Vol.2012-IS-119 No.1
2012/3/15

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

宮崎一哉[†]　木村道弘[††]　前田陽二[††]　辻秀一[†††]

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

Package Structure for Electronic Records Management Considering Evidence Preservation

Kazuya Miyazaki[†]　Michihiro Kimura[††]　Yoji Maeda[††]
and Shuichi Tsuji[†††]

Package structure for using, preserving and transferring electronic records is proposed. Evidence aspect is important for electronic records, so it is necessary to include electronic signatures in addition to electronic record contents and related meta-information. In this paper, package structure for electronic records management which is extended ASiC (Associated Signature Containers) proposed in order to unify electronic contents and detached signature by European Telecommunications Standards Institute (ETSI) is described.

1. はじめに

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

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

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

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

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

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

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 4) 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は，電子記録の証拠としての証明力が重視される．本稿では，上記電子記録マネジメント基

[†] 三菱電機株式会社
Mitsubishi Electric Corporation
[††]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
[††] 東海大学
Toukai University

盤を想定し，証拠性の確保を重視した電子記録マネジメントのための電子記録の取扱の単位となるパッケージの構造を提案する．

2. 電子記録マネジメント基盤

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

2.1 電子記録

電子記録の定義は ISO 15489-1[5]に準じる．ISO 15489-1 によると，記録とは「法的義務に従い，または商業取引の上で組織または個人が証拠および情報として作成，受領，維持する，全形式の記録された情報」である．

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

文書と記録の相違を文献 4)より引用して表 1 に示す．

表 1　文書と記録の相違点

文　書	記　録
活動の結果	決定や行為の重要な証拠
所有者（通常は作者）の管理下	組織の管理下
自由に変更が可能	変更は不可
自由に削除が可能	通常は削除不可

2.2 電子記録マネジメント

電子記録マネジメントとは，組織による事業継続／発展，リスク回避，権利保護，説明責任などを達成し，それを長期にわたって維持することを目的とした，電子記録の取得，維持，活用等の仕組みであり，その実践である．この定義もやはり ISO 15489-1[5]に準じるものである．文献 4)では， MoReq2（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 101 要件」を策定している．

2.3 電子記録マネジメント基盤

電子記録マネジメント基盤は，電子記録マネジメントの主要 101 要件に沿って電子記録マネジメントを実現する基盤（プラットフォーム）である[4].

電子記録マネジメント基盤の位置付けを図 1 に示す。

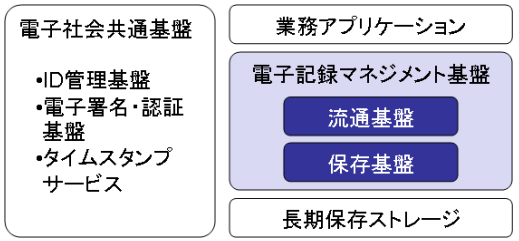

図 1　電子記録マネジメントシステムの構造と電子記録マネジメント基盤の位置付け

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

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

2.4 ケースマネジメント

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

- 決定過程を含めた記録の管理
- 記録の利活用の促進

である．

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

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

利活用促進のためには，様々な角度からの検索を容易とするために，記録の時系列

的な並びと発生事象（作成，受け取り，配布，参照など），記録相互の因果関係，関係者などのメタデータを管理する仕組みが必要となる．

3. パッケージ

3.1 パッケージの参照モデル

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

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

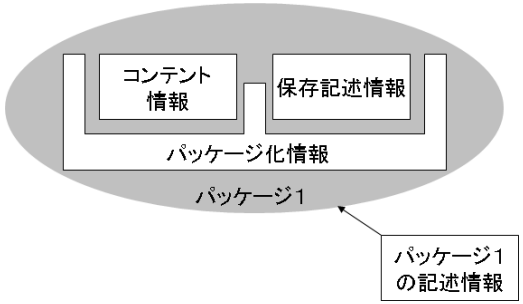

図 2　OAIS 参照モデル―パッケージの構造

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

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

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．

- 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　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 4 に示す．

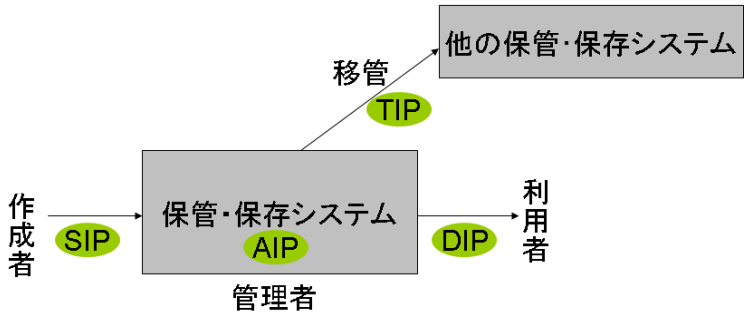

図 4　OAIS の拡張

3.2 Associated Signature Containers (ASiC)

欧州電気通信標準化機構（ETSI）では，コンテンツと電子署名あるいはコンテンツとタイムスタンプを一体化するためのパッケージとして Associated Signature Containers (ASiC)[7]を提案している．

ASiC の基本構造は次の通りである．

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

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一つ以上の署名やタイムス

タンプを含むコンテナ

- ASiC-E（拡張型 ASiC）：複数のデータオブジェクトとそれぞれに対する一つ以上の署名やタイムスタンプを含むコンテナ

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

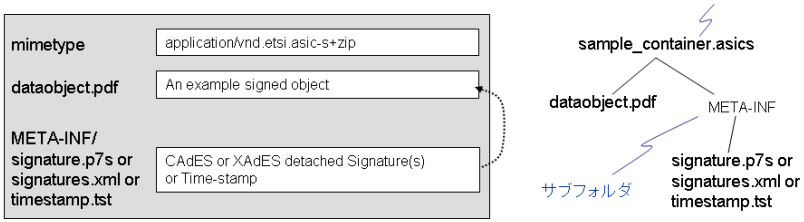

図 5　ASiC-S の構造とフォルダ構造の例

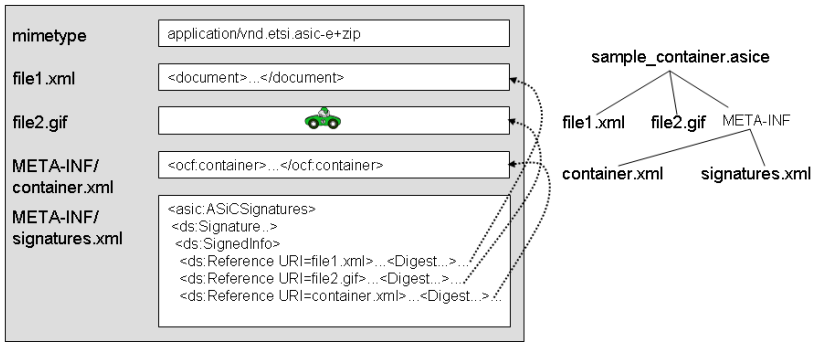

図 6　ASiC-E[XAdES を含む形式]の構造とフォルダ構造の例

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 8 に示す．

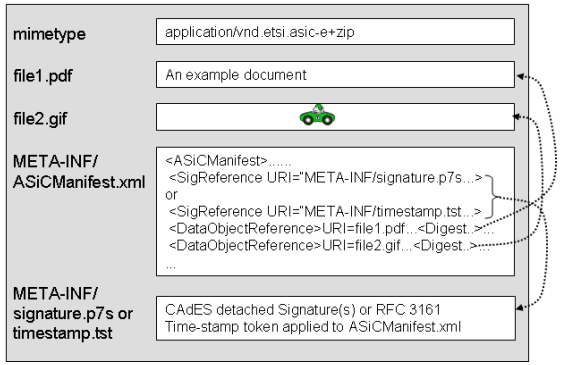

図 7　ASiC-E[CAdES またはタイムスタンプを含む形式]の構造の例

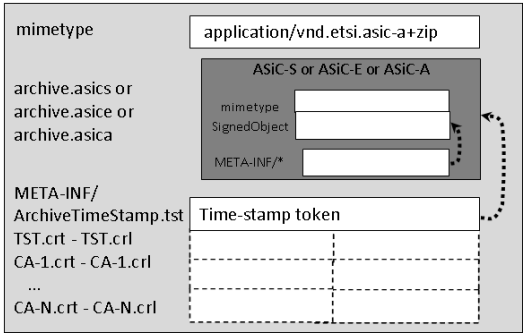

図 8　ASiC-A：長期検証型 ASiC の構造の例

3.3 証拠性確保を重視した電子記録マネジメントのためのパッケージ構造提案

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

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

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

[要件 3] 電子記録マネジメント基盤に対して，記録の受取り／保存／配布／移管を行なうにあたっては，添付可能な，あるいは添付を必要とされるメタデータが異なる

ことが考えられる．また，電子記録マネジメント基盤での管理期間中にメタデータが追記あるいは変更される可能性もある．メタデータが更新可能であることを考慮する必要がある．

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

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

まず, [要件 1]に対応するために長期署名をサポートする構造とすることを前提とする．そのためには XAdES[8]や CAdES[9]自体をパッケージの基本構造とすることも考えられるが，[要件 2]の長期署名以外のメタデータを含めるには XAdES や CAdES は適当な格納場所が用意されていない．そこで ASiC を基本構造とすることを考える．ASiC には 3.2 で示した異なる形式がある. 管理対象が単一のファイルであれば ASiC-S を用いることができる．長期間証拠性を維持するためにはアーカイブタイムスタンプの追加付与が必要であるが, ASiC-S を用いた場合, CAdES を利用した場合でも XAdES を利用した場合でも署名を格納するためのファイル（CAdES の場合 META-INF/signature.p7s，XAdES の場合 META-INF/signature.xml）を，アーカイブタイムスタンプを追加したファイルと置き換えることによって可能となる．

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

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

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

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

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

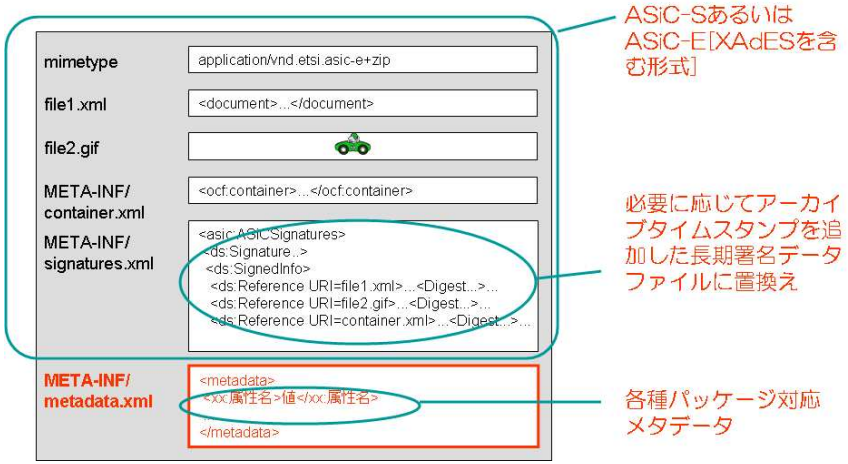

図 9　ASiC をベースとした電子記録マネジメントのためのパッケージ構造案

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

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

[要件 5]に対応するためには, 図 9 に示したパッケージ案をもとに, 提出用, 保存用, 配布用，移管用のメタデータを定義すればよい．これについては 4 章に記述する．また，配布用あるいは移管用にメタデータを含めた正当性を保証する必要がある場合，図 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．

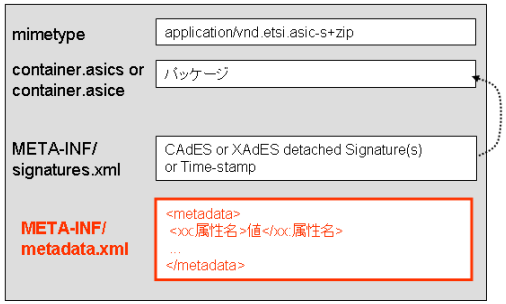

図 10　メタデータ自体を記録としたい場合のパッケージ構造例

4. メタデータ

4.1 メタデータモデル

メタデータについては 3.1 に示した OAIS 参照モデルでも触れたが，記録管理におけるメタデータの全体像を示すメタデータモデルが ISO 23081-2:2009[11]で定義されている．その中で，図 11 に示すように 6 種類のメタデータを定義している．

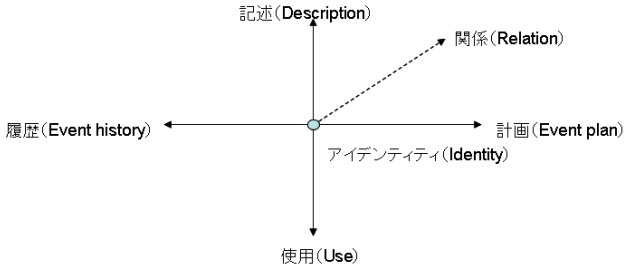

図 11　メタデータの種類と関係

6 種類のメタデータの概要を次に示す。

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

4.2 電子記録マネジメントのためのパッケージで考慮すべきメタデータ

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

(1) SIP

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

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

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

(2) AIP

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

また，計画，履歴，関係の保持／更新は必須である．

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

(3) DIP

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

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

(4) **TIP**

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

上記を表 2 にまとめる．ただし，記述及び使用は個々のメタデータ項を示し，計画，履歴，関係はメタデータの構造を示す．

表 2　各パッケージとメタデータの関係

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

5. おわりに

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

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

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

参考文献

1) 一般社団法人　電子情報技術産業協会，「データマイグレーションの必要要件」 http://home.jeita.or.jp/is/committee/tech-std/std/data_migration_201101.pdf
2) 厚生労働省，「医療情報システムの安全管理に関するガイドライン 第 4.1 版」 http://www.mhlw.go.jp/shingi/2010/02/dl/s0202-4a.pdf
3) University of Southern California, 「How Much Information Is There in the World?」 http://uscnews.usc.edu/science_technology/how_much_information_is_there_in_the_world.html
4) 木村道弘，前田陽二，辻秀一：クラウド時代の情報流通基盤，情報処理学会，第 118 回 情報システムと社会環境研究発表会, IS118-05(2012).
5) ISO 15489-1:2001 Information and documentation -- Records management -- Part 1: General
6) ISO 14721:2003 Space data and information transfer systems -- Open archival information system -- Reference model
7) ETSI TS 102 918 v1.1.1 (2011-04):Electronic Signatures and Infrastructures (ESI) ; Associated Signature Containers (ASiC)
8) ETSI TS 101 903 V1.4.1：XML Advanced Electronic Signatures - XAdES
9) ETSI TS 101 733 V.1.7.4 ：CMS Advanced Electronic Signatures - CAdES
10) International Digital Publishing Forum, OEBPS Container Format (OCF) 1.0 日本語版, http://naoki.sato.name/ocf/ocf_1_0_spec_ja.html
11) ISO 23081-2:2009 Information and documentation -- Managing metadata for records -- Part 2: Conceptual and implementation issues