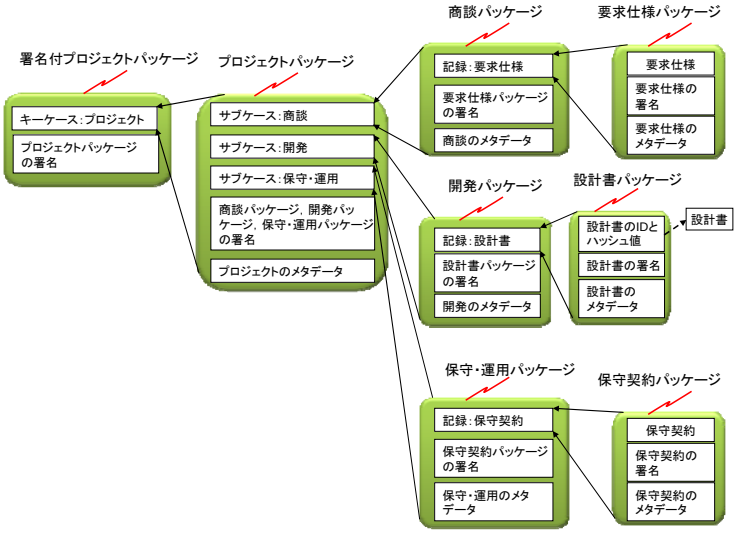

図 13　簡易ケースモデルのパッケージ構造

図 13 より，3 章で挙げた課題 1～3 に対して次のことが確認できる．

[課題 1]

要求仕様，設計書，保守契約の各記録に対して，また商談，開発，保守・運用の各サブケースに対して，そしてプロジェクト全体に対して署名を付与することができる．サブケース以下の署名は署名，署名タイムスタンプ，検証情報までを含む ES-X Long 形式[11][12]とし，プロジェクトパ

ッケージの署名を延長することにより，各記録やサブケースに付与された署名についても有効性を延長することが可能となる．

[課題 2]

キーケースであるプロジェクトに対するパッケージに，商談，開発，保守・運用の 3 つのサブケースをそれぞれパッケージ化して格納できる．この例では現れないが，キーケースが直接記録を含むような構成も可能である．また，キーケース，サブケース，記録のそれぞれに必要に応じてメタデータや署名を付与できる．

[課題 3]

設計書パッケージで示すとおり，設計書実体を含まず，そこへの参照のみを含むようにパッケージを構成できる．参照にユニーク ID を含むことにより，参照先が一意に特定でき，また実体のハッシュ値を含むことにより，実体の非改ざん性の確認，つまり証拠性の確保が可能となる．なお，参照に用いるハッシュ値を算出するためのハッシュ関数の脆弱化が予想される場合，図 14 に示すように，署名付プロジェクトパッケージに充分な強度が保証される新たなハッシュ関数による参照先の実体（設計書）のハッシュ値を含め，プロジェクトパッケージとその署名，そして参照先の新たなハッシュ値に対して取得したタイムスタンプを追加することにより，脆弱化が予想されるハッシュ関数が脆弱化する前のハッシュ値と，新規ハッシュ関数によるハッシュ値との関係を新たに取得したタイムスタンプにおいて保護できるため，旧ハッシュ関数が脆弱化した後でも実体の非改ざん性の保証が可能となる．

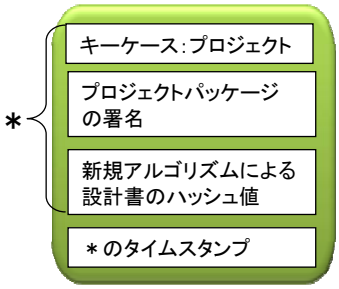

図 14 ハッシュ関数脆弱化への対応

これらにより提案したパッケージ構造を用いることにより 3 章で示した課題を解決できることが確認できた．

一方，明らかに図 5 で示すような既存のパッケージ構造では，3 章で述べたとおり長期署名対応ができないことに加え, 図 12 で示すモデルのような階層化されたケース構造を表現することができない．

6. おわりに

ケース指向電子記録管理システムにおけるパッケージ構造を提案し，ソフトウェアシステムの請負製作プロジェクトへの適用を机上で検討することにより，その有効性を示すことができた．提案したパッケージ構造の構成法によると，長期署名により長期的に証拠性を確保でき，複数の記録を格納でき，階層構造を持つケースにも適用可能で，記録の実体を含まず参照のみを含むようなケースに対応するパッケージ構造が定義できることが確認できた．

今回，パッケージ構造の定性的な評価はできたが性能等の定量的な評価ができていない．今後，運用時の様々な状況を想定した場合のパッケージの処理性能等の評価が課題である．また，パッケージが保持すき具体的なメタデータに関しても，ISO 23081-2[15]をベースとし，更に海外の例も参考にしながら検討することとしたい．

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,情報システムと社会環境研究発表会,IS118-05(2012).
2) 宮崎一哉,木村道弘,前田陽二,辻秀一:証拠性確保を重視した電子記録管理のためのパッケージ構造,情報システムと社会環境研究発表会,IS119-01(2012).
3) 木村道弘,前田陽二,樽美康一,宮崎一哉,辻秀一:電子記録管理システム要件とマチュリティモデル ,DICOMO2012, 5F-1,pp.1305-1310(2012).
4) 宮崎一哉,木村道弘,前田陽二,辻秀一: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―ケースマネジメントへの対応―,DICOMO2012,5F-2,pp.1311 -1317(2012).
5) ISO 15489-1:2001 Information and documentation -- Records management -- Part 1: General(2001).
6) 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(2012).
7) ISO 14721:2003 Space data and information transfer systems -- Open archival information system -- Reference model(2003).
8) Siegfried Hackel,Tobias Schaefer,Wolf Zimmer:Legally compliant long-term preservation of electronic documents,入手先 <http://www.archisafe.de/s/c/g8Bz1iS9/ArchiSafe_Dokumente/ArchiSafe_White_Paper_V12.pdf>(2013.04.30).
9) Microsec Ltd.:Specification of the e-Dossier Format,入手先 <http://www.e-szigno.hu/?lap=edossier30>(2013.04.30).
10) ETSI TS 102 918 v1.1.1:Electronic Signatures and Infrastructures (ESI);Associated Signature Containers (ASiC) (2011).
11) ETSI TS 101 903 V1.4.1：XML Advanced Electronic Signatures - XAdES(2009).
12) ETSI TS 101 733 V.2.2.1：CMS Advanced Electronic Signatures - CAdES(2013).
13) International Digital Publishing Forum, OEBPS Container Format (OCF) 1.0 日本語版,入手先 <http://naoki.sato.name/ocf/ocf_1_0_spec_ja.html>(2013.04.30).
14) 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 2012 (2013).
15) ISO 23081-2:2009 Information and documentation -- Managing metadata for records -- Part 2: Conceptual and implementation issues(2009).