Entrust® Securing Digital Identities & Information

Securing Your Digital Life

長期署名フォーマットの標準化と日欧相互運用実験

於：日本ネットワークセキュリティ協会
JNSA PKI Day 2007 - ＜PKIの過去、現在、未来＞ 2007年06月25日

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実証実験プロジェクトリーダー

エントラストジャパン株式会社　漆嶌 賢二

Entrust Securing Digital Identities & Information

本日の内容

- 文書を保存する際、デジタル署名だけではだめなのでしょうか？(+ デモ)

- 長期署名フォーマット CAdES / XAdES
  - CMS/PKCS#7/XML署名の拡張。データ単体で誰でもいつでも、いつまでも検証できる。

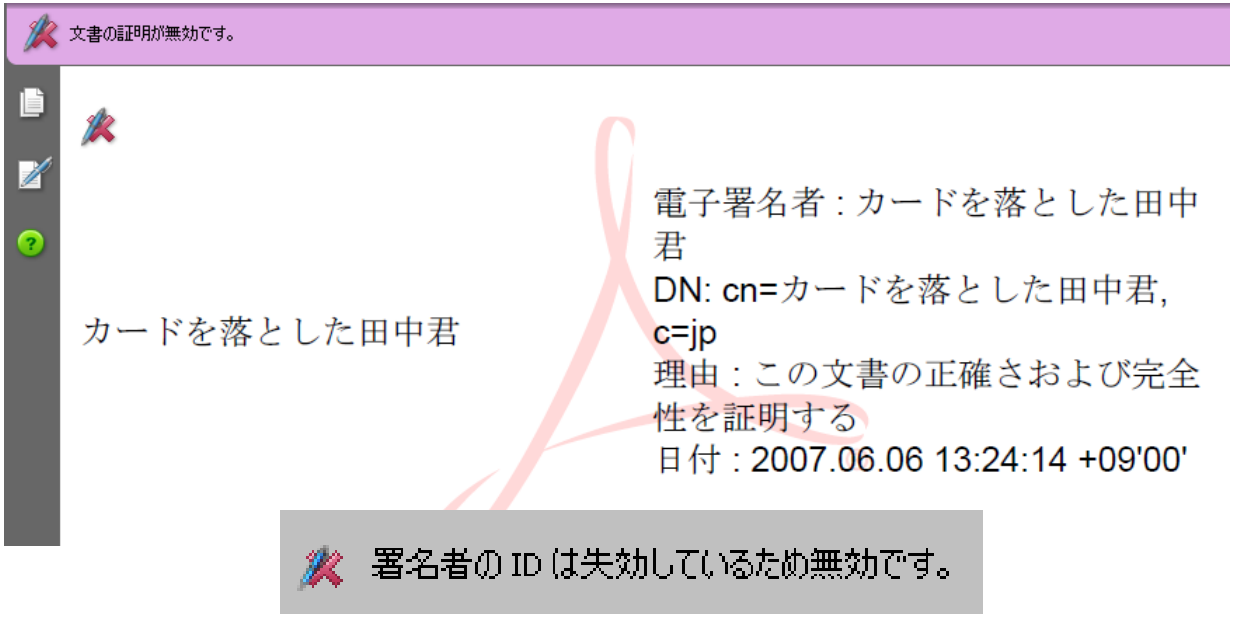
- 標準化
  - 日本国内における標準化 (JIS)
  - ETSI TC ESI との関係
  - PDF / A との関係
  - CAdES の RFC化
  - e文書法への対応

- 相互運用実証実験
  - ECOM国内実証実験
  - 日欧実証実験

- ECOM2006年報告書「長期署名ハンドブック」の紹介

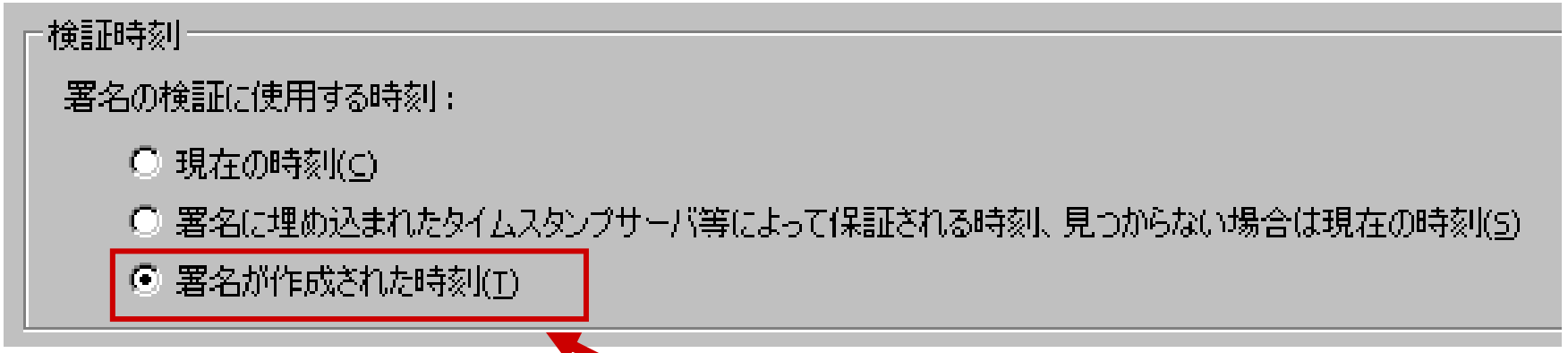
改ざんされては困る電子データを保存する際、
デジタル署名だけで大丈夫ですか？

Entrust® 簡単なデモをご覧下さい



失効している証明書でも
こんなことをすると、、、、、、、

Adobe Acrobat Reader 8ではきちんと対策されています



この設定にしたときだけ、デモのように不正な署名を受け入れてしまいます。

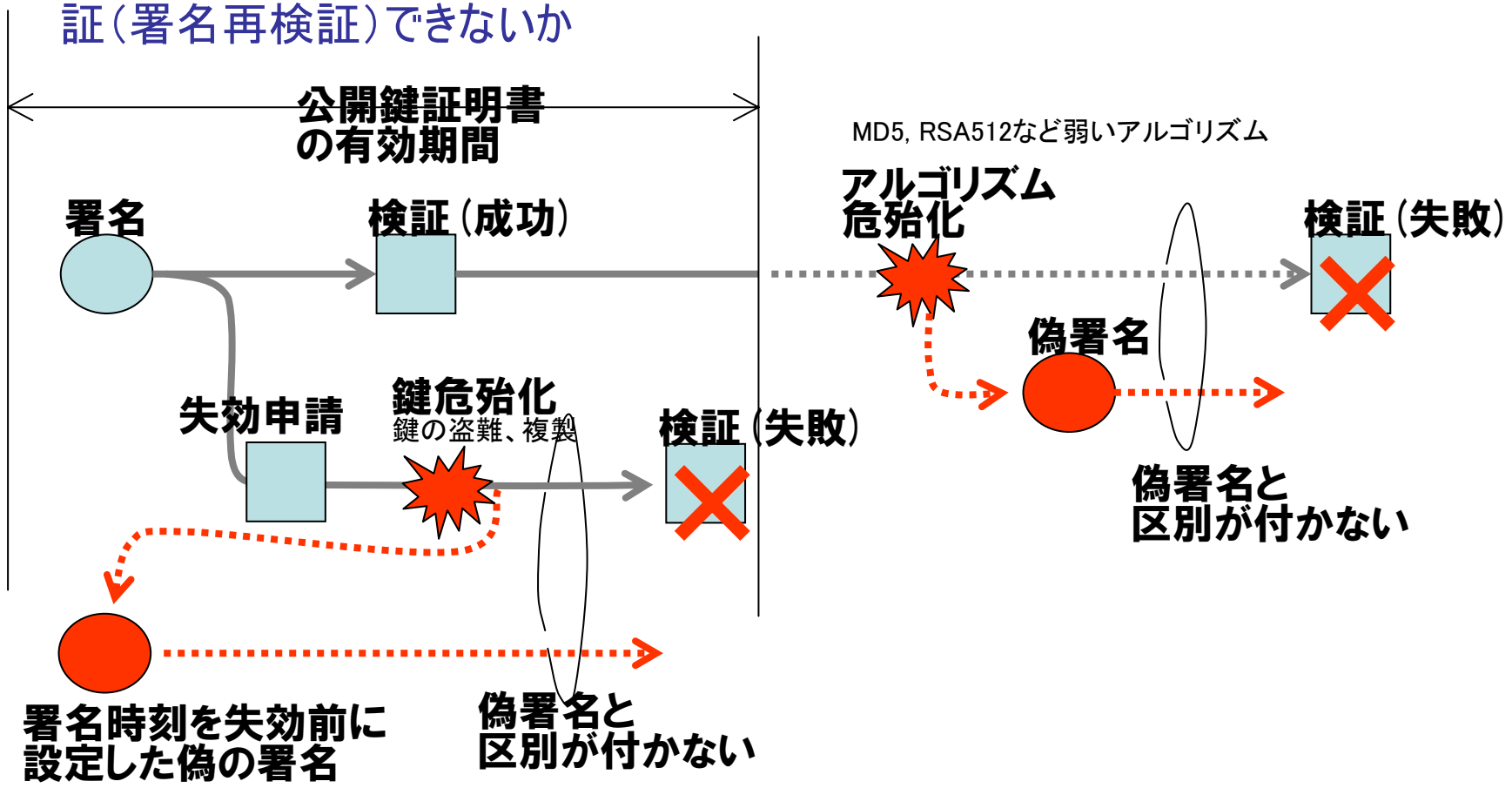
ただし、この設定にしなかった場合

・期限切れの証明書を使った場合、署名時点で有効であったとしても無効扱いになります。
・失効した証明書を使った場合、署名時点で有効であったとしても無効扱いになります。

※安全でおススメ、かつデフォルト設定は真ん中の設定

Entrust® 電子署名の限界

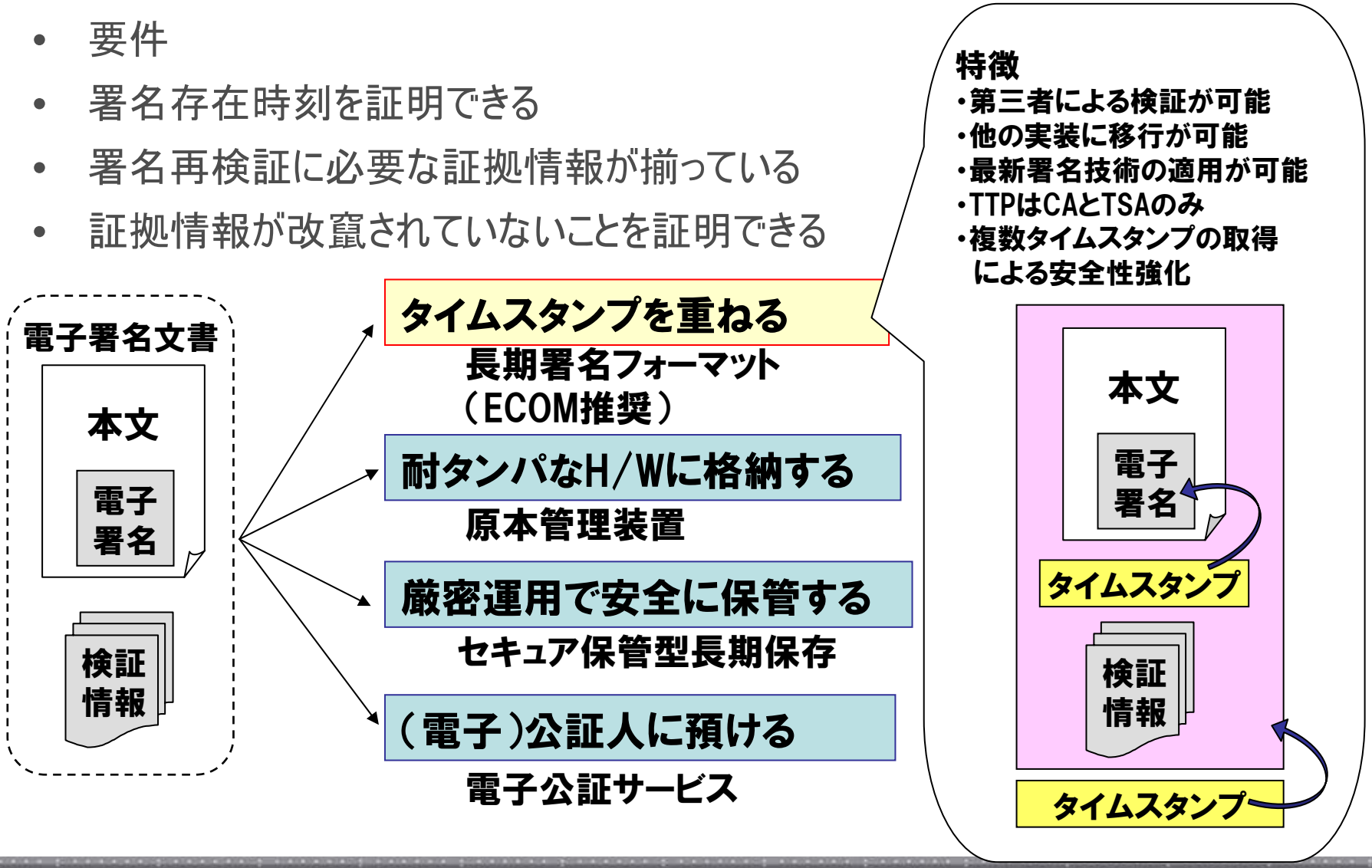
- 署名の真偽が確認できるのは、有効期間内かつ失効がないときのみ（それ以外は真偽の区別がつかない）
- 失効が発生しても有効期間が過ぎても、署名が過去に有効であったことを検証（署名再検証）できないか



長期署名フォーマット
CAdES / XAdES とは？

Entrust® 署名再検証が可能な要件と各種方式

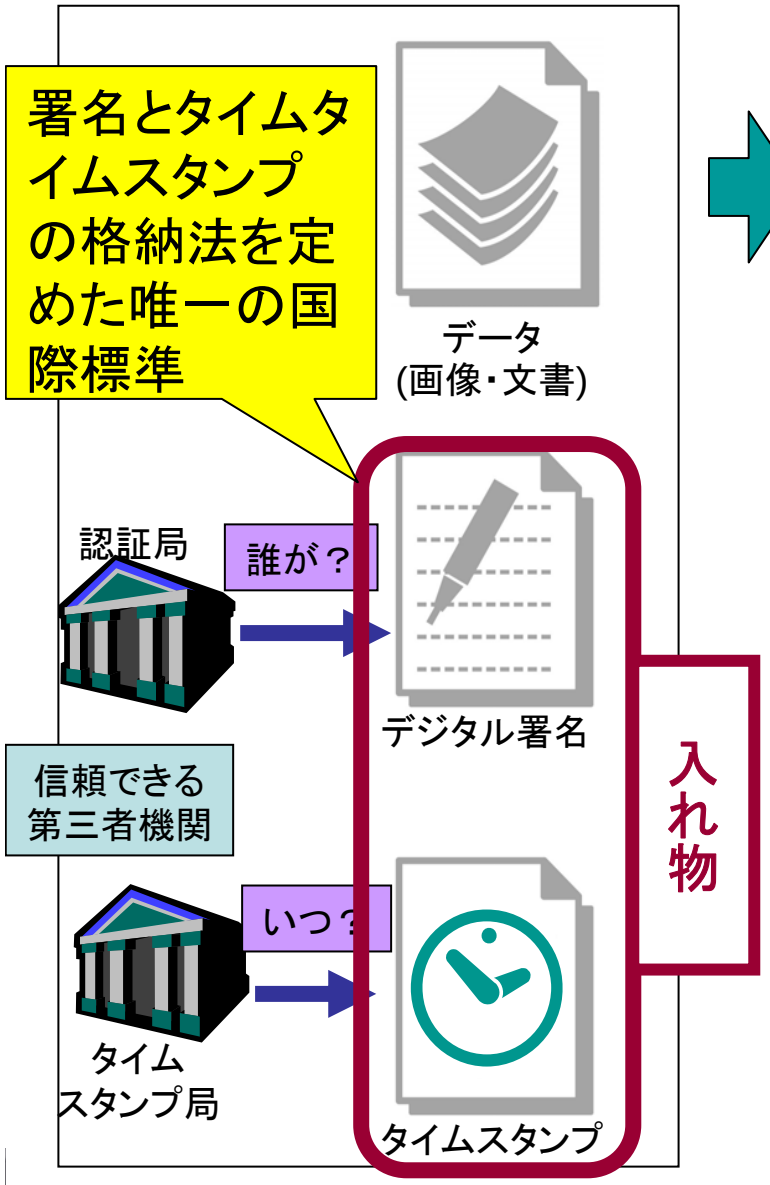
- 要件
- 署名存在時刻を証明できる
- 署名再検証に必要な証拠情報が揃っている
- 証拠情報が改竄されていないことを証明できる



長期署名フォーマット(CAdES/XAdES)とは

- 欧州通信規格協会(ETSI)で策定された。
- 署名暗号メール、PDF署名、一般的な電子署名データで使われるPKCS#7/CMS、XML署名に属性を追加したフォーマット
  - 「何時、誰が、何に署名したのか」ということを
  - 署名者の証明書の有効期限(通常1~2年)後でも
  - 将来暗号アルゴリズムが危殆化しようとも
  - 途中、タイムスタンプサービスや認証局が変わっても
  - データが改ざんされていないことを保証できる
- 長期署名フォーマットのミソ
  - 署名にタイムスタンプをつける
  - 署名およびタイムスタンプの検証に必要な証明書,CRLをつける
  - 上記を最新の暗号アルゴリズムを用いたアーカイブタイムスタンプ暗号アルゴリズムが破られる心配が無いように保存延長していく

Entrust 長期署名フォーマット(CAdES/XAdES)とは (2)



タイムスタンプが別ファイルである問題点

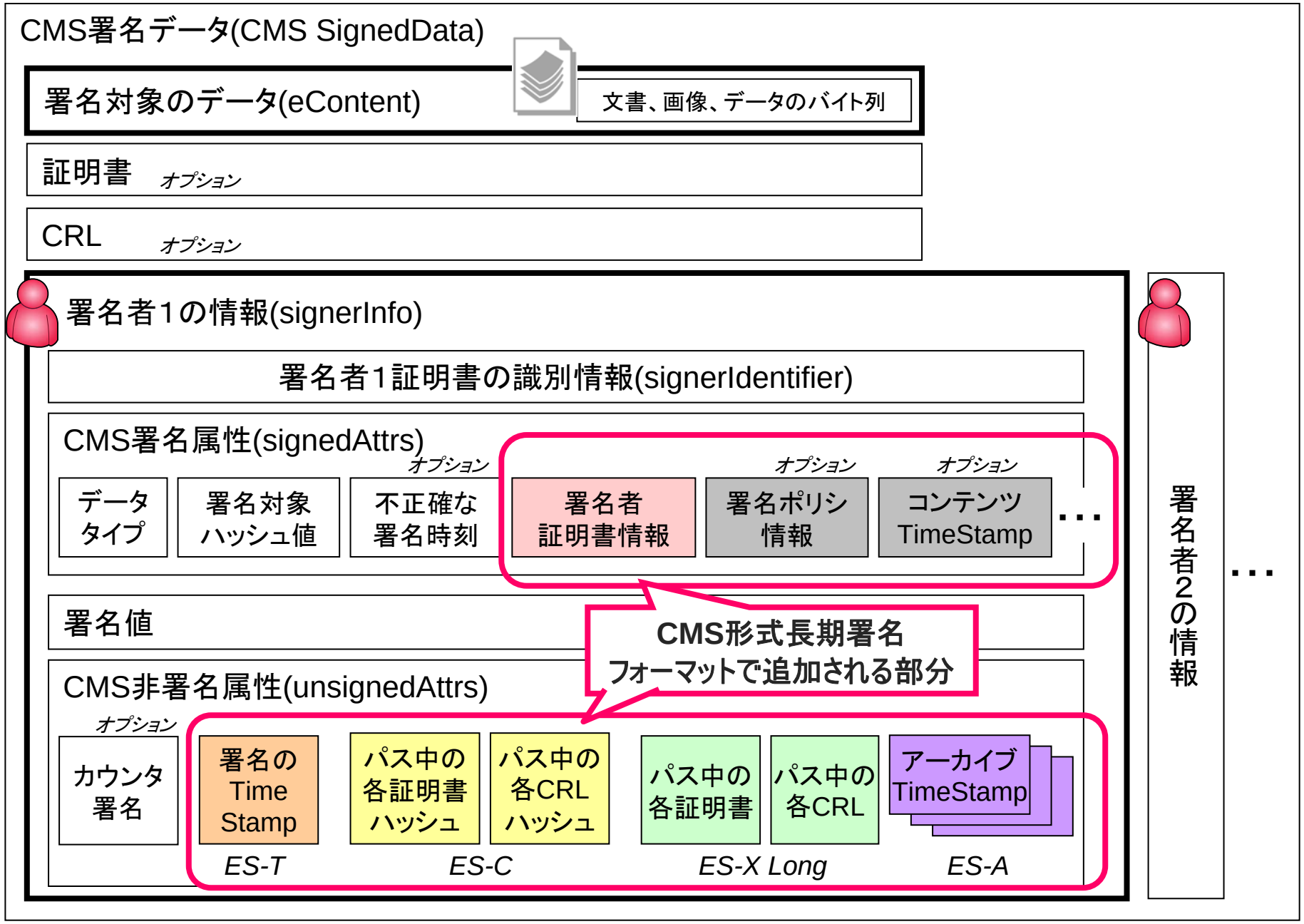
- TS単体では何を対象としたTSか不明
- 誰がタイムスタンプを押したかはわからない
- 悪意のある人でも正当なTSは押せる

- 署名とTSをまとめる「**入れ物**」が必要
- 署名者やタイムスタンプ局の証明書の有効期間である**3年、10年を過ぎても**データが改竄されていないことを保証する「仕組み」

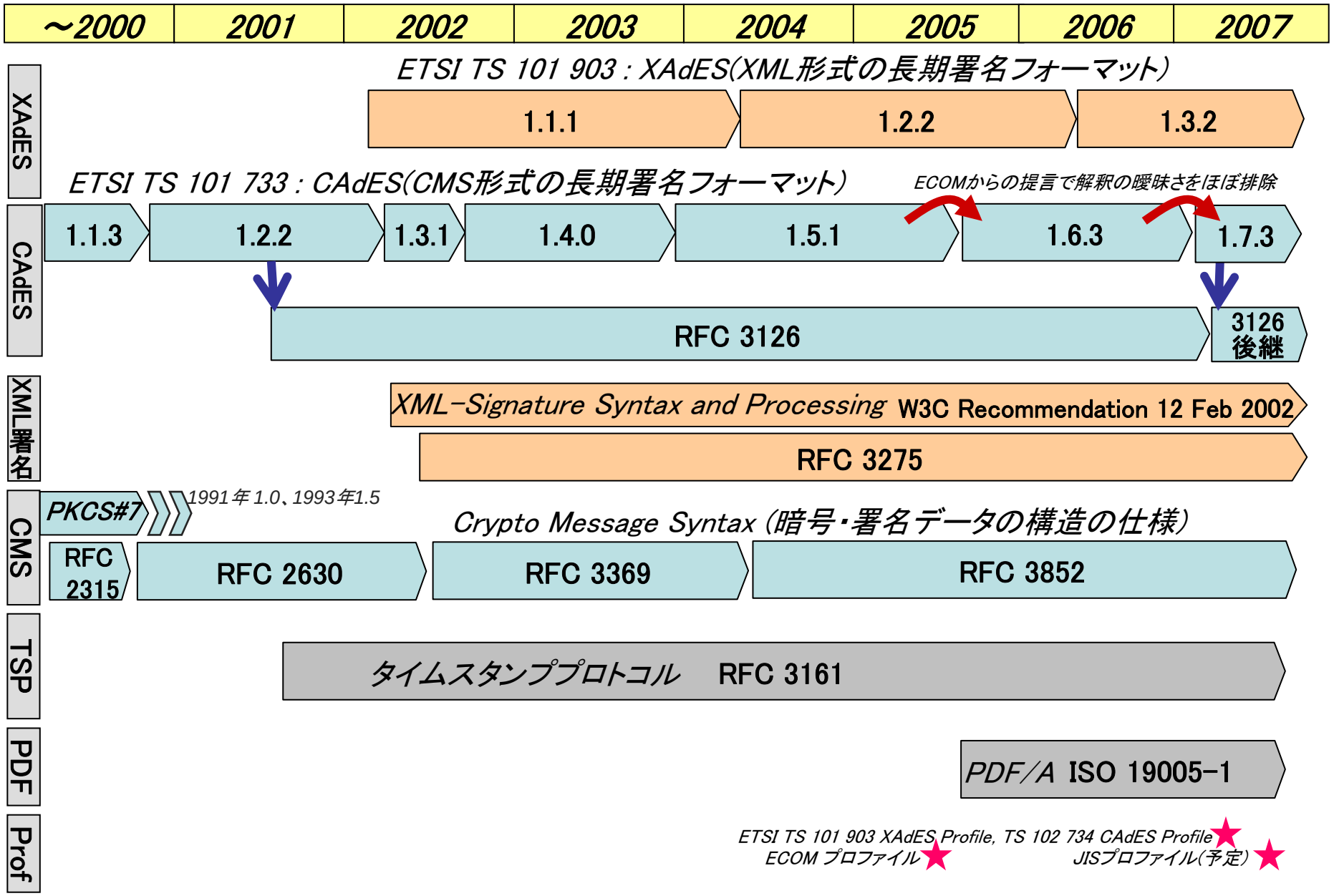
長期署名(ES)フォーマット

- ETSI(欧州通信規格協会)で2000年に策定され、その後改訂され続けている
- 2001年RFC3126となる(RFC3161の付録も)
- S/MIME署名メールで使われるCMS形式(CAdES)とXML形式(XAdES)がある

長期署名フォーマットのデータ構造(CMS形式の例)



Entrust 長期署名フォーマットに関連する標準の系譜



Entrust EUで定めたAdvanced Electronic Signatureとは？

日本の電子署名法

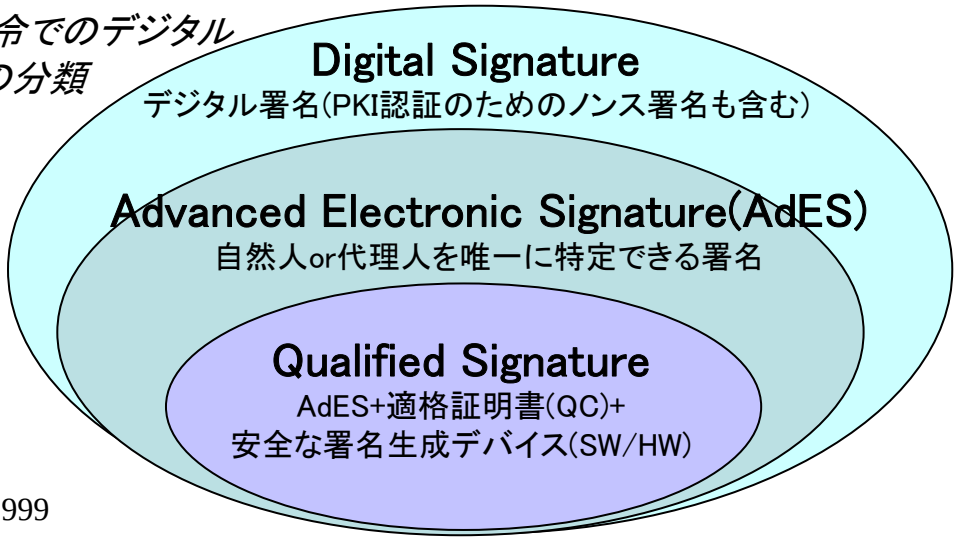
欧州連合(EU)における
電子署名に係る指針(※1)

一般原則：5.2条
全ての電子署名に対する法的効果
第二原則：5.1条
手書き署名と同等の法的効果を得る電子署名

CAdESやXAdESの
高度電子署名(Advanced Electronic Signature)とは？
本当に特定可能な自然人、または、その代理人が行った署名であることを判断できる署名。

デジタルタイムスタンプにより、「本当に」本人または代理人が行ったことを特定できる。

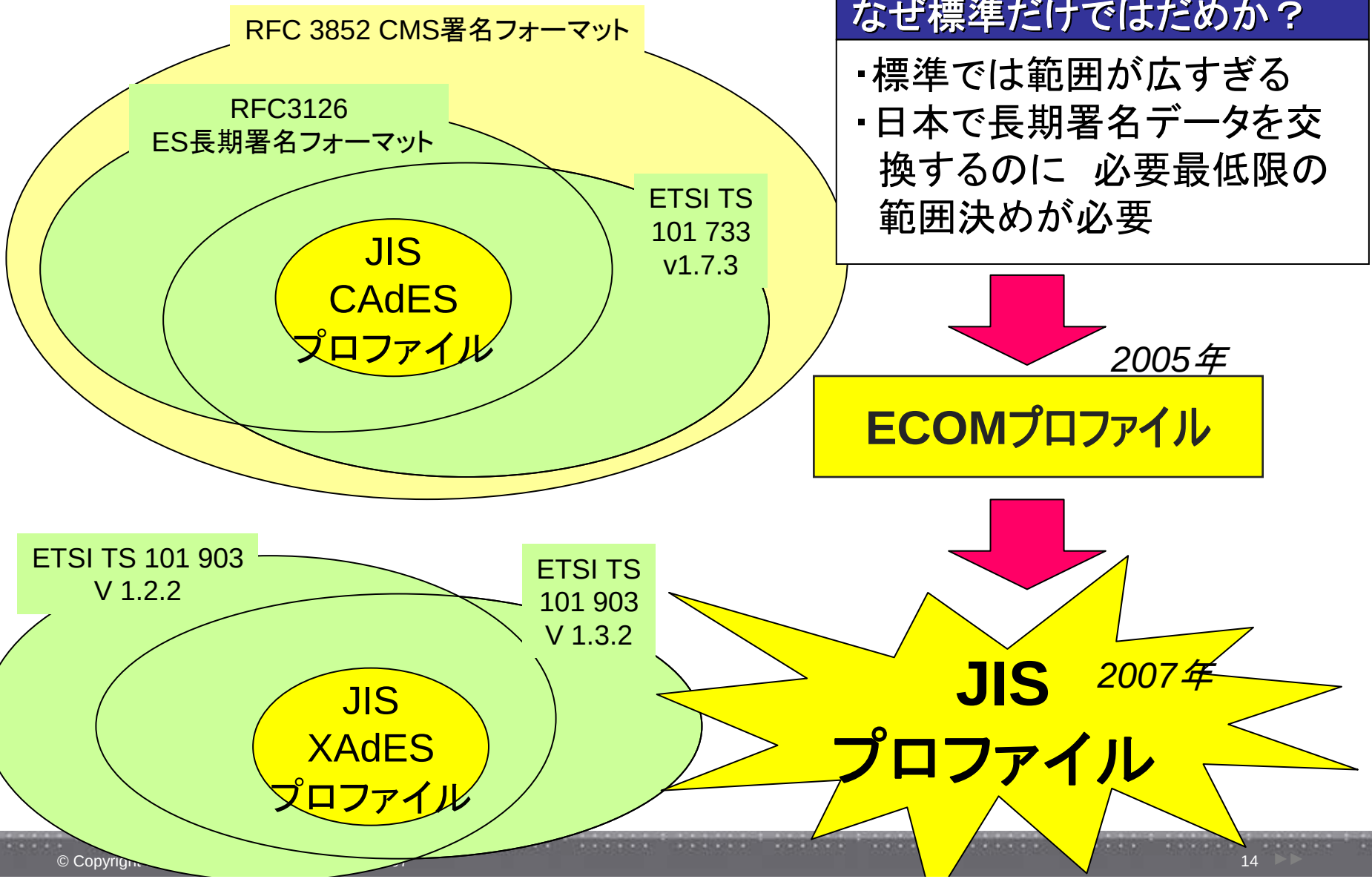
EU指令でのデジタル署名の分類



※1: DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on Community framework for electronic signatures

長期署名フォーマットのプロファイルの必要性
JIS標準化
その他の標準化

長期署名フォーマット
なぜ、プロファイルが必要か？



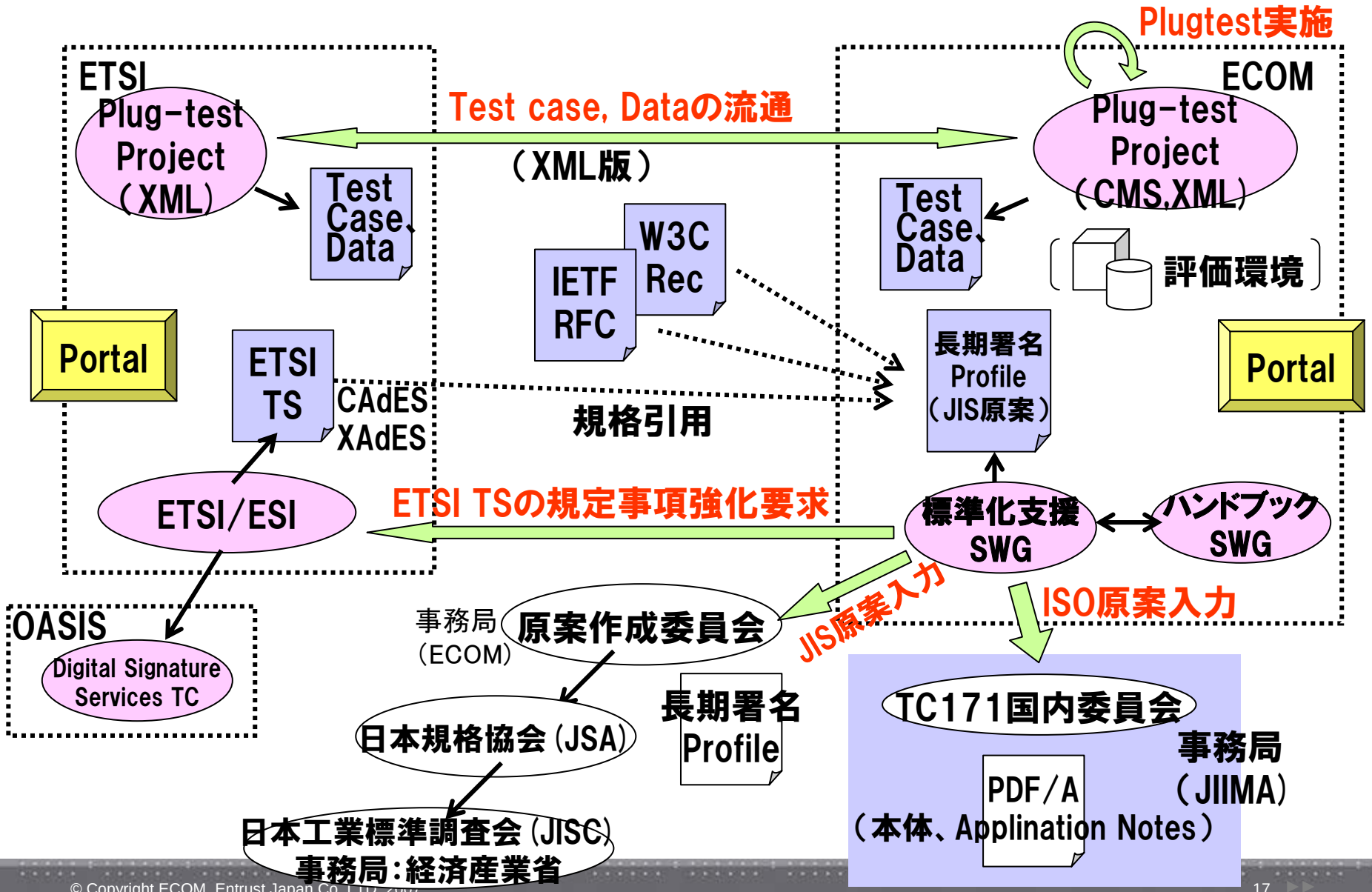
電子文書の長期保存に関するECOMの取り組み

- 2000年「電子署名文書長期保存に関する中間報告」
- 2001年「電子署名文書長期保存に関するガイドライン」
- 2002年「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「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「電子文書長期保存のための保存性・見読性ガイドライン」
- 2005年「ECOM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実験報告書」
- 2006年「長期署名プロファイルJIS化原案」
  「長期署名ハンドブック」
  「長期署名フォーマットを利用した長期保存システムガイドライン」
  ETSI TC ESI (欧州通信規格協会 電子署名基盤技術委員会)加盟
- 【連携】
  - 日本画像情報マネジメント協会(JIIMA) – (PDF/Aについて)

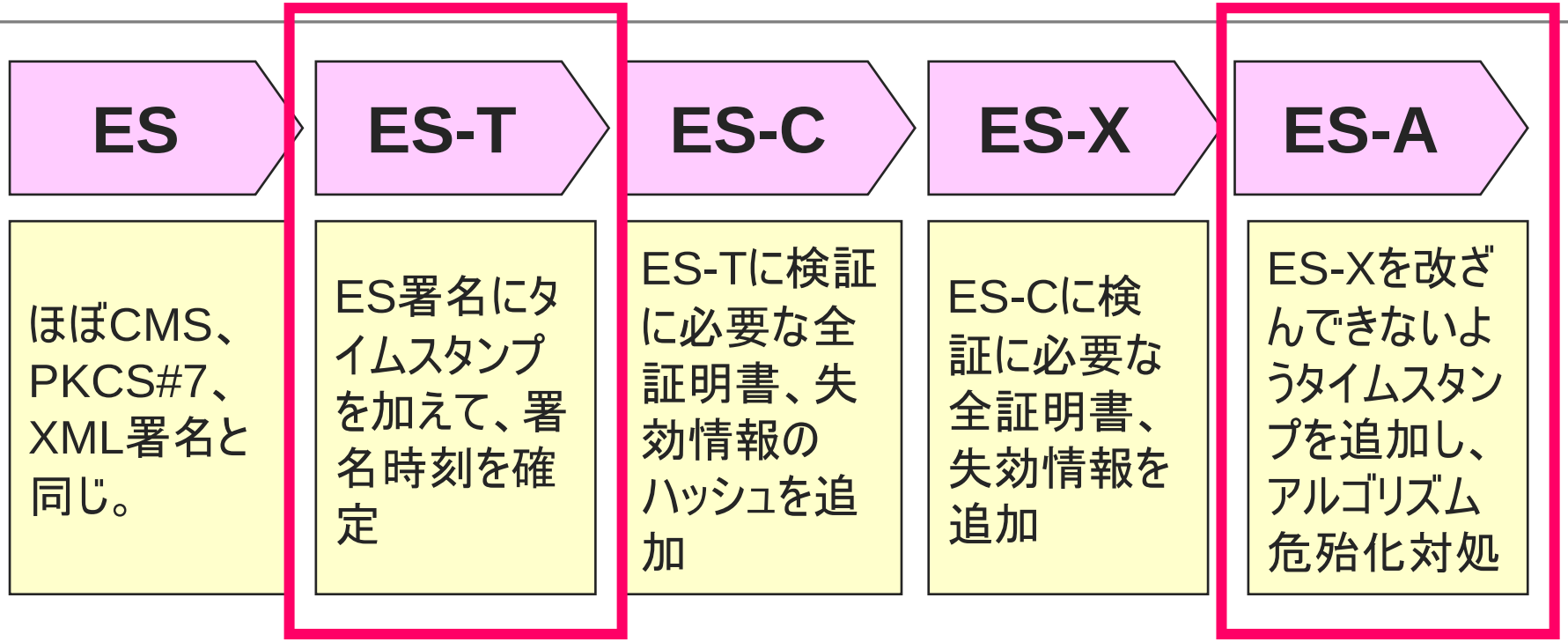
Entrust® 長期署名プロファイルのJIS化(現状)

- 2006年3月～10月
  - ECOM幹事メンバによりECOMプロファイル2005に基づいたJIS日本工業規格化のための調整、JIS原案作成委員会向けの草案作成
- 2006年11月～12月
  - JIS原案作成委員会
    - 委員長：東海大 辻教授、幹事：NEC木村、事務局：ECOM、委員20名(法律有識者、JIIMA,JIPDEC,生産者,利用者企業有識者)
- 2006年12月末：　JIS原案を日本規格協会に提出
- 2007年3月：　JIS原案をECOMより公開可能
- 2007年6月：　日本規格協会・規格調整分科会で審議中
- 2007年秋頃：　公開予定

Entrust 長期署名JIS化関連の全体像



JISプロファイルの特徴(1) ES-T, ES-Aに限定



データ交換の可能性のあるデータフォーマットとして、ES-T、ES-Aに絞込みプロファイルを作成した。これら以外は、中間生成物の扱いとし、データ交換を推奨はしない。

JISプロファイルの特徴(2) 要求レベル「要別途規定」

	ES-T	ES-A
署名属性	必須	必須
主張された署名時刻	オプション	オプション
署名場所	要別途規定	要別途規定
:		
非署名属性	必須	必須
カウンタ署名	オプション	オプション
署名タイムスタンプ	必須	必須
検証用失効情報群	不要	必須
:		
アーカイブタイムスタンプ	不要	必須

必須

オプション

不要

他の標準でも見かける
一般的な要求レベルに加え

要別途規定

別途、処理方法を定めれば、その「要素」は入れても良い。逆に、処理方法が定められていないのであれば、入れてはならない。

本要求レベルの導入により、「どう処理してよいかわからない要素」は無くなる。

JIS、ETSIにおけるCAdES / XAdESプロファイルの比較

	日本:JIS	欧州:ETSI
公開	2007年秋ごろを予定	2007年1月
仕様番号	未定	TS 102734 / 102904
対象フォーマット	ES-T, ES-Aのみ	制限しない
用途	基本を定めた。医療用など拡張可能。	基本、電子政府、電子請求書の3種
要求レベル	必須、オプション、**要別途規定**、使用不可？	必須、オプションのみ
生成・検証	生成・検証を分けておらず部分実装も可	生成と検証の要件を分けて定義
特徴	・日本限定の特殊な要件は無い。	

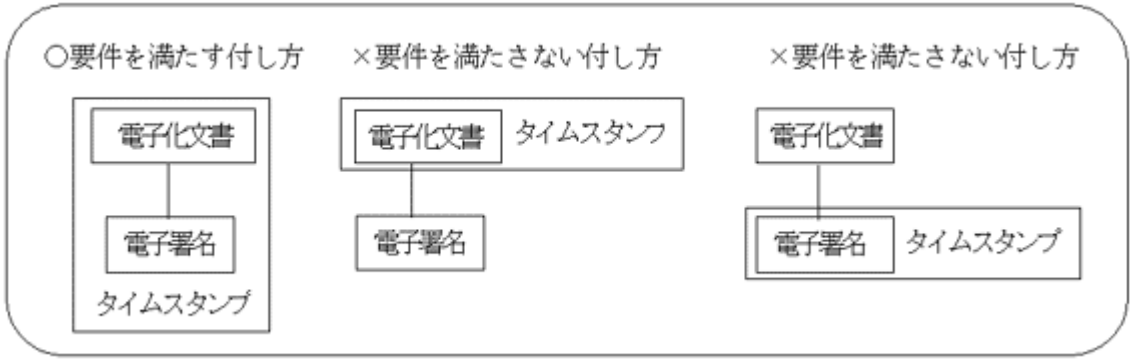
包含関係

Entrust e文書法と長期署名フォーマット

素朴な疑問

長期署名フォーマットは「e-文書法」の要件を満たす署名およびタイムスタンプか？

H17.2.28国税庁「『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
4-28 (タイムスタンプの付し方)
http://www.nta.go.jp/category/tutatu/sonota/sonota/01/03.htm#14



「画像データと電子署名データの両方に対し一のタイムスタンプを付す必要がある」が、そのようなハッシュ対象のタイムスタンプは国際標準には無い

他の関連する標準化動向

- IETF S/MIME WG
  - RFC 3126 (2001.09) Electronic Signature Formats for long term electronic signaturesの後継
    - SHA-1ハッシュ危殆化に対応した署名者証明書識別の属性がRFC化されるのを待っていた。
    - 上記が終わったことにより、CAdES v1.7.3ベースのI-Dが公開中
- PDF/A ISO 19005-1
  - 日本提案のCAdES v1.7.3改定でPKCS#7ベースでも良くなったのでCAdES-T(署名タイムスタンプの利用は問題ない)
  - Adobe Acrobat 7 以降でも署名タイムスタンプの実装をしている。
  - ただし、
    - 失効情報はAdobe専用の属性を定義しており、署名属性として格納＞大問題
    - アーカイブタイムスタンプについてはPDF/A ISOではやや否定的
    - 10年後、20年後、再度署名タイムスタンプをつける方式を米国より提案有
      - 誰が署名するのか？

長期署名フォーマットの相互運用実証実験

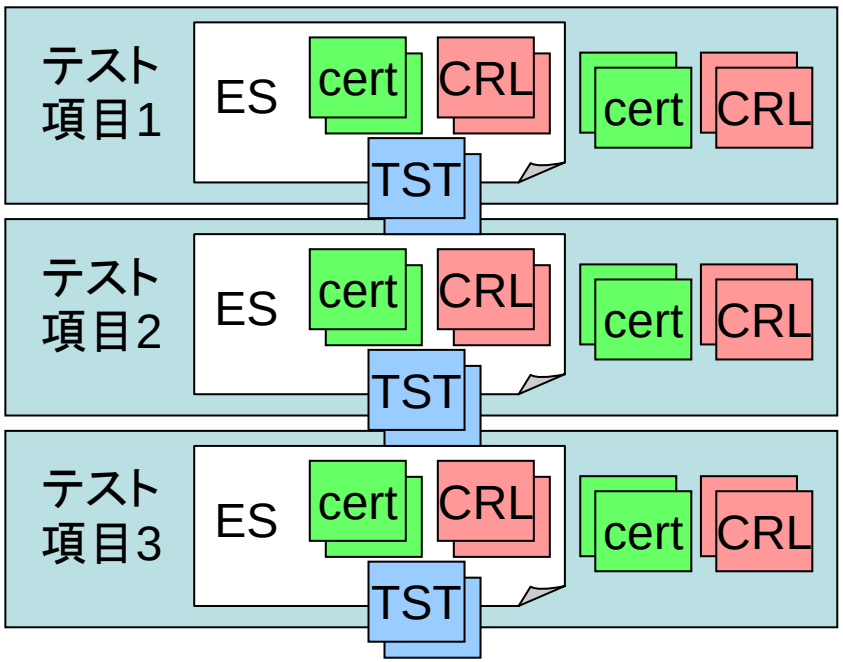
Entrust 2007年相互運用性テストの概要

目的	・JIS長期署名フォーマットへの準拠性の追加確認 ・各組織が生成するデータの相互運用性の確認 ・国際相互運用テスト(対ETSI、他)
期間	第一期：2007年1月～3月 (JIS準拠性オフラインテスト,日欧事前テスト) 第二期：2007年10月頃 (国内、国際オンラインテスト)
テスト 参加資格	・原則ECOM会員および海外組織(ETSI、他) ・CAdES, XAdESのES, ES-T, ES-C, ES-XL, ES-Aのフォーマット生成のできるソフトを持つ組織 ・文書管理ソフトでも開発ライブラリでも可 ・製品、プロトタイプの別は問わない ・テスト結果の合否を公表する
内容	・JIS準拠性オフライン共通データ検証テスト(2,3月) ・オンラインマトリックス相互生成・検証テスト(10月)
結果公表	・中間結果発表(4月)：オフライン共通データ検証テストの結果 ・最終結果発表(12月)：国際オンラインテストを含む最終報告

Entrust JIS準拠性オフライン共通データ検証テスト

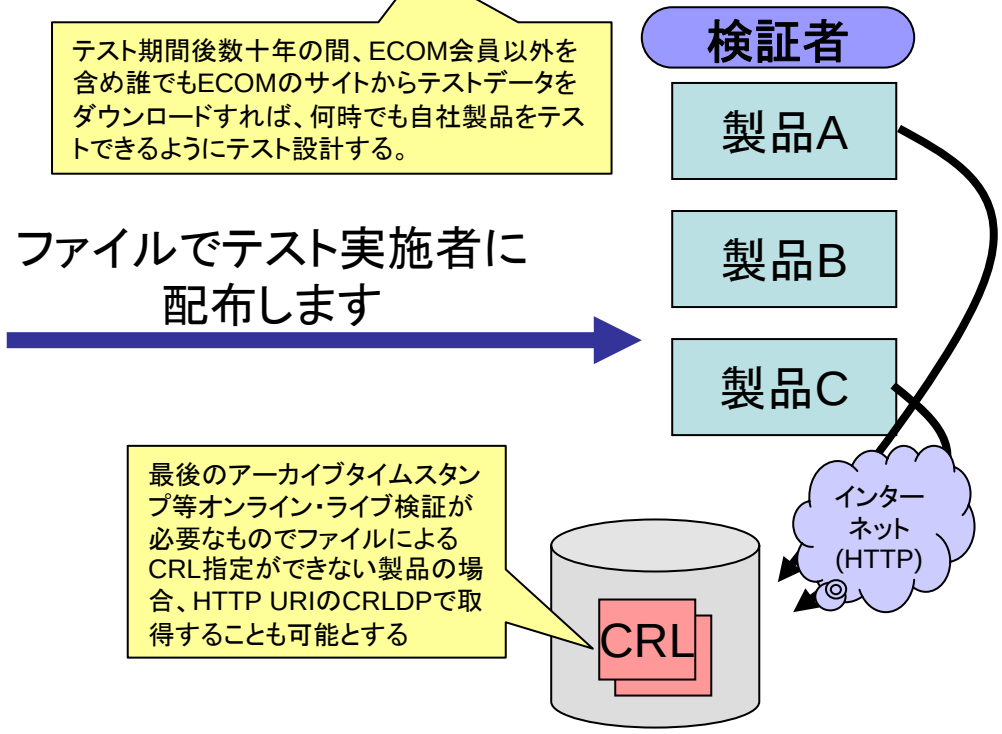
目的	・実装されている長期署名フォーマットの検証機能の確認 ・JIS準拠性の追加確認
内容	ツールにより生成されたESフォーマットのデータ(ES-T, ES-X Long, ES-A)、検証情報、設定情報のセットをテスト対象として、各社製品でオフラインにより有効性を検証する。結果は有効、無効の2種類のみ。無効の理由は問わないこととする。

テスト用の鍵、証明書、CRLの発行にはIPA/JNSA Challenge PKIテストスイートを用いる。



テスト期間後数十年の間、ECOM会員以外を含め誰でもECOMのサイトからテストデータをダウンロードすれば、何時でも自社製品をテストできるようにテスト設計する。

ファイルでテスト実施者に配布します



最後のアーカイブタイムスタンプ等オンライン・ライブ検証が必要なものでファイルによるCRL指定ができない製品の場合、HTTP URIのCRLDPで取得することも可能とする

Entrust テスト項目とテストケースの関係

テスト項目	期待値
標準の成功系テスト	有効
失効している場合	無効
サイニングタイム時点のみ失効	有効
署名タイムスタンプ時点のみ失効	無効

テスト項目の結果はテストを実行した結果有効(valid)だったか無効(invalid)だったかだけで判定する

テスト項目が全て期待値通りならばテストケース成功とする

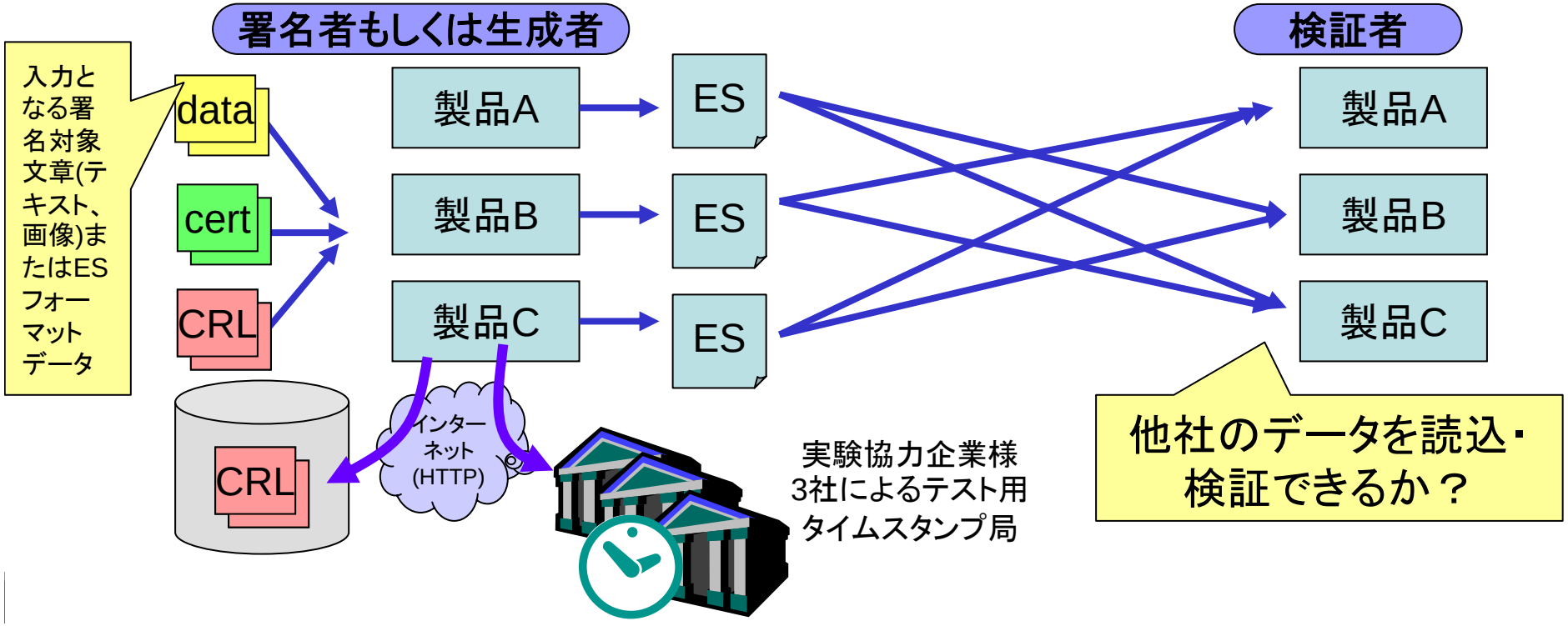
テストケース

ES-Tフォーマットでサイニングタイムに関係なく署名タイムスタンプの時刻により署名者証明書の失効検証ができる

・ブラックボックステストを想定しており、テスト項目の期待値は有効/無効のいずれか
・テスト項目の結果を組み合わせて、「ある機能が正しく動作するか」確認できる

Entrust® オンライン相互生成・検証テスト

目的	・他社製品が生成した有効なESフォーマットのデータが相互に読み取り、検証できることを確認
内容	指定した証明書、CRL、タイムスタンプサービスにより各製品により有効であるようなESフォーマット(ES-T, ES-X Long, ES-A)を生成する。各製品において読込み、他社の生成したデータが有効である事を検証する。CRL、TSAはオンライン、それ以外はオフラインとする。



Entrust 実験参加企業・協力企業 全22社 (グループ毎五十音順)

【CAdES実証実験参加企業　15社】
・RSAセキュリティ
・エントラストジャパン
・サートラスト
・サリオンシステムズリサーチ
・システムコンサルタント(日本電子公証機構)
・スカイコム
・セコム
・帝国データバンク
・日本電気
・ハイパーギア
・PFU
・ビーパークテクノロジー
・三菱電機(情報技術総合研究所)
・三菱電機インフォメーションシステムズ
・リコー

【XAdES実証実験参加企業 6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
・日本電気
・富士ゼロックス
・ラング・エッジ

【協力企業(テスト設計・データ作成)　3社】
・エントラストジャパン
・セコム
・日本電気

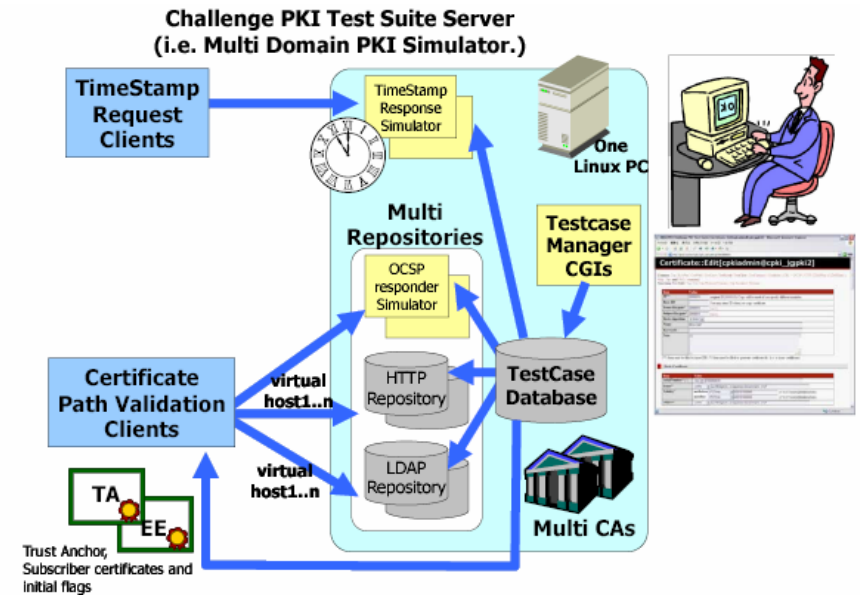
【協力企業(タイムスタンプサービス提供) 3社】
・アマノタイムビジネス
・セイコープレシジョン
・PFU

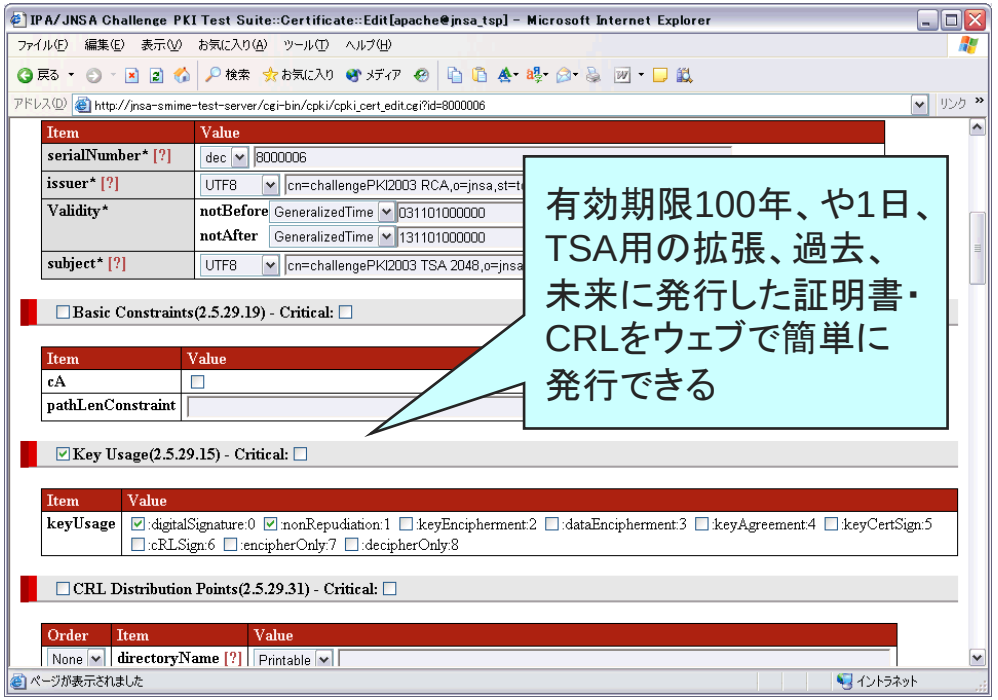
2005年実験時14社から、22社に増えました

Entrust® 実験用CA環境(証明書、CRLの発行)

IPA/JNSA Challenge PKI Test Suiteを利用

- オープンソースでフリーなPKI統合テスト環境＋ツール
  - IPA公募事業によるGPKI模擬テスト、タイムスタンプテスト
  - PKI-J：PKI国際的相互接続実証実験(日台韓新)パス検証テスト
  - JNSA S/MIME利用検討WG：メーラー11製品の署名暗号検証テスト

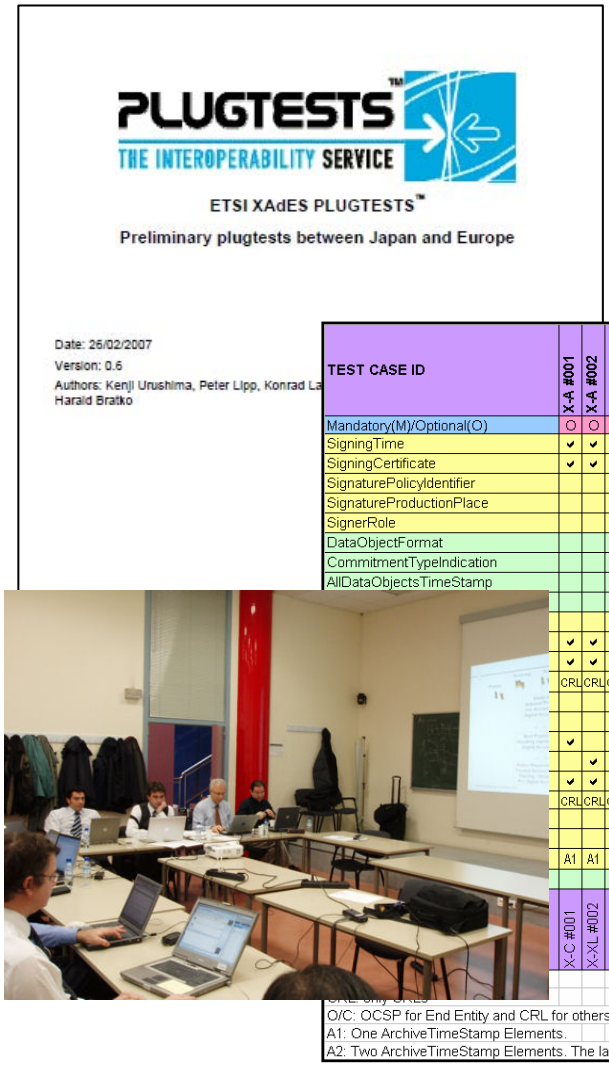




http://www.jnsa.org/mpki/よりダウンロード可

ETSI-ECOM XAdES日欧事前実験 (2007年1～3月)

- 今秋予定している日欧実験の準備としてXAdES事前実験を実施
- 参加組織
  - スペイン：カタルーニャ工科大
  - オーストリア：内務省研究所(A-SIT,IAIK)
  - 日本電気
  - エントラストジャパン
- 実験協力
  - アマノタイムビジネス (※1)
- 実験内容
  - ECOMオンラインマトリックステストと同等の生成・検証テストを実施
  - 認証局はIAIK (CRL+OCSP)
  - テスト計画、設計書、データ交換はメールベース。月1電話会議


PLUGTESTS™
THE INTEROPERABILITY SERVICE

ETSI XAdES PLUGTESTS™

Preliminary plugtests between Japan and Europe

Date: 26/02/2007

Version: 0.6

Authors: Kenji Urushima, Peter Lipp, Konrad La
Harald Bratko

TEST CASE ID	X-A #001	X-A #002	X-A #003	X-A #004	X-A #005	X-A #006	X-A #007	X-A #008	X-A #009	X-A #010	X-A #011	X-A #012	X-A #013	X-A #014	X-A #015
Mandatory(M)/Optional(O)	O	O	O	O	O	O	O	O	O	O	O	O	M	M	O
SigningTime	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
SigningCertificate	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
SignaturePolicyIdentifier															
SignatureProductionPlace															
SignerRole															
DataObjectFormat															
CommitmentTypeIndication															
AllDataObjectsTimeStamp															
	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔			
	CRL	CRL	CRL	O/C	O/C	O/C	CRL	CRL	CRL	O/C	O/C	O/C			
	✔			✔			✔			✔					
		✔			✔			✔			✔				
	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CRL	CRL	CRL	O/C	O/C	O/C	CRL	CRL	CRL	O/C	O/C	O/C	CRL	CRL	O/C
	A1	A1	A1	A1	A1	A1	A2	A2	A2	A2	A2	A1	A1	A2	A1
	X-C #001	X-XL #002	X-XL #003	X-C #002	X-XL #005	X-XL #006	X-A #001	X-A #002	X-A #003	X-A #004	X-A #005	X-A #006	X-T #001	X-A #013	X-T #001

O/C: OCSP for End Entity and CRL for others.
A1: One ArchiveTimeStamp Elements.
A2: Two ArchiveTimeStamp Elements. The lastest time-stamping the former one.

※1: アマノタイムビジネス株式会社様にはテスト用タイムスタンプサービスならびに英語版説明・ユーザ登録ページをご提供頂きました。

ECOM 2006年度 調査報告書

Entrust Securing Digital Identities & Information

「電子文書長期保存ハンドブック」

長編 320ページ

- デジタル署名ハンドブック
  - デジタル署名フォーマットであるCAdES/XAdESの詳説
  - デジタル署名の生成
  - デジタル署名の検証
  - 付録：PKCS#7/CMSの違い、ハッシュのパラメータ、複数署名
- 電子署名長期保存
  - JSOX法と記録管理
  - 記録・保存マネジメント手法
  - 電子文書保存への長期署名フォーマットの推奨
- 長期署名プロファイルのJIS化、実験、国際調整
  - 長期署名プロファイルのJIS化
  - 長期署名フォーマット国内/日欧相互運用実証実験
  - 国際標準化調整の経緯(ETSI TC ESI / PDF/A)
  - 付録：CAdES/XAdES長期署名プロファイル JIS原案

長期署名フォーマットがよくわかる

電子文書保存管理がよくわかる

標準化の最新動向がわかる

4月冊子配布済、近日中(8月頃) ECOMサイトでPDF公開予定)

まとめ

- 文書を保存する際、デジタル署名だけではだめなのでしょうか？(+ デモ)

- 長期署名フォーマット CAdES / XAdES
  - CMS/PKCS#7/XML署名の拡張。データ単体で誰でもいつでも、いつまでも検証できる。

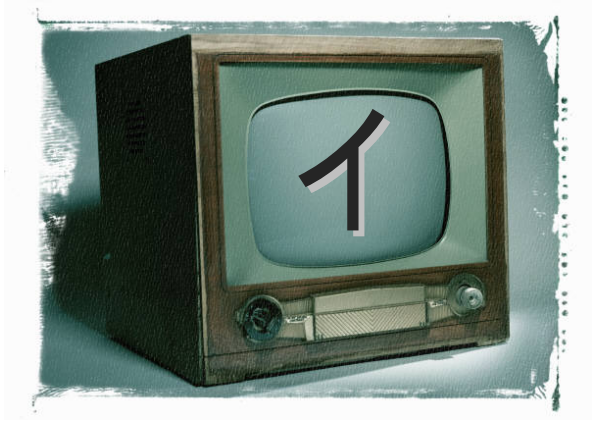
- 標準化
  - 日本国内における標準化 (JIS)
  - ETSI TC ESI との関係
  - PDF / A との関係
  - CAdES の RFC化
  - e文書法への対応

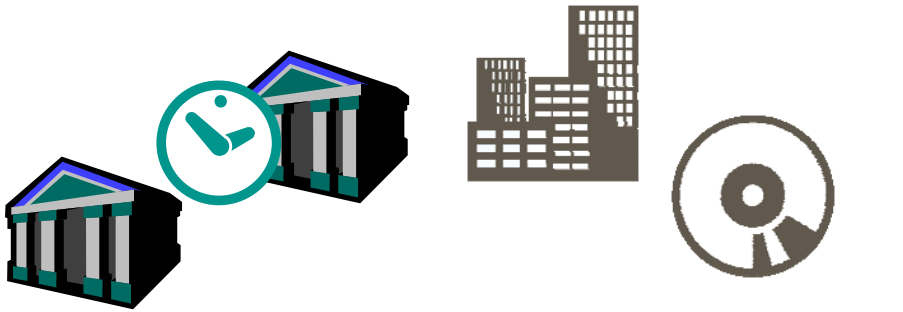
- 相互運用実証実験
  - ECOM国内実証実験
  - 日欧実証実験

- ECOM2006年報告書「長期署名ハンドブック」の紹介

電子文書を100年間保存するプロジェクトをやりませんか？

1926年に日本発のブラウン管での試験放送に成功しました。最初の文字は「イロハ」の「イ」だったそうです。





様々な組織・団体の皆様の協力が必要となるでしょう。

世界初で100年間、改ざんされずに残っていることが保証される「電子データ」。あなたなら、何を残しますか？

Entrust 参考リンク

- ETSI Electronic Signatures and Infrastructures (CAdES, XAdES仕様, プロファイル)
  - http://portal.etsi.org/esi/el-sign.asp
- IETF RFC
  - Electronic Signature Formats for long term signatures
    - http://www.ietf.org/rfc/rfc3126.txt
    - http://www.ietf.org/internet-drafts/draft-ietf-smime-cades-02.txt (2007.05.24 CAdES 1.7.3ベースのドラフト)
  - Cryptographic Message Syntax (CMS)
    - http://www.ietf.org/rfc/rfc3852.txt
  - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
    - http://www.ietf.org/rfc/rfc3161.txt
    - http://www.ipa.go.jp/security/rfc/RFC3161JA.html
  - ESS Update: Adding CertID Algorithm Agility (ESSSigCertV2の定義)
    - http://www.ietf.org/internet-drafts/draft-ietf-smime-escertid-06.txt (2007.05 IESG承認)
- 次世代電子商取引推進協議会(ECOM)
  - プロジェクトホームページ http://www.ecom.jp/LongTermStrage/project.html
  - プレスリリース
    - http://www.ecom.jp/report/report.html 長期署名フォーマットJIS原案
    - http://www.ecom.jp/press/2006_002.html 本年度実験
    - http://www.ecom.jp/press/2005_002.html
  - ECOM CAdES, XAdESプロファイル
    - http://www.ecom.jp/press/2005_005.html
  - (旧)ECOMの認証公証WGの長期署名に関する調査報告およびガイドライン
    - http://www.ecom.jp/pindex.html
- タイムビジネス推進協議会(TBF)
  - タイムスタンプ長期保証ガイドライン
    - http://www.scat.or.jp/time/seika.html
- JNSA Challenge PKI Project
  - PKI相互運用テストスイート(PKI,GPKI,LGPKI,JPKI,TSP,S/MIME)
    - http://www.jnsa.org/mpki/
- ASN.1変換規則 (BER, CER, DER)
  - http://www.geocities.co.jp/SiliconValley-SanJose/3377/index.html