電子署名JIS制定の背景と今後の展望

2008年7月3日

ECOM電子署名普及WG
木村道弘 (NEC)

目次

- JIS化のきっかけ
- JIS制定に至るまで
- 何故長期署名なのか
  アルゴリズム危殆化への備え
- 電子記録のリスク対策
- 今後の展望

JIS化のきっかけ

- 2005年(平成17年) 4月，e-文書法施行
  - 民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律(平成16年法律第149号)
  - 民間事業者等が法令により書面で保存、作成、縦覧、交付等を義務付けられていたものを電子的に可能とする法律
- 真正性 (何時，誰が，何を) を証明できなければ証拠として認められない (自由心証主義)

  しかしながら，署名やタイムスタンプの技術的な基準がない
  - 先行省庁は個別に要件を提示するものの，仕様の提示がないことから，製品間の相互運用性が保てない
  - 紙と同じ保存期間が適用され，長期署名は不可欠 (何も対策を施さないと，証明書の期限切れ以降は署名の検証ができない)

「電子帳簿保存法取扱通達の制定について」の一部改正について（法令解釈通達）

平成17年2月28日
国税庁長官

平成10年5月28日付課法5-4ほか6課共同「電子帳簿保存法取扱通達の制定について」（法令解釈通達）の一部を下記のとおり改正したから、今後はこれによられたい。

（省略）

（タイムスタンプの付し方）

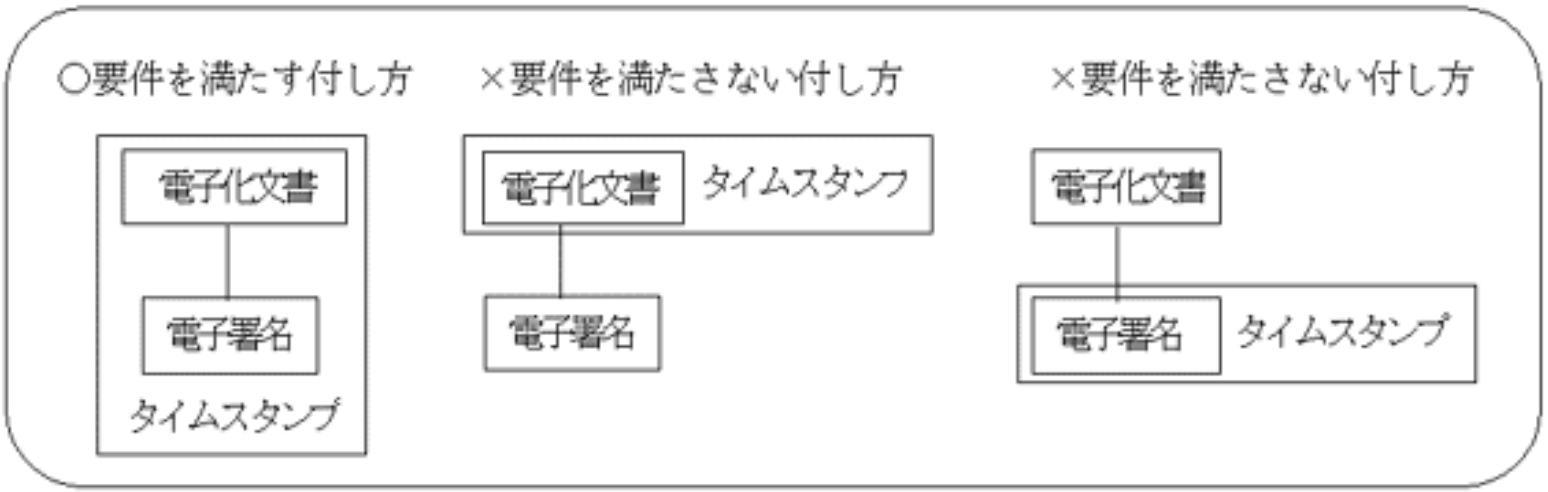
4－28 規則第3条第5項第2号ハ（（タイムスタンプ））の規定の適用に当たり、「電子署名が行われている当該国税関係書類に係る電磁的記録の記録事項」とは、電子署名を行うことにより作成された電磁的記録の記録事項（以下4－28において「電子署名データ」という。）及び国税関係書類に係る電磁的記録の記録事項（以下4－28において「画像データ」という。）の両方を指すのであるから、電子署名データと画像データの両方を対象として、一のタイムスタンプを付す必要があることに留意する。

（以下省略）

「『電子帳簿保存法取扱通達の制定について』の一部改正について」（法令解釈通達）等の趣旨説明について

【解　説】

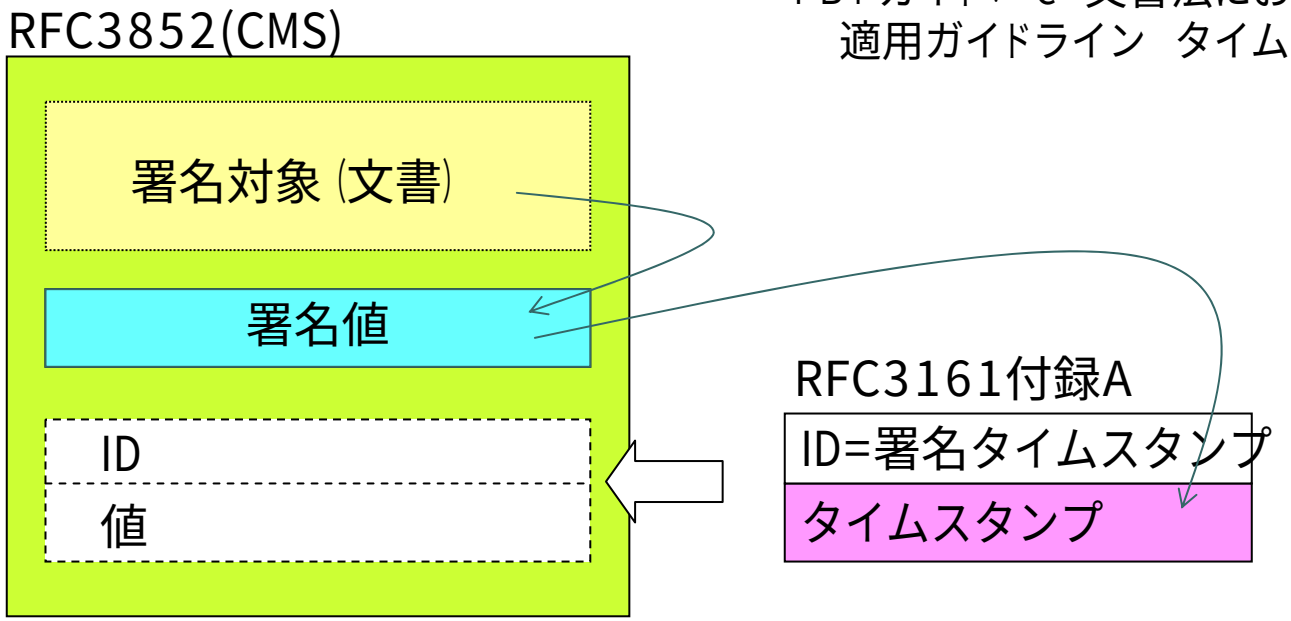
規則第3条第5項第2号ハでは、電子署名が行われている画像データにタイムスタンプを付すこととされている。ところで、画像データに電子署名を行う場合、電子署名データと画像データが一つのファイルとなる場合のほか、画像データのファイルと電子署名データのファイルの2つのファイルとなる場合がある。電子署名が行われている画像データとは、電子署名データと画像データと解されることから、電子署名データと画像データが一つのファイルとなる場合だけでなく、2つのファイルとなる場合であっても、タイムスタンプは画像データ及び電子署名データの両方に付すこととなる旨を明らかにしたものである。この内容を図示すれば次のとおりとなる。



タイムスタンプに関する問題点

	RFC	電子帳簿、医療情報
付与対象	署名値	本文＋署名
付与規程	CMS＋RFC3161付録A	未定義
長期署名	RFC3126	未定義
備考	TBFガイド　例1	TBFガイド　例2

ＴＢＦガイド：　e-文書法におけるタイムスタンプ
適用ガイドライン　タイムビジネス推進協議会



JIS制定に至るまで

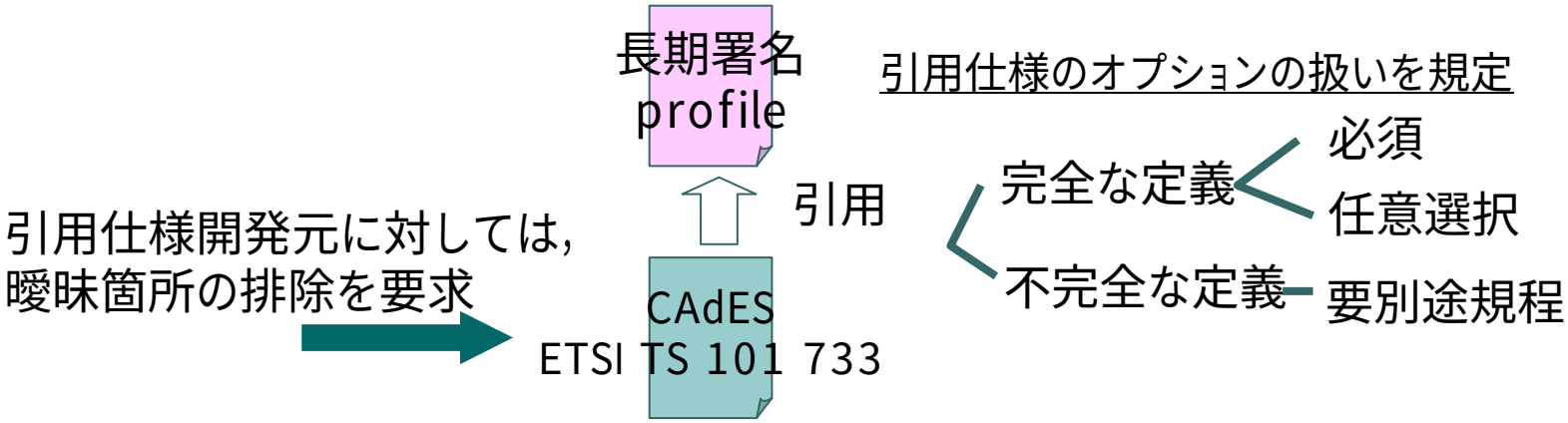
- JIS X 5092　CMS利用電子署名（CAdES）のプロファイル
- JIS X 5093　XML署名利用電子署名（XAdES）のプロファイル

経緯

- ２００６年5月　　12条案件として申請
- ２００６年6月　　原案作成作業部会発足
- ２００６年１１月　原案作成委員会承認
- ２００６年１２月　原案を規格協会に送付
- ２００７年3月～　規格協会との調整
- ２００７年6月　　規格調整分科会
- ２００8年2月　　JISC情報技術専門委員会
- ２００８年3月　　発行

何故プロファイルなのか

- 必要な仕様は各機関で開発済み/開発中である
- 相互運用の観点からの実装規定が欲しい



- JIS化に当たっての問題
  - 引用規格
  - 文章の書き方 (引用仕様の用語との対応)
  - 規格適合性

JIS Z 8301
規格票の様式及び作成方法

6.2.3 引用規格

引用規格の箇条には，その規格の規定の一部を構成するために必要な日本工業規格，国際規格又はこれらに準じる規範文書を引用規格として列記する。ただし，次のものは引用規格とはしない。

- 一般に利用できない参考文献
- 単に情報として利用する参考文献
- 参考的要素（3.15 参照）及び参考事項（注記，例などで示す参考事項）の中で引用する規格又は規範文書
- TS 及びTR

附属書G（規定）　文章の書き方，用字，用語，記述符号及び数字

G.1 文章の書き方

文章の書き方は，次による。

a) 文章 文章は，漢字仮名混じり文とする。
b) 文体 文体は，文章口語体とする。
c) 書き方 書き方は，左横書きで箇条書きとする。

引用規格の拡大

JIS X 5092本体

1　適用範囲

この規格は，長期署名プロファイルのうち，CMS利用電子署名 (CAdES) に関するプロファイルについて規定する。

2 引用規格

次に掲げる規格は，この規格に引用されることによって，この規格の規定の一部を構成する。バージョン指定のない引用規格は，その最新版（追補を含む。）を適用する。

JIS X 0001　情報処理用語－基本用語

JIS X 0008　情報処理用語－セキュリティ

ETSI TS 101 733　CMS Advanced Electronic Signatures (CAdES)　v1.7.3

注記　http://pda.etsi.org/pda/queryform.aspから入手可能。

供給者適合宣言

JIS X 5092附属書 (規定)

長期署名プロファイル供給者適合宣言書

番号:
発行者の名称:
発行者の住所:
宣言の対象:
上記宣言は, 次の長期署名プロファイルに適合している:
JIS X 5092:2008 CAdES-T 及び／又は JIS X 5092:2008 CAdES-A
実装されている要素は, 別紙のとおりである。
追加情報:
(ここに動作確認結果などを記載することができる。)
代表者又は代理者の署名:
(発行場所及び発行日)
(氏名, 役職)

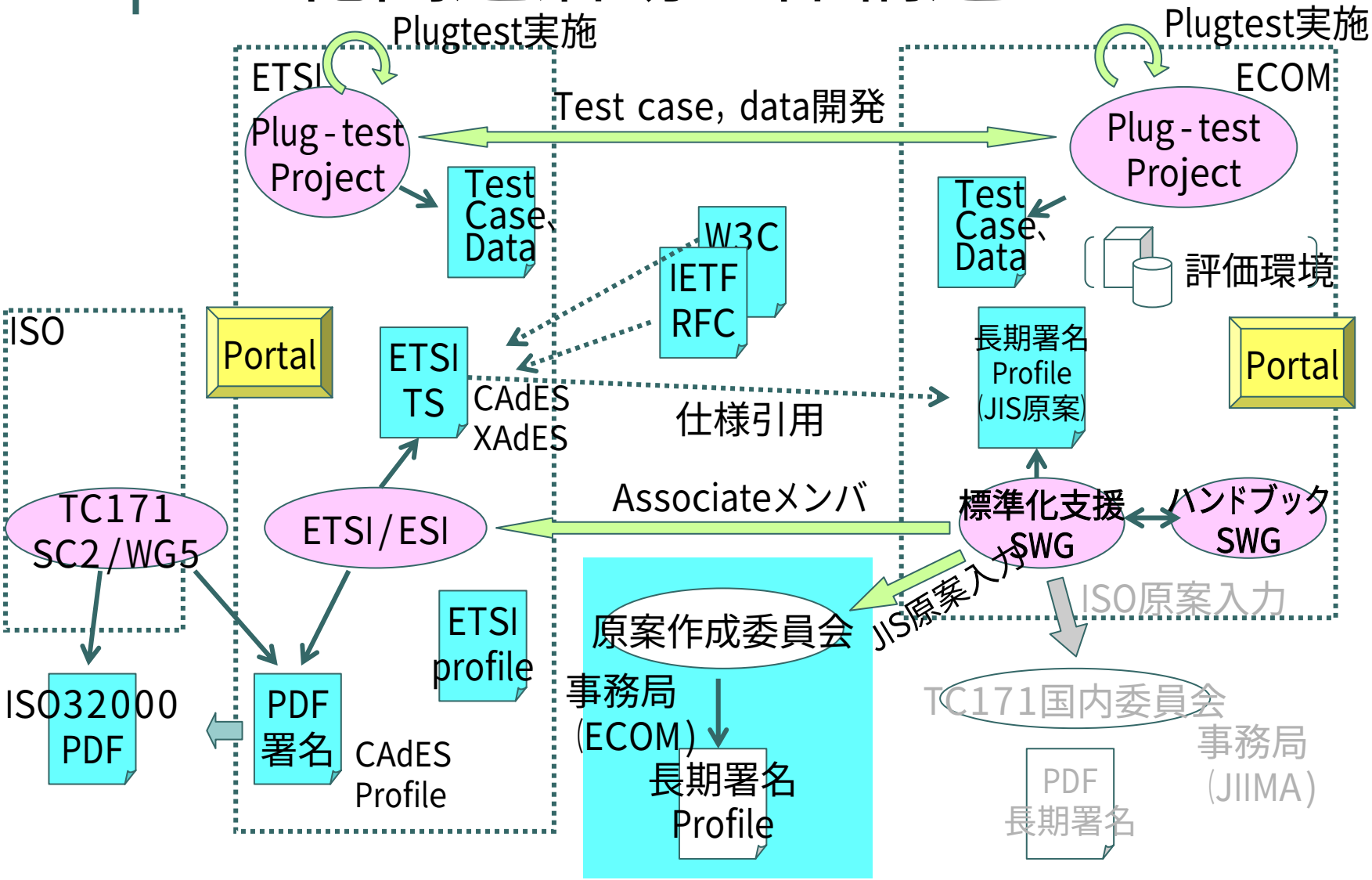
表A.4－署名属性

要素	要求レベル	生成	検証
コンテント種別	必す	レ	レ
メッセージダイジェスト	必す	レ	レ
署名者証明書の参照情報	必す	レ	レ
- ESS署名者証明書の参照情報	任意選択		レ
- ESS署名者証明書の参照情報2版	任意選択	レ	レ
- 他の署名者証明書の参照情報	要別途規定		
署名ポリシ識別子	要別途規定		
署名時刻	任意選択	レ	レ
コンテント参照情報	要別途規定		
コンテント識別子	要別途規定		
コンテントのヒント	要別途規定		
コミットメント識別表示	要別途規定		
署名者所在地	要別途規定		
署名者の属性情報	要別途規定		
コンテントタイムスタンプ	要別途規定		

表A.5－非署名属性

要素	要求レベル	生成	検証
カウンタ署名	任意選択	レ	レ
(署名時刻を確定する情報)	必す	ー	ー
- 署名タイムスタンプ	任意選択	レ	レ
- タイムマークなどその他の方式	要別途規定		

JIS化関連活動全体構造



相互運用性テスト（2007年度）
国内外２１社参加

①共通データ検証機能標準準拠性テスト
　ツールによるオフラインでの検証
②署名生成・検証相互運用性テスト
　各社製品間の相互運用テスト
③国際相互運用性テスト
　海外企業と国内各社による相互運用性テスト

参加企業（五十音順）

CAdES　（参加16社）

ＲＳＡセキュリティ㈱　エントラストジャパン㈱　サートラスト㈱　㈱スカイコム　セコム㈱　㈱帝国データバンク　日本電気㈱　㈱日本電子公証機構　㈱ハイパーギア　㈱ＰＦＵ　ビーパークテクノロジー㈱　三菱電機㈱　三菱電機インフォメーションシステムズ㈱　㈱リコー　Cryptolog International SAS (フランス)　Safelayer Secure Communications, S.A. (スペイン)

XAdES（10社）

エントラストジャパン㈱　関電システムソリューションズ㈱　大日本印刷㈱　東北インフォメーションシステムズ㈱　日本電気㈱　富士ゼロックス㈱　三菱電機㈱　(有)ラング・エッジ　Cryptolog International SAS (フランス)　⑩　Safelayer Secure Communications, S.A. (スペイン)

協力企業

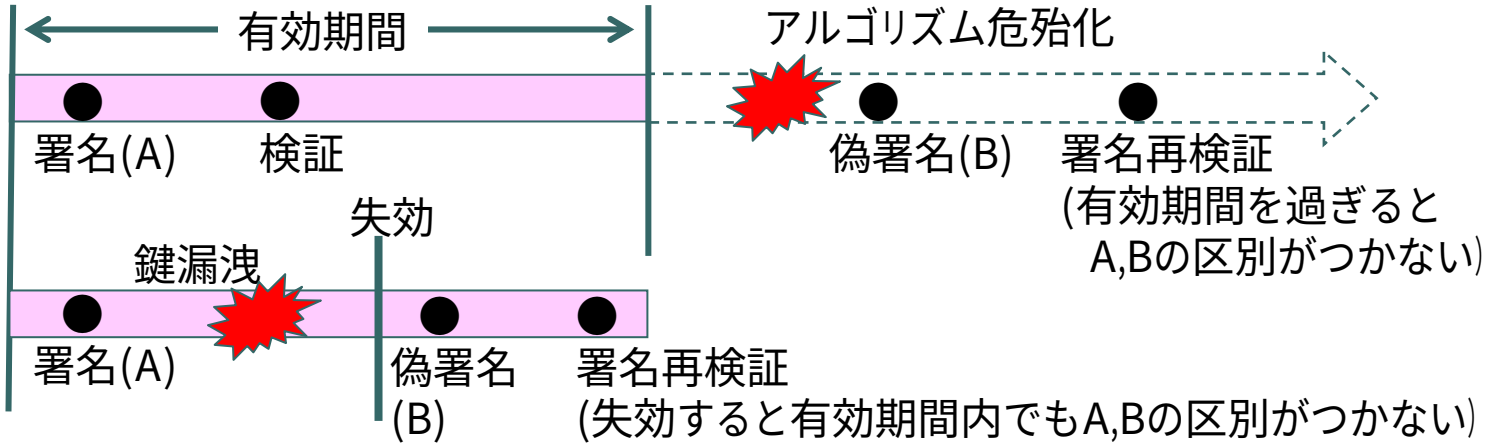
1．テスト用タイムスタンプサービス提供
　アマノタイムビジネス㈱　セイコープレシジョン㈱　㈱ＰＦＵ

2．テスト設計・テストデータ作成
　エントラストジャパン㈱　日本電気㈱　セコム㈱

何故長期署名なのか
～デジタル署名の限界～

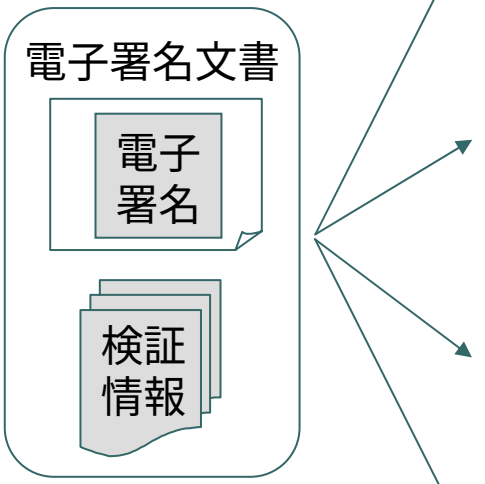
- 署名鍵は、盗難にあったり偽造されると真偽の区別が付かないため。。
  - 盗難/失格対策　→　失効の仕組みを導入
  - 偽造対策　→　有効期限を設定

しかしながら。。
署名の真偽が確認できるのは、有効期間内かつ失効がないときのみ
（それ以外は真偽の区別がつかない）



? 失効が発生しても有効期間が過ぎても、署名がかって有効であったことを検証（署名再検証）できないか

署名再検証を可能にする各種方式



タイムスタンプを重ねる

長期署名フォーマット
(ECOM推奨)

特徴
・第三者による検証が可能
・他の実装に移行が可能
・最新署名技術の適用が可能
・ＴＴＰはＣＡとＴＳＡのみ
・複数タイムスタンプの取得による安全性強化

耐タンパなH/Wに格納する

原本管理装置

厳密運用で安全に保管する

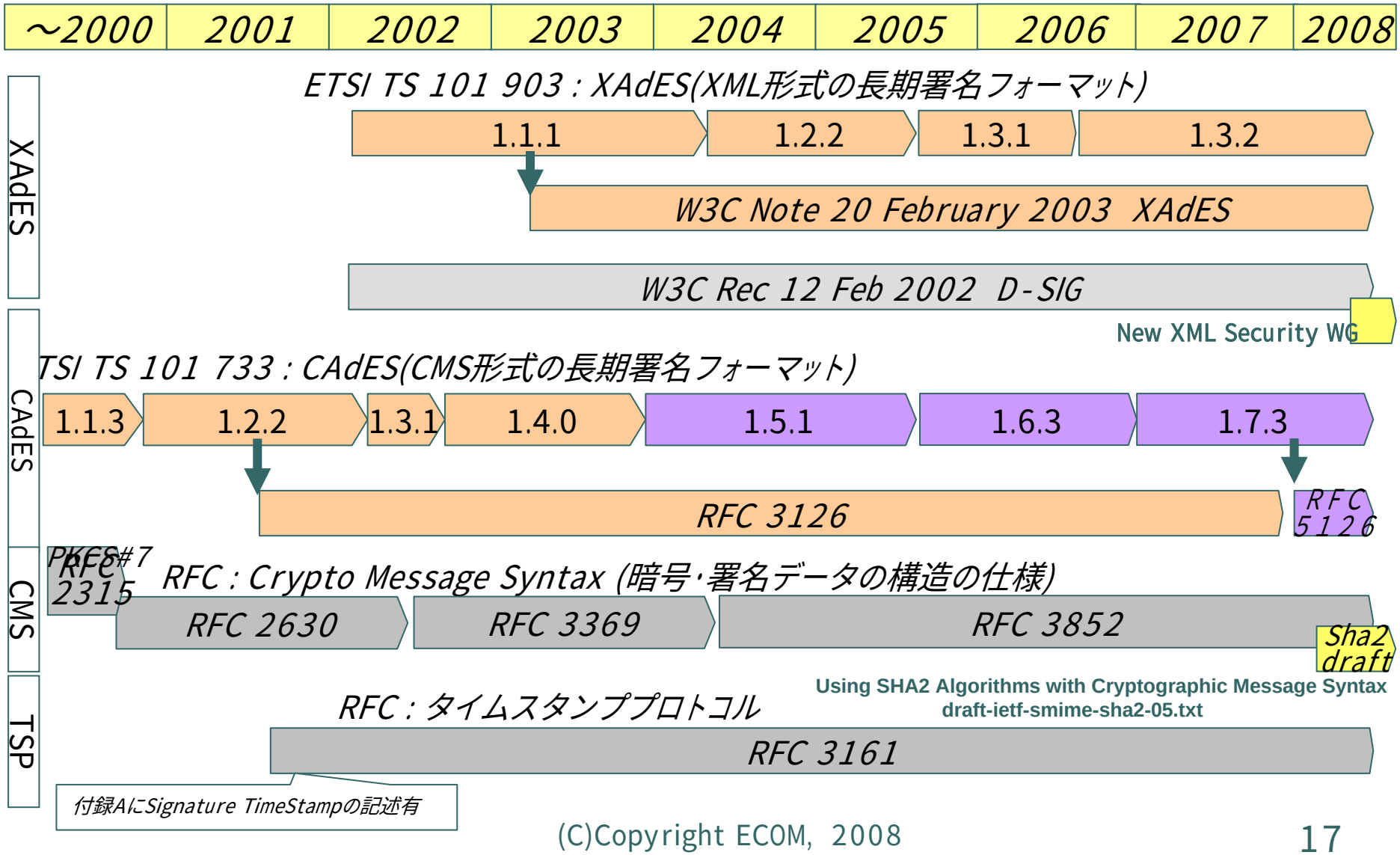
セキュア保管型長期保存

(電子) 公証人に預ける

公証役場による (電子) 公証サービス

署名再検証を可能にするには
①署名時刻を確定し
②検証情報を安全に保管

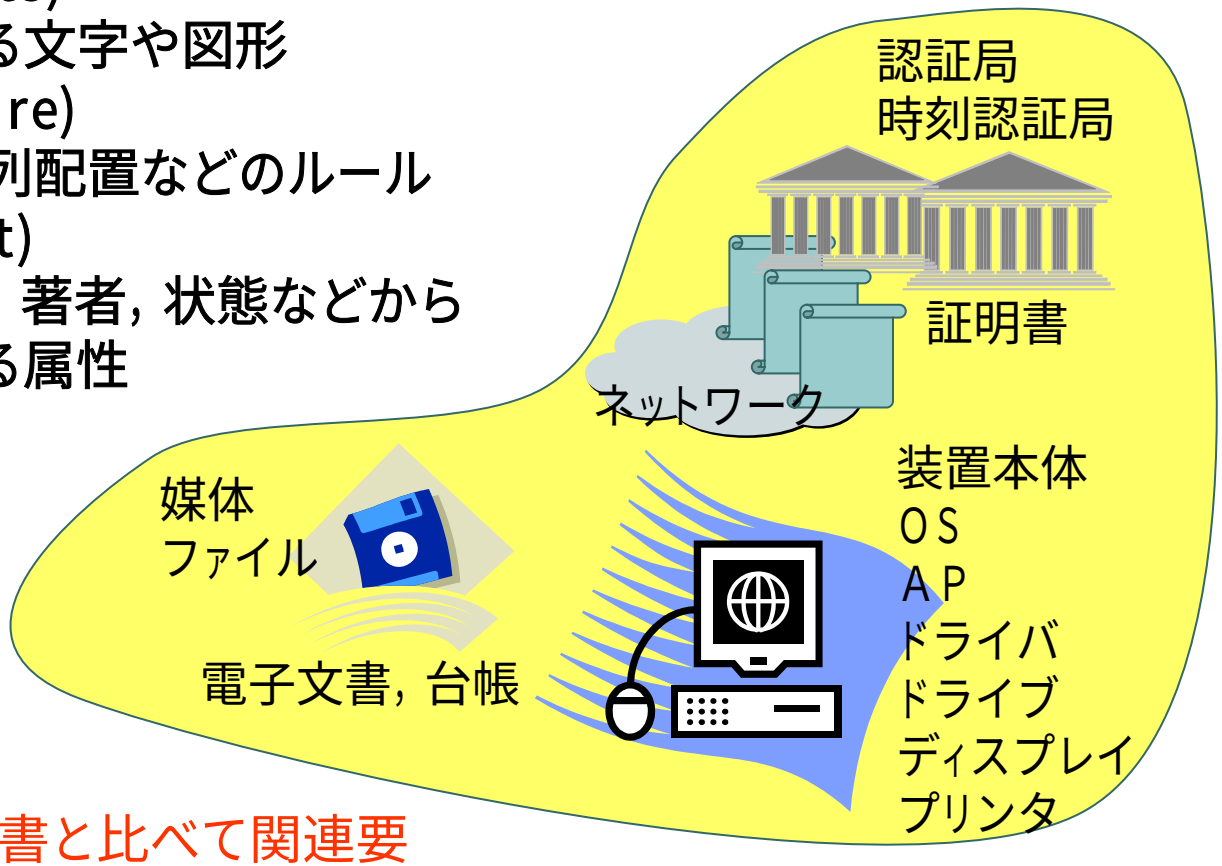
長期署名標準化経緯



電子文書の長期保存要件

文書を構成する要素

- 内容(Contents)
  - 意味のある文字や図形
- 構造(Structure)
  - 文字の配列配置などのルール
- 文脈(Context)
  - 作成日付，著者，状態などから判断できる属性



電子文書は，紙文書と比べて関連要素が多岐にわたる

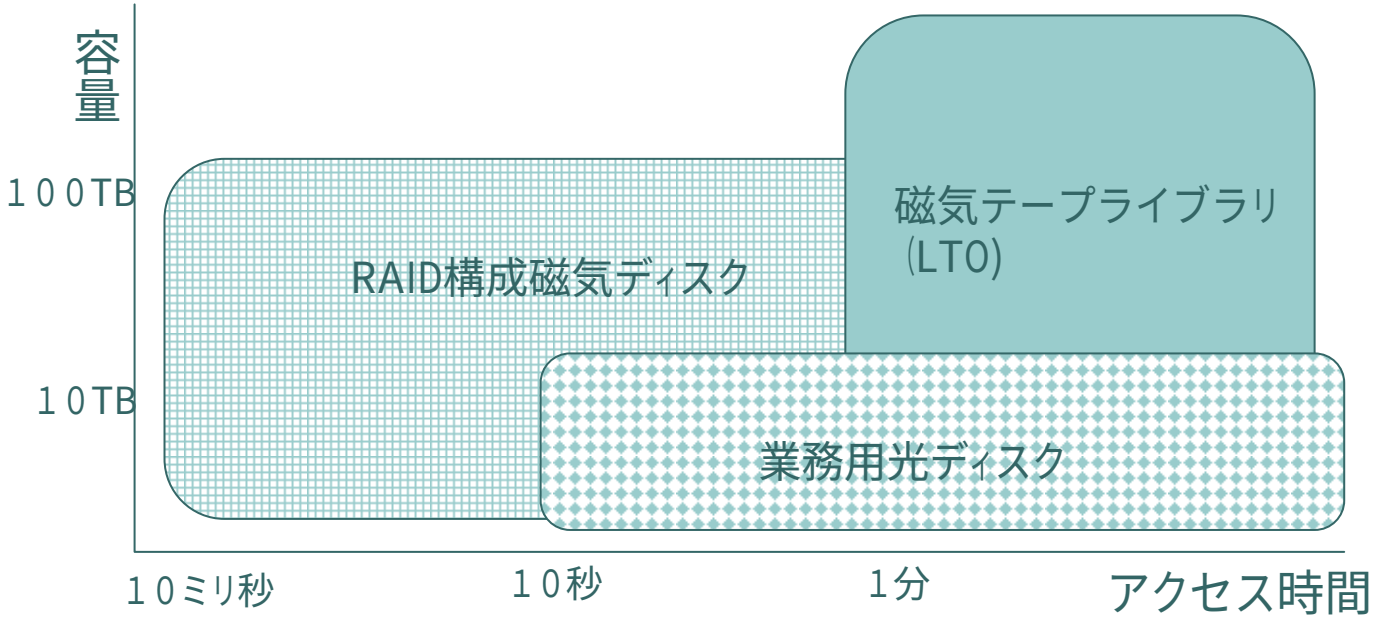
電子文書長期保存問題と対策

問題		原因（長期保存阻害要因）	対策
1	文書の所在不明(散逸)	・管理システム不在，不整合 ・検索方式不整合	問題が発生する前にコントロール可能な適切な措置を行い、問題の発生に至らないようにする
2	正しく読めない，表示されない	・記録媒体劣化 ・機器保守停止 ・ファイル，OS，AP後方非互換 ・罹災（破壊）	
3	真正性を検証できない	・署名検証情報提供停止 ・署名アルゴリズム危殆化 ・コンテキスト情報不足	

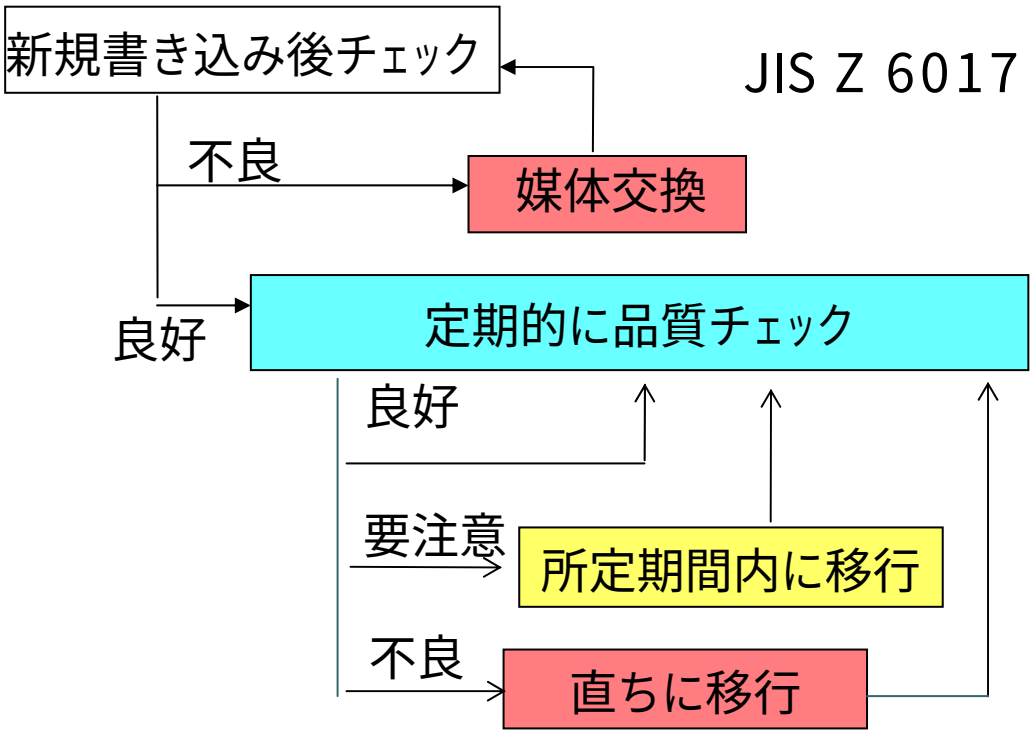
長期保存ストレージの管理

容量，アクセス時間，転送速度，消費電力，コストを勘案して階層化

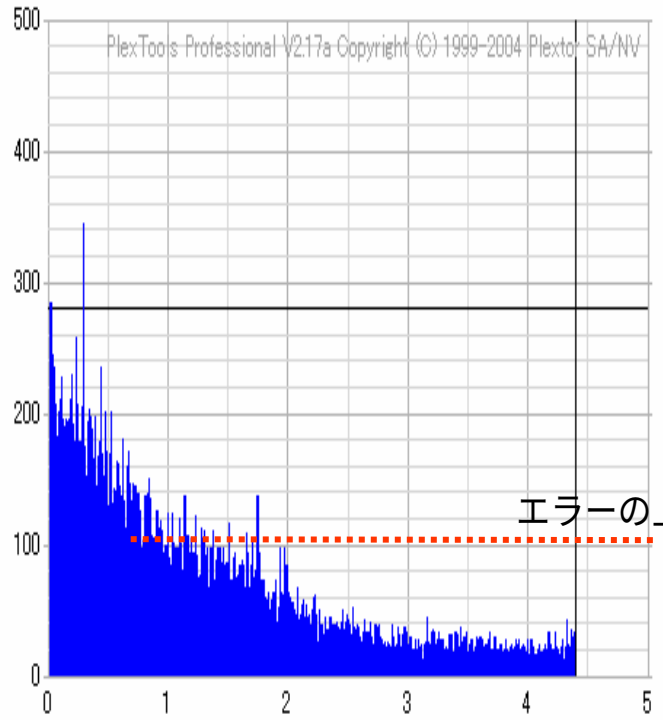
	容量	アクセス時間	転送速度	消費電力	コスト
RAID構成磁気ディスク	大	小	大	大	大
業務用光ディスク	小	中	小	小	小
磁気テープライブラリ	大	大	大	小	小



高品質媒体の選定とマイグレーション



JIS Z 6017

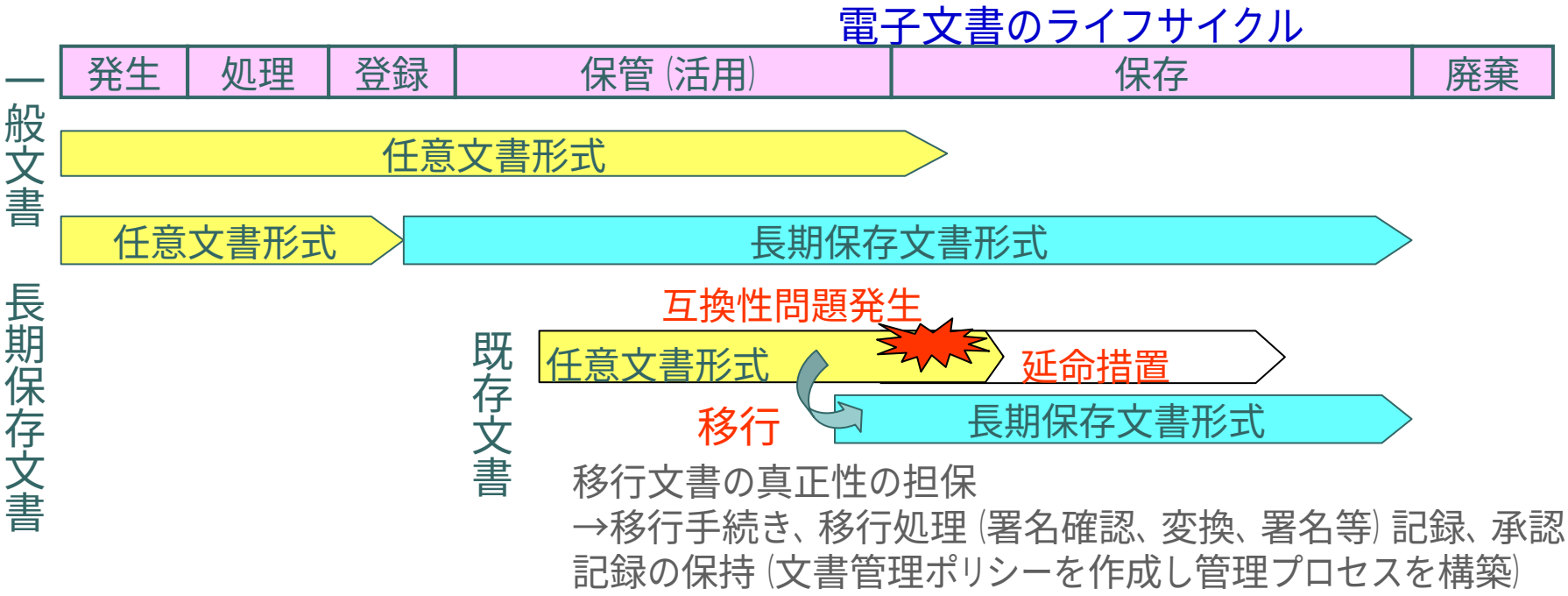


不良媒体(DVD)の例

長期保存に適したファイル形式（文書形式）の選択

- 推奨ファイル形式

  ＴＩＦＦ形式，ＰＤＦ形式，ＭＬ形式　注）



注　ISO32000 PDF, ISO19005 PDF/A
　　ISO26300　Open Document Format (ODF)
　　DIS29500　Office Open XML

記録の管理

記録管理プロセス及びコントロール

- 文書の決定 Determining documents to be captured into a record system)
- 記録の保存期間の決定 Determining how long to retain records)
- 記録の取込み（メタデータ埋込み） Records capture
- 登録 Registration
- 分類 Classification
- 収納及び取扱い Storage and handling
- アクセス　Access
- 追跡　Tracking
- 処分の実施 Implementing disposition
- 記録管理プロセスの文書化 Documenting records management processes
- 監視と監査　Monitoring and auditing
- 研修 Training

（ISO15489/JIS X 0902）

メタデータの管理

- 管理(administrative)
  - 入手経路，配置
- 記述(descriptive)
  - 目録（検索用）
- 保存(preservation)
  - 保存処置
- 技術(technical)
  - HW/SW/認証情報
- 利用(use)
  - 利用者追跡

	要素名
1	タイトル(Title)
2	作成者(Creator)
3	主題(Subject)
4	内容記述(Description)
5	公開者(Publisher)
6	寄与者(Contributor)
7	日付(Date)
8	資源タイプ(Type)
9	フォーマット(Format)
10	資源識別子(Identifier)
11	情報源(Source)
12	言語(Language)
13	関係(Relation)
14	時間的空間的範囲(Coverage)
15	権利関係(Rights)

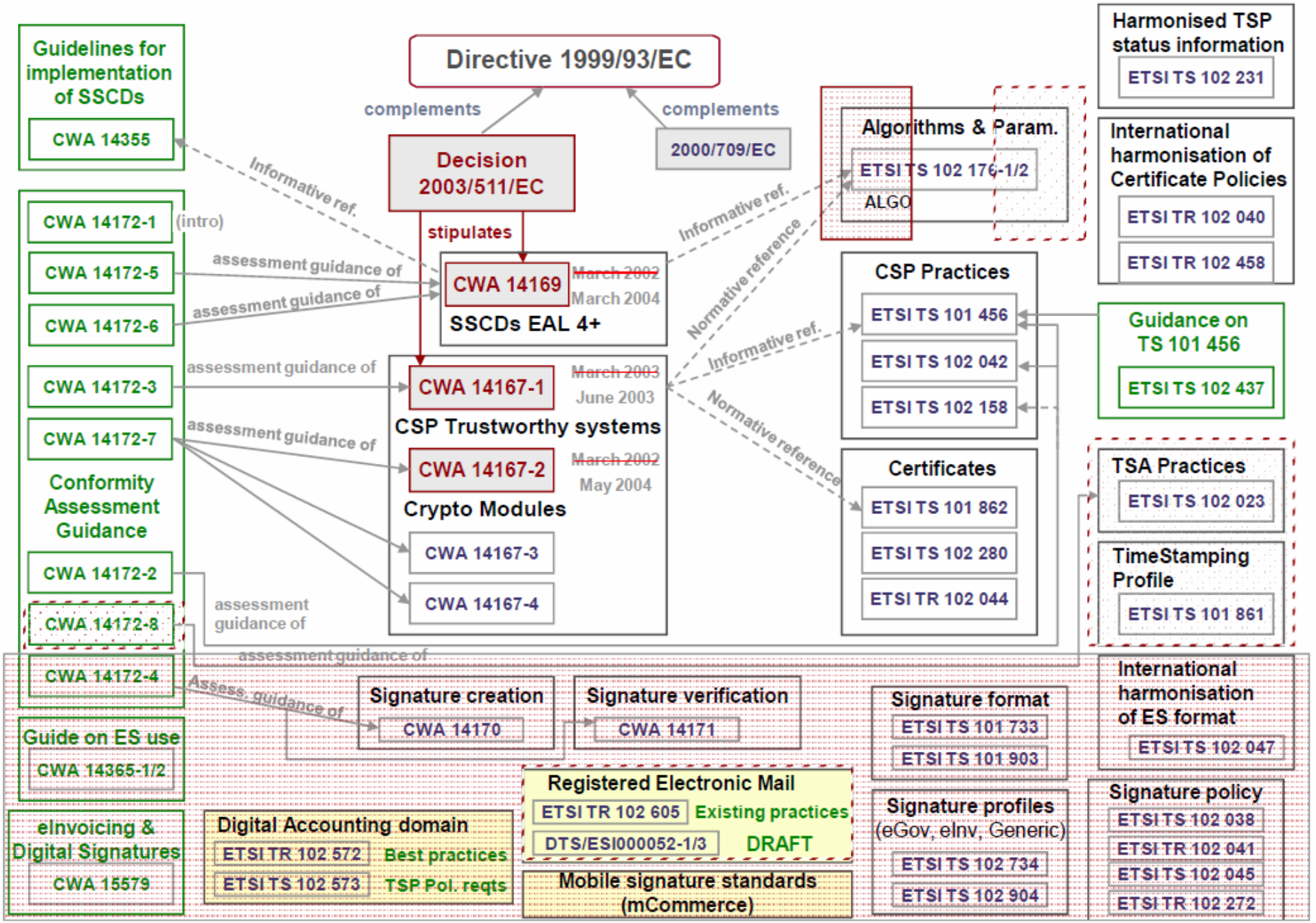
ISO15836　Dublin Core

今後の展望

- 全体Map（利用，標準，法令・ガイドライン）
  - 使われ方，ポリシ，プロファイル
  - 認証局，証明書，タイムスタンプ
  - 署名生成・検証処理，署名フォーマット
  - 暗号アルゴリズム，暗号モジュール，暗号デバイス注

    注　SSCD : Secure Signature-Creation Device
- 懸案事項
  - 一括アーカイブタイムスタンプ
  - 複数署名
  - 名前空間
  - トラストアンカ
- 記録管理
  - 実態調査，ガイドライン策定
  - メタデータ定義

EU eSignature Standardisation Work overview



CAdESのReference

	タイトル	引用内容
1	ITU-T Recommendation X.509 / ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".	属性証明書
2	IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".	証明書/CRL
3	IETF RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".	OCSP
4	IETF RFC 3852: "Cryptographic Message Syntax (CMS)".	CMS
5	IETF RFC 2634: "Enhanced Security Services for S/MIME".	ESS
6	IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".	MIME形式
7	IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".	タイムスタンプ
8	ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".	ASN.1
9	ITU-T Recommendation X.501 / ISO/IEC 9594-1: "Information technology - Open Systems Interconnection - The Directory: Models".	署名者の属性情報
10	IETF RFC 3370: "Cryptographic Message Syntax (CMS) Algorithms".	CMS
11	ITU-T Recommendation F.1: "Operational provisions for the international public telegram service".	署名者所在地
12	ITU-T Recommendation X.500: "Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services".	名前形式
13	IETF RFC 3281: "An Internet Attribute Certificate Profile for Authorization".	属性証明書
14	ITU-T Recommendation X.208 (1988): "Specification of Abstract Syntax Notation One (ASN.1)". NOTE: ITU-T Recommendation X.208 has been withdrawn on 30 October 2002 as it has been superseded by ITU-T Recommendations X.680-683. All known defects in X.208 have been corrected in ITU-T Recommendations X.680-683 (1993) further revised in 1997 and 2002. However, the reference is kept in the current to ensure compatibility with RFC 3852 [4].	ASN.1
15	IETF draft-ietf-smime-escertid-03.txt (December 2006): "ESS Update: Adding CertID Algorithm Agility" J. Schaad. http://www.ietf.org/internet-drafts/draft-ietf-smime-escertid-03.txt. NOTE: This Internet Draft is due to be shortly published as an Internet RFC. The present document will be re-issued with the RFC reference when it becomes available.	ESS追加

参考文献

- ECOM推薦図書
  電子文書保存の仕組みと実務（中央経済社）
  ～記録管理の基本と標準化～