ECOM CAdES/XAdES Plugtest 2007
結果報告

第28回ECOMセミナー 文書保存管理と長期保存技術
2008年1月24日 15:50～16:40

ECOM長期署名普及ワーキンググループ　副主査
ECOMプラグテストプロジェクト リーダー
エントラストジャパン株式会社　漆嶌　賢二

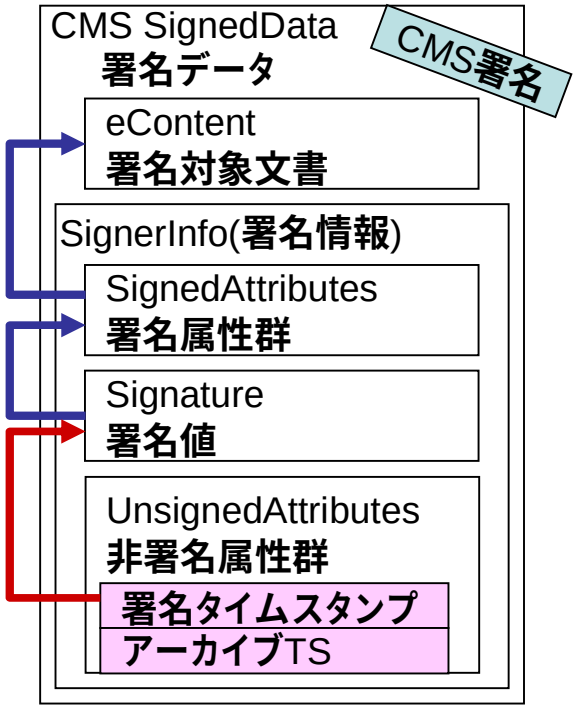
本日のアジェンダ

- **はじめに**
  - **長期署名フォーマット**(CAdES/XAdES)**とは**
  - **実証実験の必要性**
- ECOM CAdES/XAdES Plugtest 2007 **実証実験**
  - **実験概要**
  - **実験内容**
  - **実験結果**
  - **考察と課題**

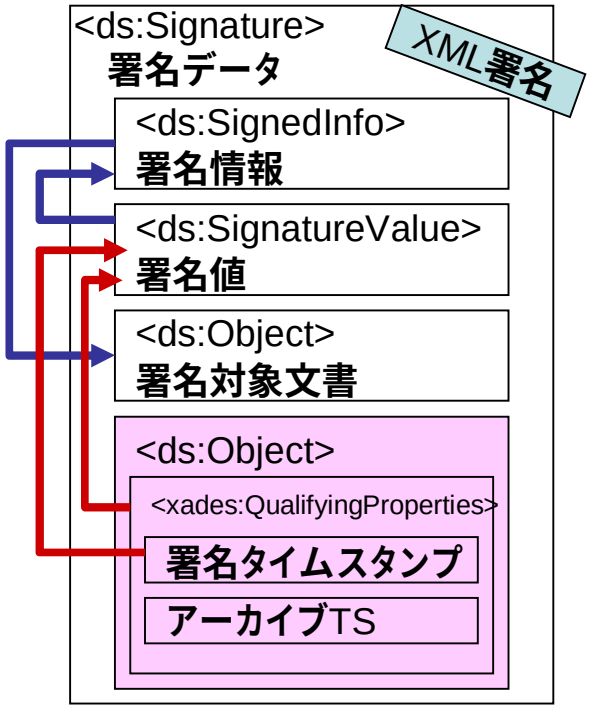
CAdES / XAdES
長期署名フォーマットとは

CAdES/XAdESとはCMS署名,XML署名の拡張

S/MIME,PDF署名で使うCMS署名



XML署名



【CMS署名,XML署名の問題点】
・本人性を示す証明書が有効であったときに署名されたものかわからない
・将来、暗号アルゴリズムが破られた際に正しかったかどうかわからない

単に基本の署名にタイムスタンプ要素を追加するだけで問題を解決

【メリット】
・元となるCMS署名、XML署名の検証ツールで、大筋は検証できる。
・追加された要素に対してのみ、別途検証すればよい。

EUで定めたAdvanced Electronic Signatureとは？

日本の電子署名法

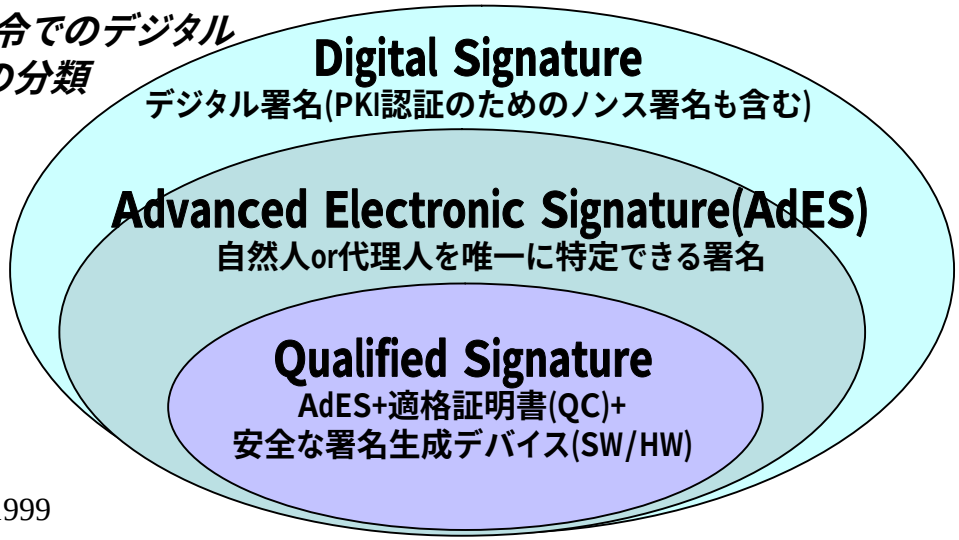
欧州連合(EU)における電子署名に係る指針(※1)

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。

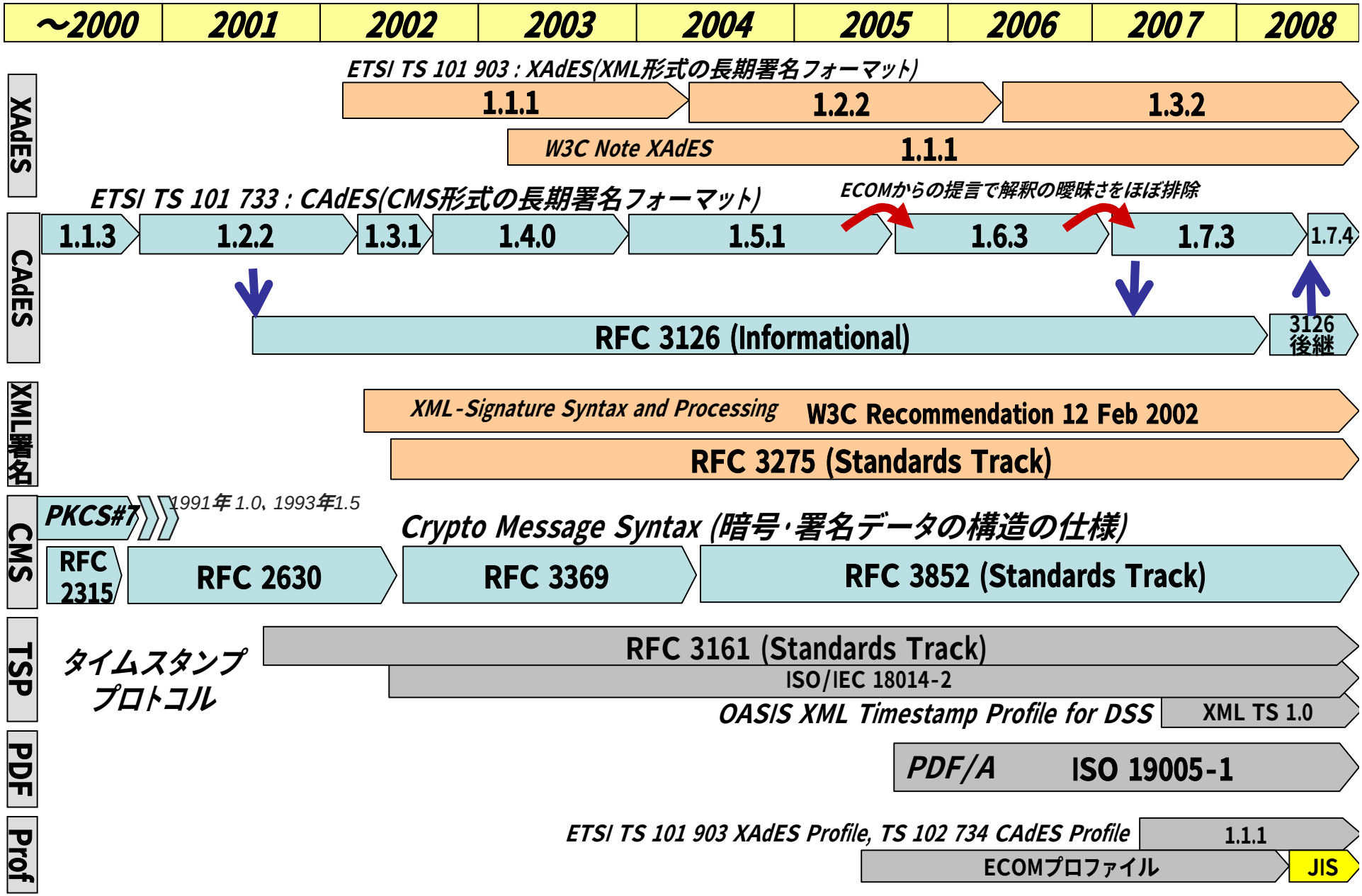
デジタルタイムスタンプにより、「本当に」本人または代理人が行ったことを特定できる。

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に関連する標準の系譜



ECOMからのIETF RFC,ETSI TSへの提言と寄与

・ECOMはETSI TC ESIのAssociate Memberとして正式加入
・IETF S/MIME Working Groupへの参加

- CAdES: ETSI TS 101 733 (1.5.1〜1.7.3) (2004-2008)
  - 実装経験を踏まえた相互運用性確保のための加筆・修正(ArcTS)
  - 計算方式の違うArchiveTimeStampV1/V2のOIDの区別
  - CMS SignedData Version 3に限定せずPKCS#7へも対応可能に
  - SHA2に対応したESSSigningCertificateV2の利用
- CAdES: RFC 3126の後継
  - SigningTime比較問題の修正
  - 曖昧な部分、誤植の修正依頼
- XAdES: ETSI TS 101 903 v1.3.2の後継 (2008.03検討開始)
  - SigingTime比較問題の修正(反映予定)
- XML署名ポリシ: ETSI TR (
  - 曖昧な部分、スキーマ、誤植の修正依頼(反映予定)

IESG承認済
2008年上旬公開

実証実験の必要性

実証実験の必要性

- CAdES/XAdES長期署名フォーマットの普及促進
  - CAdES/XAdESのテスト仕様やテストデータを公開することにより、これらがリファレンスとなり、実装の数自体が増え、普及促進につながる。また実装が増えることにより、相互運用性上の課題が浮かびあがり、これを修正し続けより良い仕様、より良い実装になっていき、普及を促進するという良い連鎖が生まれる。

- 標準仕様へのフィードバック
  - 標準仕様(ETSI TS, RFC, W3Cなど)は、机上で設計されたものであるため、実装してみないと問題点が発覚しないことがある。実証実験でおきた仕様上の問題をフィードバックする。

- 標準仕様準拠性、相互運用性があることを宣言するチャンス
  - ある製品がどの程度まで従っているのか、標準全体のうちどの機能まで提供しているか、相互運用性は確保されているか、利用者が理解するのは難しい。実証実験の結果、およびJIS原案の供給者適合性宣言の公表により利用者の製品選択の助けとなる。

ECOM CAdES/XAdES Plugtest 2007
実施内容

2007年長期署名フォーマット相互運用性テストの概要

目的	・標準やJIS原案への長期署名フォーマットへの準拠性の確認 ・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)
内容	・共通データ検証機能準拠性テスト(2007年2~3月) ・国内署名生成・検証相互運用性テスト(2007年10~12月) ・JIS(原案)供給者適合宣言書の集計(2007年12月) ・国際実験 (2007年11月～2008年2月:実施中)
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-T, ES-Aのフォーマット生成・検証ができる実装を持つ組織 ・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
結果公表	・最終結果発表(2008年1月)

2007年実証実験参加企業(25組織)

(五十音順)

CAdES実験 (10→14)

- 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 ★
- 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
- リコー (オフラインのみ)

ETSI-ECOM 日欧XAdES事前実験

- エントラストジャパン
- カタルーニャ工科大 (スペイン)
- グラッツ工科大 / IAIK / A-SIT (オーストリア)
- 日本電気

全25社 前回比60%増

XAdES実験 (3→8)

- 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 (オフラインのみ)
- 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 情報技術総合研究所 ★
- ラングエッジ

ECOM国際実験 (0→9)

- Cryptolog (フランス)
- Safelayer (スペイン)
- 他、★印の日本企業7社

テスト用タイムスタンプ局 (1→3)

- アマノタイムビジネス
- セイコープレシジョン
- PFU

テストケース設計 (2→3)

- エントラストジャパン
- セコム
- 日本電気

ECOM CAdES/XAdES Plugtest 2007の特徴・メリット

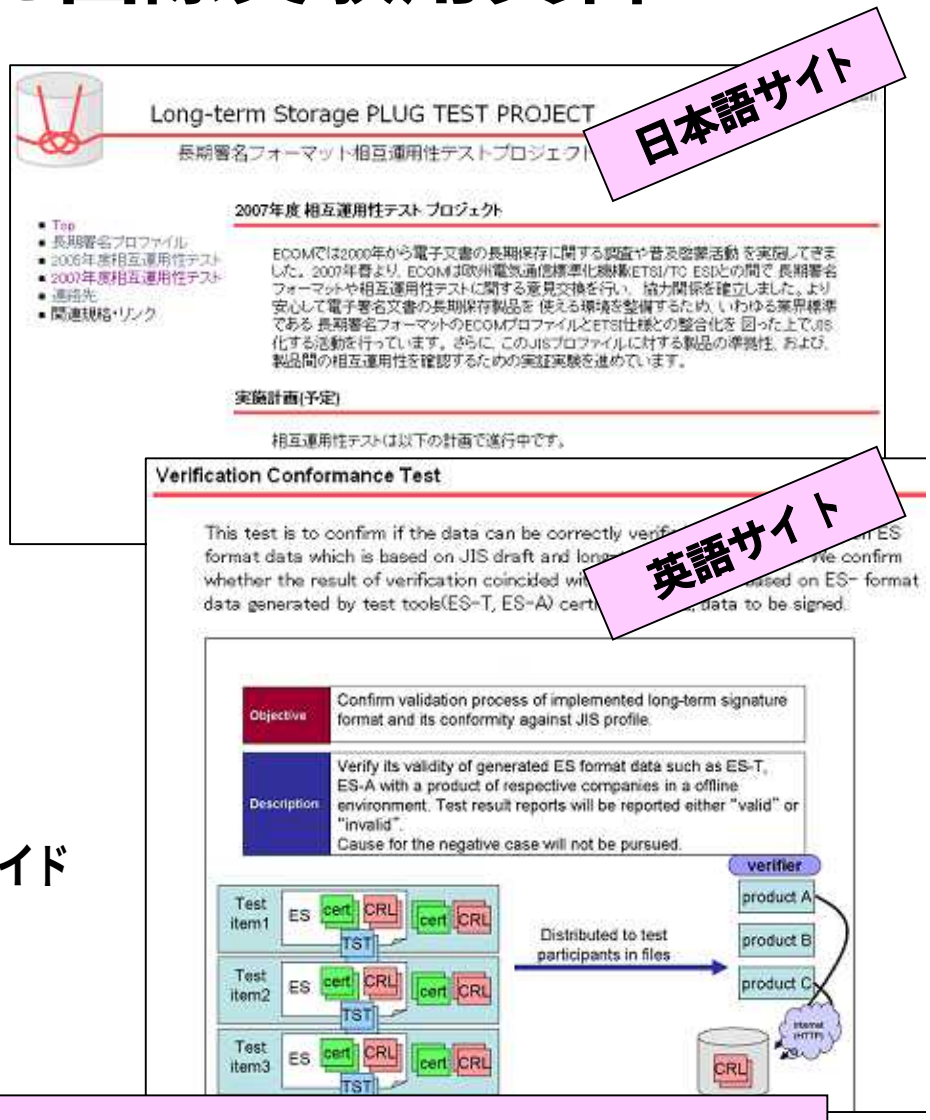
- CAdESおよびXAdESに関する世界最大の相互運用テストイベント
- 署名の生成と検証の双方の機能のテストができる
- 国内ほぼ全ての実装との相互運用性の確認
- 実験結果の公表
- 日本の時刻認証認定事業者3社による有償サービスと同等のハードウェアによるテスト用TSAの利用
- TSAは認証無しで利用でき、特別なTSP SDKは必要なし
- 連絡はメーリングリストで、ファイル交換はウェブを使い、担当者が時間がある時に何時でもテストできる。対面会議テスト説明会の2回のみ。
- 国内のみならず国際実験の実施
- JIS原案への準拠性の確認
- 標準仕様の確認、問題点の共有、最新情報の交換ができる貴重な機会
- 開発ツールキット、生成・検証ソフトウェア、文書管理システムのいずれでも参加できるようなテストケース設計

2005年と2007年の実験の違い

- 参加者数 60%増
- JIS原案の要件であるES-T, ES-Aフォーマットをテスト対象とした。ES-C、ES-Xなどは ES-Aテストに含まれる。
- タイムスタンプ取得には特別なTSP SDKを必要とせず、純粋なRFC 3161 TSP over HTTPを用いる。
- タイムスタンプ事業者3社を利用でき、いずれを使ってもよい。
- 準備不足により共通データ標準準拠性テストのテスト項目数は半減
- 生成･検証相互運用性テストの項目数は大幅増
- テスト合否判定基準を明瞭化(特に相互運用性テスト)
- カウンタ署名のテストの追加
- Enveloped XML署名のテストの追加
- Content/DataObject TS、ES-X Type1/Type2のテストの追加
- テスト概要、テスト仕様書、テストデータダウンロードのためのウェブサイトの整備
- 国際実験のため、英語版のサイト、ドキュメント類の整備

テスト用ウェブサイトと国際実験用資料

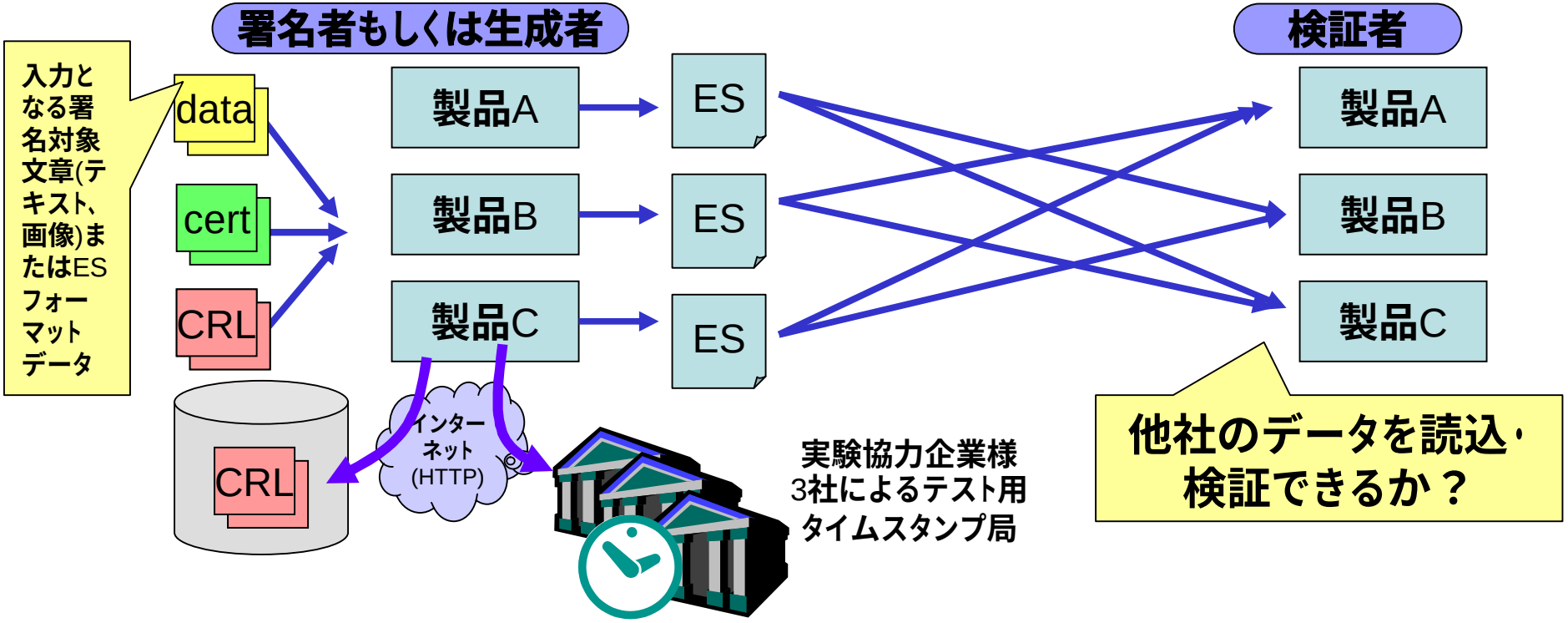
- 公開資料
  - テストケース仕様書(日本語/英語)
  - 共通データ検証テストのデータ
- 国内参加者向け資料
  - プラグテスト説明会資料
  - タイムスタンプ局に関するメモ
- 海外参加者向け英語資料
  - プラグテスト概要スライド
  - 署名者用CAガイド
  - タイムスタンプ局ガイド
  - ECOM電子会議室(ファイル共有)ガイド



公開資料･データは全て以下のURLからダウンロードできます
http://www.ecom.jp/LongTermStorage/index.html

署名データ生成･検証相互運用性テスト(旧オンラインテスト)

目的	･他社実装が生成した有効なCAdES/XAdES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を用いて各実装により有効であるようなCAdES/XAdESフォーマット(T, A)を生成する。各実装において読込み、他社の生成したデータが有効である事を検証する。

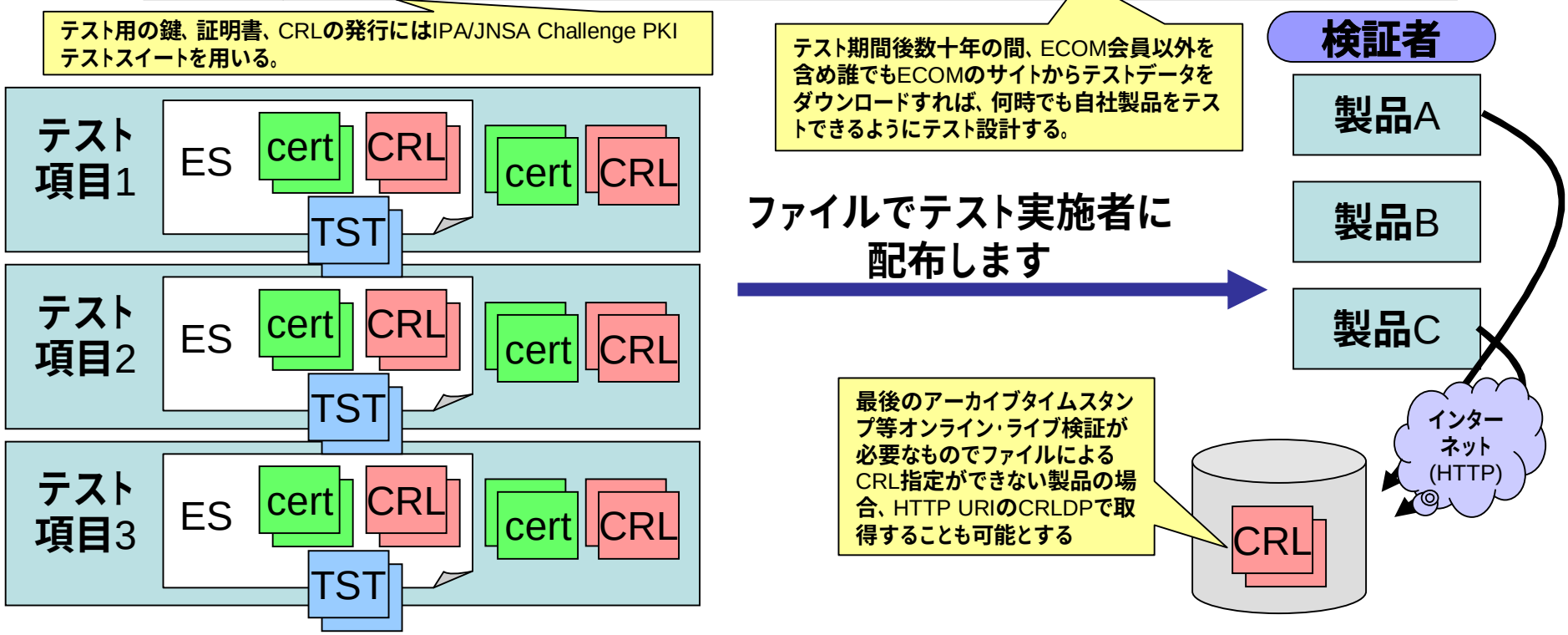


署名生成･検証相互運用性テストのテストケース

テストケース	内容
ES-T基本テスト	署名形式(enveloping, enveloped, detached)毎のタイムスタンプ付き署名の生成検証テスト
ES-Tタイムスタンプ局テスト	3つのテスト用タイムスタンプ局に対応しているか、確認するテスト
ES-Tオプショナル属性/プロパティテスト	ES-Tに付与可能なCAdES / XAdES で定められた各属性 / プロパティに対応しているか確認するテスト
ES-A基本テスト	署名形式(enveloping, enveloped, detached)毎に3個までのアーカイブタイムスタンプ付き署名の生成検証テスト
ES-Aオプショナル属性/プロパティテスト	ES-X Long Type 1 / 2、他 ES-A で付与可能な属性 / プロパティに対応するか確認するテスト

検証機能の標準準拠性テスト(旧オフラインテスト)

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-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。



共通データ検証機能標準準拠性テストのテストケース (CAdESの例)

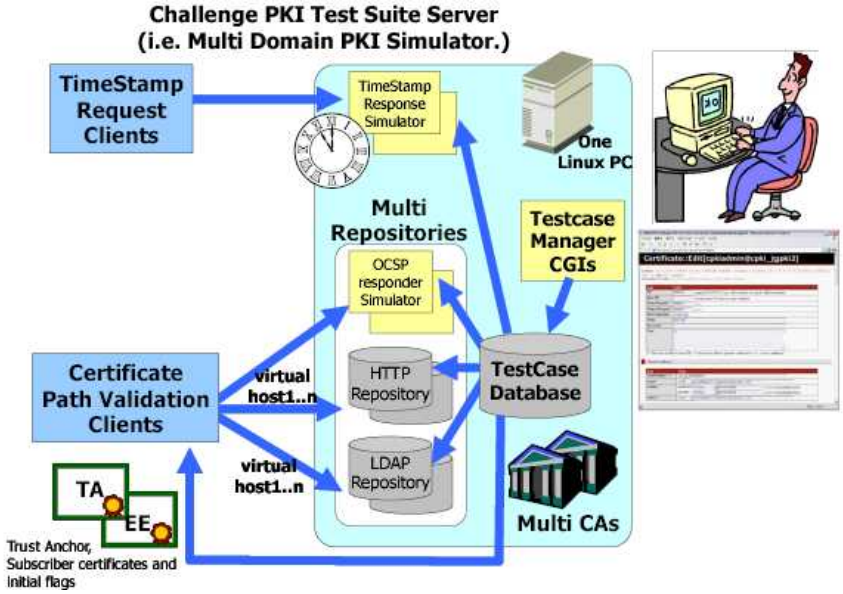
テストケース	テストケース内容
OFF-T-1	有効である一般的な内包署名のES-Tを読み込める
OFF-T-2	ES-Tの署名者証明書の期限切れを扱える
OFF-T-3	ES-Tの署名者証明書の失効を扱える
OFF-T-4	ES-Tの署名者証明書の認証パス検証を正しく行える
OFF-T-6	ES-TのSignerInfoの署名値の改竄を検知できる
OFF-T-7	ES-Tの署名タイムスタンプのトークンのSignerInfoの署名値改竄を検知できる
OFF-T-8	ES-TのMessageDigestのハッシュ値の改竄を検知できる
OFF-T-9	ES-Tの署名タイムスタンプのトークンのMessageDigestのハッシュ値改竄を検知できる
OFF-T-OP-11	ESSSigningCeritificateV2属性においてSHA-256であるES-Tフォーマットを扱える
OFF-T-OP-12	ESSSigningCeritificateV2属性においてSHA-512であるES-Tフォーマットを扱える
OFF-T-OP-13	カウンタ署名を付したES-Tフォーマットを扱える。
OFF-A-3	ETSI TS 101 733 v1.7.3に基づく内包署名の第一世代のES-Aを扱える
OFF-A-4	ETSI TS 101 733 v1.7.3に基づく分離署名の第一世代のES-Aを扱える
OFF-A-5	ETSI TS 101 733 v1.7.3に基づく内包署名の第二世代のES-Aを扱える
OFF-A-6	ETSI TS 101 733 v1.7.3に基づく分離署名の第二世代のES-Aを扱える

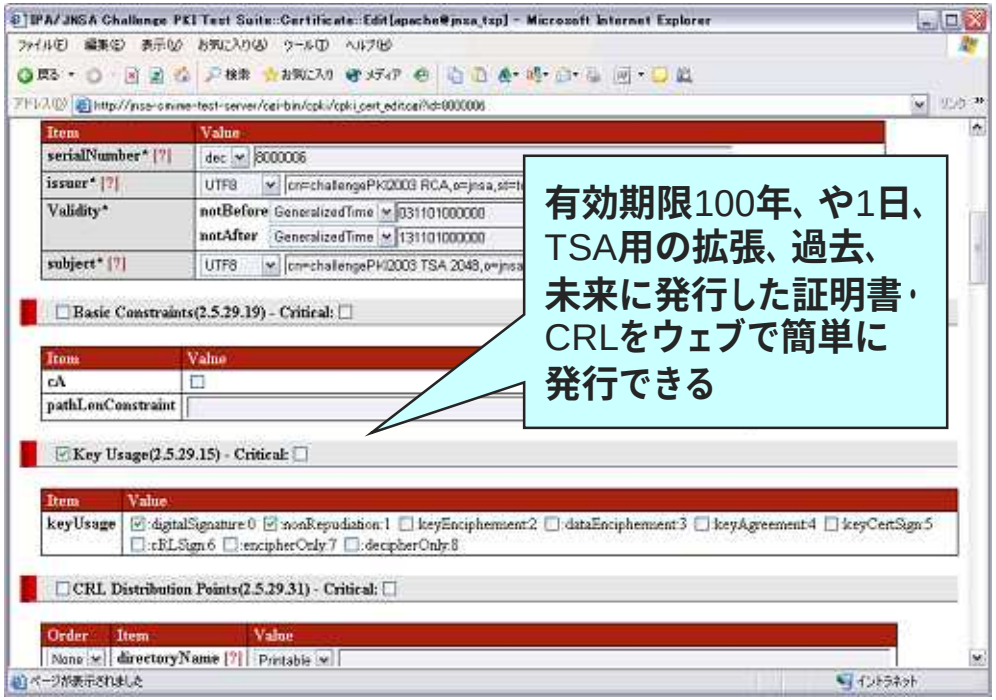
有効および、失効や改ざんなどで無効な署名を正しく検証できるかを確認

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**

JIS(原案)供給者適合宣言書の提出

- **<u>供給者適合宣言とは</u>**
  長期署名フォーマットの実装が生成と検証において、どの要素の対応を具備しているか生産者が公表するためのシート。JIS原案の付録となっている。

- **今回のプラグテストでは、宣言作成の練習として、参加者に記入してもらった。**

表 A.4－署名対象プロパティ要素

要素	要求レベル	生成	検証
署名対象の署名プロパティ	必ず	✔	✔
- 署名時刻	任意選択 a)	✔	✔
- 署名者証明書の参照情報	任意選択 a),b)	✔	✔
- 署名ポリシ識別子	要別途規定	—	—
- 署名生成場所	要別途規定	—	—
- 署名者の肩書き	要別途規定	—	—
署名対象データオブジェクトのプロパティ	要別途規定	—	—
- データオブジェクト形式	要別途規定	—	—
- コミットメント種別表示	要別途規定	—	—
- 全データオブジェクトに対するタイムスタンプ	要別途規定	—	—
- 個別データオブジェクトに対するタイムスタンプ	要別途規定	—	—
注 a) **ETSI TS 101 903** v1.1.1 の場合は必ずである。 b) 署名者証明書の参照情報か，又はかぎ情報（**表 A.2**）のいずれか一方が必要である。			

表 A.5－非署名対象プロパティ要素

要素	要求レベル	生成	検証
非署名対象の署名プロパティ	必ず	✔	✔
- カウンタ署名	任意選択		
- （署名時刻を確定する情報）	必		
- 署名タイムスタンプ			✔
- タイムマークなどその他の方式			—
非署名のデータオブジェクトのプロパティ		—	—

XAdESの例

CAdES-A プロファイルへの適合

表 A.6－追加される非署名属性

要素	要求レベル	生成	検証
全証明書参照情報群	必ず	✔	✔
全失効参照情報群	必ず	✔	✔
- CRL 形式の失効参照情報群	任意選択	✔	✔
- OCSP 形式の失効参照情報群	任意選択	✔	✔
- 他の形式の失効参照情報群	要別途規定	—	—
属性証明書の参照情報群	要別途規定	—	—
属性失効情報の参照情報群	要別途規定	—	—
証明書群	必ず	✔	✔
- 証明書	任意選択	✔	✔
- CA 等による証明書の保管	要別途規定	✔	✔
失効情報群	必ず	✔	✔
- CRL による失効情報	任意選択	✔	✔
- 基本 OCSP 応答	任意選択	✔	✔
- 他の失効情報	要別途規定	—	—
- CA 等による失効情報の保管	要別途規定	✔	
CAdES-C データへのタイムスタンプ(CAdES-C-timestamp)	要別途規定	✔	
タイムスタンプが付与された証明書及び失効情報に関する参照情報	要別途規		
（改ざん検知を可能とする情報）			✔

CAdESの例

実験結果

CAdES生成・検証相互運用テストの結果

テスト参加組織名(五十音順)		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		NEC		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		三菱電機 インフォメーション システムズ		JIS要求レベル
実装の提供形態(SDK/生成検証アプリ/文書管理システム)		SDK		SDK		アプリ		アプリ		SDK		SDK		アプリ		SDK		文管		SDK		アプリ		SDK		文管		
製品 / 試作品 区分		製品		試作		製品		製品		製品		試作		試作		製品		製品		試作		製品		試作		製品		
生成 / 検証		生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	
CAdES-T 基本テスト	ON-T-BASIC-ATTACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
	ON-T-BASIC-DETACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
CAdES-T タイムスタンプ局 テスト	ON-T-TSA-AMANO-ATTACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-T-TSA-PFU-ATTACHED	○	○	○	○	○	○	○	○	○	○	ー	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-T-TSA-SEIKO-ATTACHED	○	○	○	○	○	○	○	○	○	○	ー	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
CAdES-T オプショナル属性 テスト	ON-T-ATTR-SIGNINGTIME	ー	ー	○	○	○	○	ー	ー	○	○	ー	ー	ー	ー	○	○	ー	ー	ー	○	ー	ー	○	○	×	○	任意選択
	ON-T-ATTR-EPES-RFC3125	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	要別途
	ON-T-ATTR-SIGNERLOCATION	ー	ー	○	○	ー	○	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	要別途
	ON-T-ATTR-SIGNERATTRIBUTES-CLAIMED	ー	ー	○	○	ー	ー	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	要別途
	ON-T-ATTR-CONTENTHINTS	ー	ー	○	○	○	○	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	要別途
	ON-T-ATTR-COMMITMENTTYPEINDICATION	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	要別途
	ON-T-ATTR-CONTENTTS-CLAIMEDTIME	ー	ー	○	○	ー	ー	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	要別途
	ON-T-ATTR-CONTENTREFERENCE	ー	ー	○	○	ー	ー	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	要別途
	ON-T-ATTR-CONTENTIDENTIFIER	ー	ー	○	○	ー	ー	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	要別途
	ON-T-ATTR-COUNTERSIGNATURE	ー	ー	○	○	ー	○	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	○	○	○	ー	ー	任意選択
	ON-T-ATTR-ESSCERTV2	ー	ー	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ー	ー	ー	○	○	○	○	○	○	○	任意選択
CAdES-A 基本テスト	ON-A-BASIC-A1-ATTACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-A-BASIC-A1-DETACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-A-BASIC-A2-ATTACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-A-BASIC-A3-ATTACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
CAdES-A オプショナル属性 テスト	ON-A-ATTR-A1-ARCTSV1-ATTACHED	ー	ー	○	○	ー	ー	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	○	ー	○	ー	ー	ー	ー	任意選択
	ON-A-ATTR-A1-TIMESTAMPEDCERTSCRLS	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	要別途
	ON-A-ATTR-A1-ESCTIMESTAMP	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	ー	要別途
生成時のTSA証明書パス検証情報の格納方法		UA		F		F		UA		UA		F		UA		UA		UA		UA		UA		F		F		

XAdES生成・検証相互運用テストの結果

テスト参加組織名(五十音順)		エントラストジャパン		関電システムソリューションズ		TOiNX		NEC		富士ゼロックス		三菱電機		ランダエッジ		JIS要求レベル
実装の提供形態(SDK/生成検証アプリ/文書管理システム)		SDK		SDK		SDK		文管		文管		SDK		SDK		
製品 / 試作品 区分		試作		製品		試作		製品		製品		試作		製品		
生成 / 検証		生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	
XAdES-T 基本テスト	ON-T-BASIC-ENVELOPING	○	○	○	○	○	○	○	○	-	-	○	○	○	○	
	ON-T-BASIC-DETACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	
	ON-T-BASIC-ENVELOPED	○	○	○	○	○	○	○	○	-	-	○	○	○	○	
XAdES-T タイムスタンプ局テスト	ON-T-TSA-AMANO-ENVELOPING	○	○	ー	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-T-TSA-PFU-ENVELOPING	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-T-TSA-SEIKO-ENVELOPING	○	○	ー	○	○	○	○	○	-	-	○	○	○	○	任意選択
XAdES-T オプショナルプロパティテスト	ON-T-PROP-SIGNINGTIME	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-T-PROP-EPES-FREEXML	○	○	○	○	○	○	○	○	-	-	-	-	-	-	要別途
	ON-T-PROP-EPES-TR102038-V111	○	○	○	○	○	○	○	○	-	-	-	-	-	-	要別途
	ON-T-PROP-SIGNERPRODUCTIONPLACE	○	○	○	○	○	○	○	○	-	-	○	○	-	-	要別途
	ON-T-PROP-SIGNERROLE-CLAIMED	○	○	○	○	○	○	○	○	-	-	○	○	-	-	要別途
	ON-T-PROP-DATAOBJECTFORMAT	○	○	ー	ー	○	○	-	-	-	-	○	○	-	-	要別途
	ON-T-PROP-COMMITMENTTYPEINDICATION	○	○	○	○	○	○	-	-	-	-	○	○	-	-	要別途
	ON-T-PROP-ALLDATATS-CLAIMEDTIME	○	○	ー	○	○	○	-	-	-	-	-	-	-	-	要別途
	ON-T-PROP-INDVDATATS-CLAIMEDTIME	○	○	ー	○	○	○	-	-	-	-	-	-	-	-	要別途
	ON-T-PROP-COUNTERSIGNATURE	○	○	○	○	○	○	-	-	-	-	○	○	-	-	任意選択
	ON-T-PROP-SIGNINGCERTIFICATE	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
XAdES-A 基本テスト	ON-A-BASIC-A1-ENVELOPING	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-A-BASIC-A1-DETACHED	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-A-BASIC-A1-ENVELOPED	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-A-BASIC-A2-ENVELOPING	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-A-BASIC-A3-ENVELOPING	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
XAdES-A オプショナルプロパティテスト	ON-A-PROP-A1-REFS	○	○	○	○	○	○	○	○	-	-	○	○	-	ー	任意選択
	ON-A-PROP-A1-REFS-REFSONLYTS	○	○	ー	○	○	○	○	○	-	-	-	-	-	ー	要別途
	ON-A-PROP-A1-REFS-SIGANDREFSTS	○	○	ー	○	○	○	○	○	-	-	-	-	-	ー	要別途
生成時のTSA証明書パス検証情報の格納方法		F		F		F		F		F		F		FS		

凡例：
- 製品：有償、無償を問わず2008年までに製品またはソリューションの一部として提供予定の実装
- 試作品：社内の試作目的で開発された実装、もしくは2008年内に提供予定のない実装
- SDK：開発ツールキットまたはライブラリとして提供
- アプリ：独立した署名生成・検証ソフトウェアとして提供
- 文管：文書管理システムとして提供

共通データによる検証機能標準準拠性テスト

CAdES
結果

テストケース	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	NEC	日本電子公証機構	ハイパーギア	PFU	ビーパーケテクノロジー	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	テストケース内容
OFF-T-1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	有効である一般的な内包署名のES-Tを読み込める
OFF-T-2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-Tの署名者証明書の期限切れを扱える
OFF-T-3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-Tの署名者証明書の失効を扱える
OFF-T-4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-Tの署名者証明書の認証パス検証を正しく行える
OFF-T-6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-TのSignerInfoの署名値の改竄を検知できる
OFF-T-7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-Tの署名タイムスタンプのトークンのSignerInfoの署名値改竄を検知できる
OFF-T-8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-TのMessageDigestのハッシュ値の改竄を検知できる
OFF-T-9	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ES-Tの署名タイムスタンプのトークンのMessageDigestのハッシュ値改竄を検知できる
OFF-T-OP-11	ー	○	○	○	○	○	○	○	ー	○	○	○	○	○	ESSSigningCeritificateV2属性においてSHA-256であるES-Tフォーマットを扱える
OFF-T-OP-12	ー	○	○	○	○	○	○	○	ー	○	○	○	○	○	ESSSigningCeritificateV2属性においてSHA-512であるES-Tフォーマットを扱える
OFF-T-OP-13	ー	○	ー	○	○	ー	○	○	ー	ー	○	○	○	○	カウンタ署名を付したES-Tフォーマットを扱える。
OFF-A-3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ETSI TS 101 733 v1.7.3に基づく内包署名の第一世代のES-Aを扱える
OFF-A-4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ETSI TS 101 733 v1.7.3に基づく分離署名の第一世代のES-Aを扱える
OFF-A-5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ETSI TS 101 733 v1.7.3に基づく内包署名の第二世代のES-Aを扱える
OFF-A-6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ETSI TS 101 733 v1.7.3に基づく分離署名の第二世代のES-Aを扱える

XAdES
結果

テストケース	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	TOiNX	NEC	富士ゼロックス	三菱電機	ランゲエッジ	テストケース内容
OFF-T-1	○	○	○	○	○	○	○	○	有効である一般的な内包署名のES-Tを読み込める
OFF-T-2	○	○	○	○	○	○	○	○	ES-Tの署名者証明書の期限切れを扱える
OFF-T-3	○	○	○	○	○	○	○	○	ES-Tの署名者証明書の失効を扱える
OFF-T-4	○	○	○	○	○	○	○	○	ES-Tの署名者証明書の認証パス検証を正しく行える
OFF-T-6	○	○	○	○	○	○	○	○	ES-TのSignerInfoの署名値の改竄を検知できる
OFF-T-7	○	○	○	○	○	○	○	○	ES-Tの署名タイムスタンプのトークンのSignerInfoの署名値改竄を検知できる
OFF-T-8	○	○	○	○	○	○	○	○	ES-TのMessageDigestのハッシュ値の改竄を検知できる
OFF-T-9	○	○	○	○	○	○	○	○	ES-Tの署名タイムスタンプのトークンのMessageDigestのハッシュ値改竄を検知できる
OFF-T-10	○	○	○	○	○	○	○	○	detached署名のES-Tを扱える
OFF-A-1	○	○	○	○	○	○	○	○	enveloping署名の第一世代のES-Aを扱える
OFF-A-2	○	○	○	○	○	○	○	○	detached署名の第一世代のES-Aを扱える
OFF-A-3	○	○	○	○	○	○	○	○	enveloping署名の第二世代のES-Aを扱える
OFF-A-4	○	○	○	○	○	○	○	○	detached署名の第二世代のES-Aを扱える

総合合否結果

CAdES総合結果

テスト参加組織名	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		NEC		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	
生成 / 検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証
CAdES-Tの基本機能の提供	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	－	○1
CAdES-Tのオプション機能の提供	－	－	○	○	○	○	○	○	○	○	○	○	○	○	○	○	－	－	－	○	○	○	○	○	○	○	－	－
CAdES-Aの基本機能の提供	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	－	○1
CAdES-Aのオプション機能の提供	－	－	○	○	－	－	－	－	○	○	－	－	－	－	－	－	－	－	－	○	－	○	－	－	－	－	－	－

XAdES総合結果

テスト参加組織名	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		TOiNX		NEC		富士 ゼロックス		三菱電機		ランゲエッジ	
生成 / 検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証	生成	検証
XAdES-Tの基本機能の提供	○	○	○	○	-	○1	○	○	○	○	○	○	○	○	○	○
XAdES-Tのオプション機能の提供	○	○	○	○	-	-	○	○	○	○	-	-	○	○	○	○
XAdES-Aの基本機能の提供	○	○	○	○	-	○1	○	○	○	○	○	○	○	○	○	○
XAdES-Aのオプション機能の提供	○	○	○	○	-	-	○	○	○	○	-	-	○	○	-	-

【参加した全実装が合格】

基本テストに合格していれば、生成、検証のいずれかがJIS原案の必須要件を満足している。

凡例
○ 合格：生成/検証の結果に標準準拠性並びに相互運用性上の問題が無い
○1 合格：共通データ検証テストのみ実施した結果、検証機能に問題が無い
× 不合格：生成/検証の結果に標準準拠性もしくは相互運用性上の問題がある
－ 非サポート：実装が該当する生成/検証の機能を提供していない

国際実験状況

ETSI-ECOM XAdES日欧事前実験 (2007年1～3月)

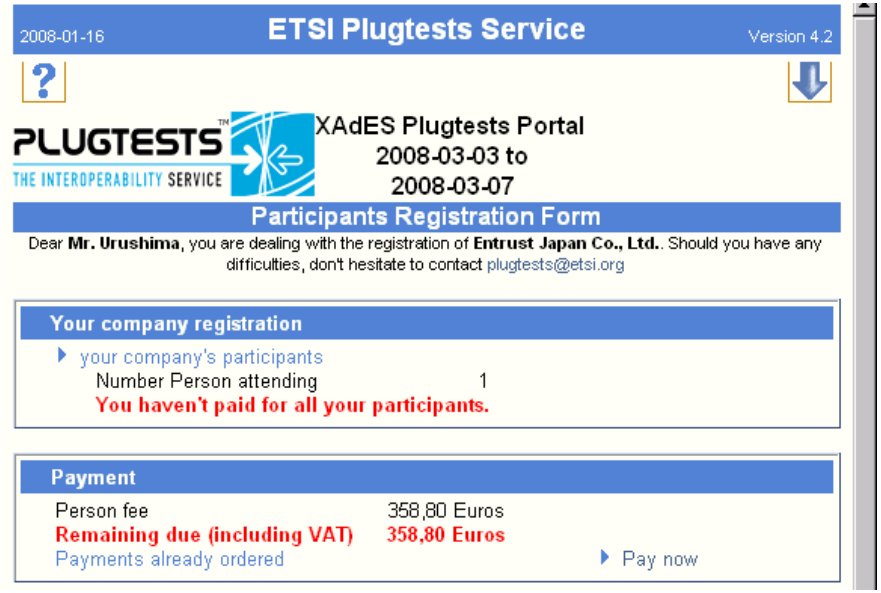
- 2008年3月に実施されるETSI XAdES Plugtestの準備として XAdES事前実験を実施
- 参加組織
  - スペイン：カタルーニャ工科大
  - オーストリア：内務省研究所(A-SIT,IAIK)
  - 日本電気
  - エントラストジャパン
- 実験協力
  - アマノタイムビジネス (※1)
- 実験内容
  - ECOM署名生成・検証相互運用性テストと同等
  - 認証局はIAIK (CRL+OCSP)
  - テスト計画、設計書、データ交換はメールベース。月1電話会議


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)
SigningTime
SigningCertificate
SignaturePolicyIdentifier
SignatureProductionPlace
SignerRole
DataObjectFormat
CommitmentTypeIndication
AllDataObjectsTimeStamp
OVC: 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。

ETSI XAdES Plugtest (2008年3月)

- **参加費 税込**358.8**ユーロ**
- **期間**：2008 03/03-03/07
- **実施内容**
  ECOM**テストと同じリモートテスト**
  - **共通データ標準準拠性テスト**
  - **生成･検証相互運用性テスト**
  - **電話会議･自己紹介･製品紹介**
- **スケジュール**
  2007.12.10 **ポータル**,ML**公開**
  2008.02.15**申込、送金**✔
  2008.03.03**テスト開始**



ETSI**に対しCAdES、XAdES双方の相互運用テストの実施に向け働きかけをしてきたが、**XAdES**テストのみしか実現できなかった。**

http://www.etsi.org/plugtests/XAdES/XAdES.htm

ECOM 国際実験 (2007年11月～2008年2月)

- ETSI ESI会議やMLでのアナウンスやホームページからの問い合わせにより、参加の申し出のあった海外2社および日本の有志企業8社が参加
  - Safelayer社 (スペイン)
  - Cryptolog社 (フランス)

- 実験内容
  - CAdESおよびXAdESの双方の実験を実施
  - 署名データ生成・検証相互運用性テストのみ
  - テストケースは国内実験と全く同じ
  - 1月末：署名生成結果送付〆、2月中旬：署名検証結果送付〆

現在、実験実施中

テスト結果にみる
日本国内の実装の傾向

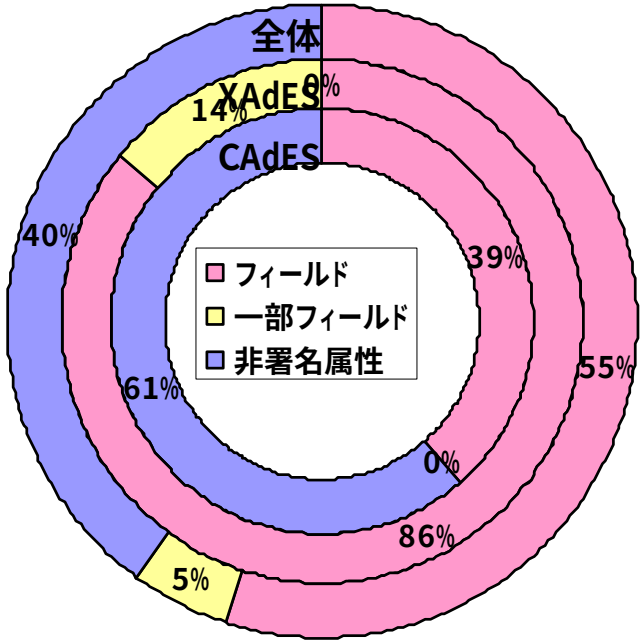
テスト結果にみる日本のCAdES/XAdES実装の傾向(1/2)

- **全体**
  - CAdES/XAdES**比率**：CAdES=65% XAdES=35%
  - **製品**: 60%、**試作品**: 40%
  - **実装種別**：SDK:60%, **生成検証アプリ**:20% **文書管理製品**:20%
- JIS
  - JIS**任意選択のサポート**：CAdES: 81% XAdES:85% **全体**:82%
  - JIS**要別途規定のサポート**：CAdES:13% XAdES:53% **全体**:27%
- CAdES / XAdES**の属性/プロパティのサポート状況**
  - **署名ポリシのサポート**：CAdES: 8% XAdES:57% **全体**:25%
  - **カウンタ署名のサポート**: CAdES: 31% XAdES:57% **全体**:40%
  - CAdES RFC 3126 ArcTSV1**サポート率**：**生成**:15% **検証**:30%
  - ES-X Long Type ½**のサポート**：CAdES:8% XAdES:50% **全体**:23%

CAdESはJIS対応の最小限の機能を実装し、XAdESはJISにとらわれず柔軟に幅広くプロパティを実装する傾向がある。

テスト結果にみる日本のCAdES/XAdES実装の傾向(2/2)
~ タイムスタンプのTSA証明書検証情報の格納 ~

- **日本の実装の100%はタイムスタンプトークン内にTSA証明書を検証するのに必要な全ての証明書、CRLを格納する事に対応している。**
- **4つの格納方式**
  - **フィールド: トークンのcertificatesおよびcrlsフィールドに格納**
  - **一部フィールド: 上と同じだが署名タイムスタンプのみ署名者証明書用のCertificate Values, RevocationValuesに格納**
  - **非署名属性: トークンの非署名属性のCertificateValues, RevocationValuesに格納**
  - **ファイル: 検証情報はトークンに格納せず別途ファイルとして提供する。**



CAdESでは非署名属性に格納するケースがやや多く(61%)、
XAdESではフィールドに格納するケースがほとんど(86%)である。
検証については、どこに格納されていても100%の実装が対応できる。

CAdES / XAdES フォーマット
相互運用性上の課題

テスト期間中に修正され解決された起こりやすい問題

実証実験は2回目を向え、7割が前回実験の参加者であることから、概ね大きな問題は発生しなかった。

- CAdES
  - eContent、certificates, crlsフィールドがBERであることを想定していなかった処理の誤り
  - signedAttrsがDER SET OFでソートされていない
  - CompleteCertificateRefsのOtherCertIDのissuerSerialの不足
  - CompleteRevocationRefsの構造の誤り(CertRefsとの対応関係)
- XAdES
  - XML署名のId属性の重複、不足、入れてはならない場所への挿入
  - ReferenceのSignedPropertiesのType属性の値
- **共通**
  - TimeStampTokenがミリ秒以下の分解能を持つ場合の処理の誤り
  - **検証時刻前の古い検証情報の誤った格納**
  - **検証情報、検証参照情報の不足**
  - TSA証明書検証情報の格納方法の対応/非対応による検証失敗
  - **失効情報の猶予期間**
  - TimeStampTokenとSigningTimeの順序関係

タイムスタンプトークンの時刻監査証に起因する相互運用性上の問題点

【時刻監査証(TAC)とは】時刻配信事業者(TA)が時刻認証事業者(TSA)の機器に対し時刻配信する際、どれくらい時間のずれがあったかTAが監査した結果を表すX.509 V2属性証明書。

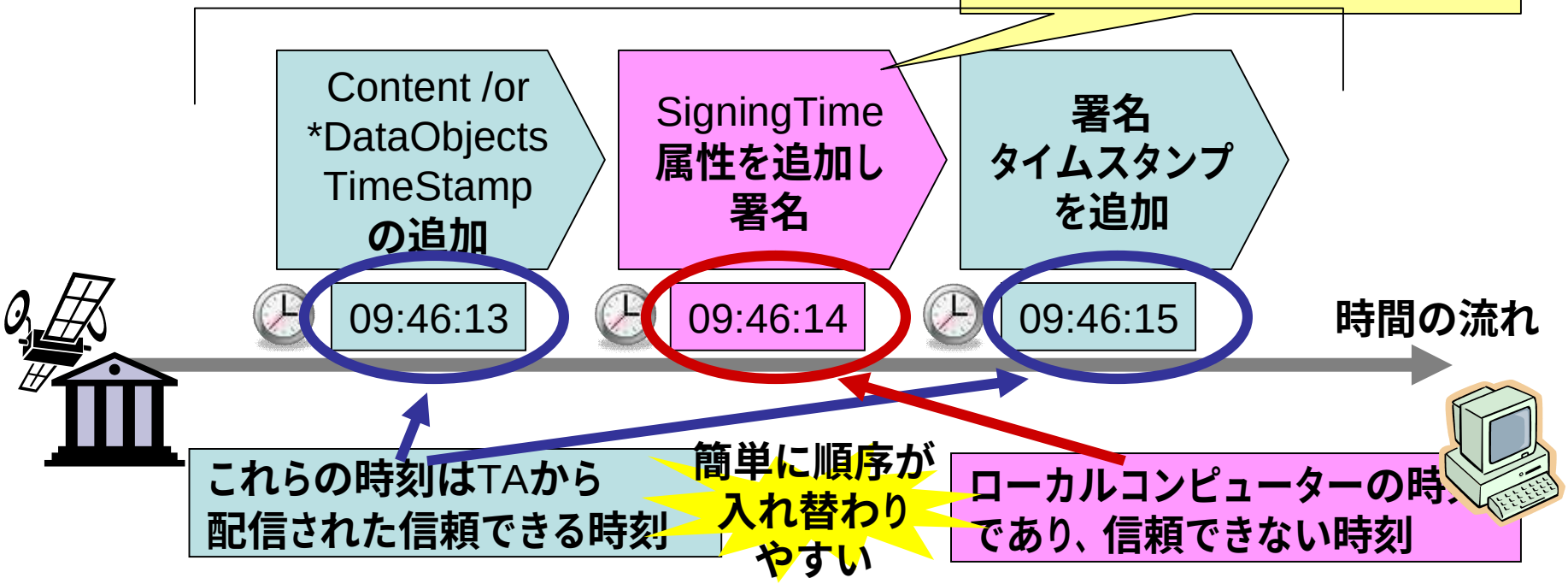
問題	原因	解決策もしくは解決案
TACを含むトークンを読込む際、エラー、警告が現れる	[TA] TACのASN.1 INTEGERのエンコーディングに誤りがある	TAにて改修して頂ける予定
	[TSA]V2属性証明書であるTACをV1属性証明書の領域に格納しており、CMSに違反している	CMS違反だがPDF対応のため仕方ない面もある。日本ではCAdES/XAdES実装側で工夫している場合も。TACを知らない海外実装の一部では問題がある場合も
トークン検証時にTACの改ざんエラーが出る	[アプリ]上記2点をファイル出力時に自動的に修復してしまうCMSの実装があった	TACを外してトークンを含めるか、トークンのエンコーディングが変更されないようCAdES/XAdESの実装側で工夫する。

SigningTimeとタイムスタンプの比較の問題

SigningTimeは古くからCMSにある署名者が主張する(正しいかどうかわからない)署名時刻であるが、タイムスタンプと一緒に使う場合、順序関係が問題となる。

署名アプリケーションでは、一回のボタン操作で署名から署名タイムスタンプの付与まで行ってしまう実装があるが、このような場合問題が発生しやすい。

署名するマシンのローカル時計が合っていなければ、順序は守れず**無効な署名**となる。
(CAdES v1.7.3 C3.6)
(XAdES v1.3.2 G2.2.16)



【解決結果】そもそも、このような時刻の比較は意味がなく、時刻としてはタイムスタンプのみを信頼すれば十分なので、CAdES、XAdESの仕様から削除するようECOMからETSI ESIに提言。またIETF S/MIME WGの議論でも提言を行い、RFC 3126の後継となるCAdESのRFCではこのような比較は削除された。CAdES v1.7.4ドラフトでも同様に削除されている。

CAdES / XAdESに関連する脆弱性問題 (参考)

CAdES	- 2002〜2003年 OpenSSL ASN.1関連のバッファーオーバーフロー問題 - 2004年 Microsoft ASN.1 Libraryのバッファーオーバーフロー問題
XAdES	- 2007年 XMLDSIG Command Injection: XSLTに起因するXML署名の脆弱性

ほぼ解決？

NEW

2007年4月 脆弱性情報「XML Digital Signature Command Injection Vulnerability」
[出典] http://www.isecpartners.com/advisories/2007-04-dsig.txt

原因	Java SE 6にも標準で組み込まれている Apache Xalan系のXSLT処理系でデフォルトextensionを有効になっており、XSLTで任意のプログラムコードが実行できる。 (Java SE 6 update 2で修正済)
影響	XML署名のSignedInfoのReferenceやKeyInfoのRetrievalMethodではTransformにXSLTが使えるため、攻撃者がそこにコマンド実行や意図的に負荷を高める処理を含めた場合、コマンド実行によるホストの乗っ取りや、DoS攻撃が可能となる。

```
<Signature>
 ...
 <Reference URI="#aa">
  <Transform>
   <xsl:stylesheet>
   任意のJava実行可→
   Runtime.exec(CMD実行)
   </xsl:stylesheet>
  </Transform>
 </Reference>
 ...
</Signature>
```

XML署名,XAdES,SAML,SOAP,WS-Securityなど不特定多数から受け取るXML署名/暗号の場合に問題となる。

実証実験に関する今後の課題

実証実験に関する今後の課題

- **後方互換性を確認するテストの充実**
  - **フォーマットができて数年なのに過去のフォーマットを検証できない実装が多いのは大問題** → 10**年、**20**年とフォーマットが持たない**
  - CAdES：ArchiveTimeStamp V1 / V2 **のテスト**
  - XAdES：**バージョン毎に名前空間が違う問題の解決とテストケースの提供**
- XAdES**における**SHA2**ファミリのテストの充実**
  - XML**署名では**SHA2**アルゴリズム**URL**を規定する組織が**W3C**でなく混乱**
  - SHA2**に対応する実装も少ないのでは？**
- **その他テストケースの充実**
  - OCSP、OASIS DSS XML TimeStamp
  - **共通データ検証テストでは今回準備の都合で**25%**減少したが、これを復活**
  - **共通データ検証テストで、全ての属性、プロパティのテストを提供**
- **国際実験用のファイル共有スペース**
  - **現状の**ECOM**電子会議室では日本語**GUI**のため無理がある**
  - sourceforge.com**など使ってはどうか？**
- OASIS DSS (CAdES/XAdES) **の生成、検証プロトコルのテスト？**

まとめ

- CAdES / XAdES **長期署名フォーマット**
  - CMS,XML**署名の拡張**

- ECOM CAdES / XAdES Plugtest 2007
  - **世界最大の**CAdES/XAdES**テストイベント**(25**社が参加**)
  - **国内実験完了**
  - **国際実験**2008**年**2**月終了予定**
  - **国内参加の全実装が**JIS**原案準拠性に合格**
  - **テスト手順、テスト仕様、合否判定がより洗練され明瞭になった**
  - **相互運用性上の残課題** (ASN.1 BER, **後方互換性**, TAC)
    - **→ 標準へのフィードバック** (ETSI ESI)
  - **テスト内容に関する課題はテストケース拡充(後方互換**, OCSP, SHA2)

  - **テスト結果の詳細なレポートはウェブサイトで公開予定**

http://www.ecom.jp/LongTermStorage/index.html

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
  - http://www.w3.org/TR/XAdES/ (W3C XAdES 2003.02, ETSI TS 101 903 v1.1.1**にもとづく**)
- 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-07.txt (2007.11.20 CAdES 1.7.3**ベースの最終ドラフト**)
  - 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/LongTermStorage/index.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