ECOM CAdES/XAdES Plugtest 2007

結果報告書

初版：2008 年 2 月 25 日

次世代電子商取引推進協議会
電子署名普及ワーキンググループ
長期署名フォーマット相互運用性実証実験プロジェクト

.

目次

1 はじめに

次世代電子商取引推進協議会(ECOM)では、2004 年 CAdES/XAdES 長期署名フォーマット[1][2]の普及に伴い日本国内での相互運用性を確保する目的でフォーマットの最小限の要件として ECOM プロファイル[3][4]を定め、その翌年 2005 年に ECOM プロファイルの準拠性を確認するための相互運用実証実験[5]を行った。2006 年には ECOM プロファイルに基づき関係団体ならびに有識者が集まり CAdES/XAdES プロファイルの JIS 原案[6][7]を作成し、2008 年 3 月にはこれが JIS として制定される見通しである[10][11]。その間、着実に国内外における CAdES / XAdES の実装が増えており、2007 年度、国内外の CAdES/XAdES の実装を持つ 21 の組織が集まり標準仕様ならびに JIS 原案の相互運用性ならびに標準準拠性を確認するため実証実験「ECOM CAdES/XAdES Plugtest 2007」を実施した。本報告書では、この実証実験の概要について報告する。

2 テスト概要

テストは CAdES/XAdES で規定されたフォーマットのうち、異なる組織間で交換されることが多く、JIS 原案における要件ともなっている CAdES-T、XAdES-T、CAdES-A および XAdES-A フォーマットを対象とし、CAdES/XAdES を規定する基礎となる標準と、このうち最小限の要件を定めた JIS 原案に対する準拠性ならびに相互運用性を確認することを目的とし、以下の 2 種類のテストを実施した。

- 共通データ検証機能標準準拠性テスト(2007 年 1 月～3 月)
  実証実験事務局で事前に作成した ES-T、ES-A フォーマットの署名データ、検証情報を用い、これが正しい署名か、そうでないかを期待値通り正しく検証する機能を有しているかを確認するテスト。署名値やハッシュ値の不一致、証明書の失効、期限切れなど無効な署名データの検証も含まれている。

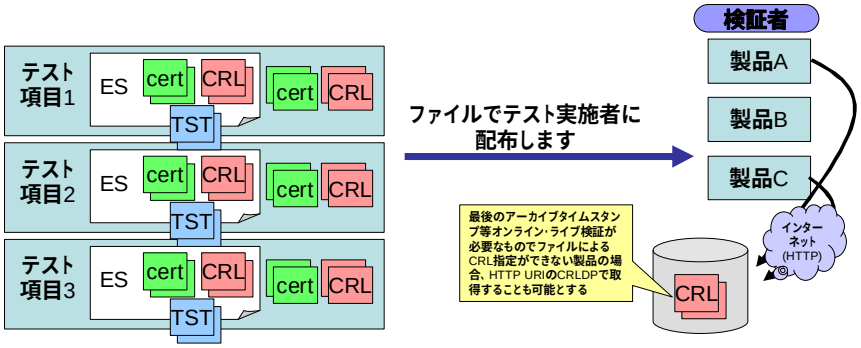


図 2.1 共通データ検証機能標準準拠性テストの方法

- 署名生成･検証相互運用性テスト(2007 年 10 月～12 月)
  各参加者の持つ実装により、テスト用タイムスタンプ局を用いてテスト仕様書の要件にあった ES-T、ES-A フォーマットの署名を生成し、これを他の実装が正しく検証できるか、生成･機能の相互運用性を確認するテスト。

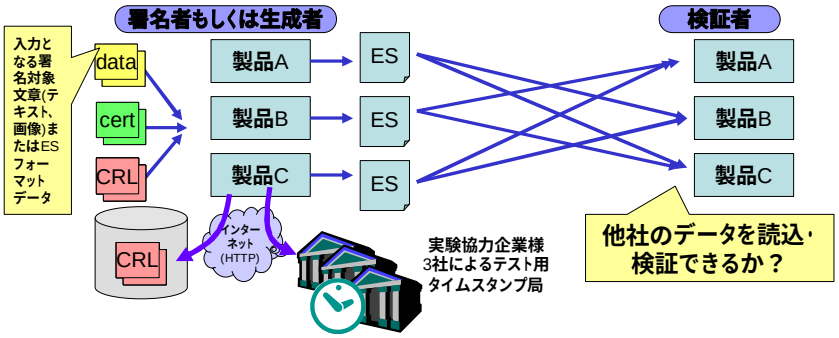


図 2.2 署名生成･検証相互運用性テストの方法

JIS の長期署名フォーマットプロファイルには供給者適合宣言書(文献[10][11]附属書 A を参照)というチェックシートが含まれている。これは、署名のどの要素の生成および検証をサポートしているのか、導入側が参考にできるようにするための情報である。本実験では参加者に供給者適合宣言書の提出を依頼した。

実験に際し、国内外向けの実証実験用のウェブサイトを整備した[8]。テストの方法、内容、テストケースなどを定めたテスト仕様書やテストデータは日本語版および英語版の双方がウェブサイトよりダウンロード可能である。テスト内容の詳細については、ウェブサイトの資料の方を参照されたい。

2.1 実証実験メンバー

(参加組織名五十音順、敬称略)

リーダー	エントラストジャパン株式会社	漆嶌　賢二
メンバー	RSA セキュリティ株式会社	八束　啓文
メンバー	RSA セキュリティ株式会社	井上　正彦
メンバー	関電システムソリューションズ株式会社	末武　陽一
メンバー	関電システムソリューションズ株式会社	竹村　健一
メンバー	サートラスト株式会社	三崎　友明
メンバー	株式会社スカイコム	柴田　信彦
メンバー	大日本印刷株式会社	長島　健一
メンバー	セコム株式会社	佐藤　雅史
メンバー	株式会社帝国データバンク	和田　宗樹
メンバー	東北インフォメーション・システムズ株式会社	横田　勇一
メンバー	東北インフォメーション・システムズ株式会社	劉　樹軍
メンバー	日本電気株式会社	後藤　淳
メンバー	日本電気株式会社	石井　真之
メンバー	株式会社日本電子公証機構	大野　雅生
メンバー	株式会社ハイパーギア	天田　敦
メンバー	株式会社 PFU	今井　秀和
メンバー	株式会社 PFU	南　能之
メンバー	ビーパークテクノロジー株式会社	赤星　昌幸
メンバー	富士ゼロックス株式会社	小池　正通
メンバー	富士ゼロックス株式会社	時得　克司
メンバー	三菱電機株式会社 情報技術総合研究所	山中　忠和
メンバー	三菱電機インフォメーションシステムズ株式会社	田中　学
メンバー	有限会社ラング・エッジ	宮地　直人
メンバー	株式会社リコー	斉藤　聡
メンバー	Cryptolog International (フランス)	Julien Stern
メンバー	Safelayer Secure Communications (スペイン)	Susana A. Bello

実験協力	アマノタイムビジネス株式会社	市川　桂介
実験協力	アマノタイムビジネス株式会社	上田　祐輔
実験協力	株式会社ＰＦＵ	今井　秀和
実験協力	セイコープレシジョン株式会社	浜原　研作
実験協力	セイコープレシジョン株式会社	中嶋　勝治
相談役	日本電気株式会社	木村　道弘
相談役	三菱電機株式会社 情報技術総合研究所	宮崎　一哉
事務局	次世代電子商取引推進協議会	前田　陽二

2.2 実験実施体制

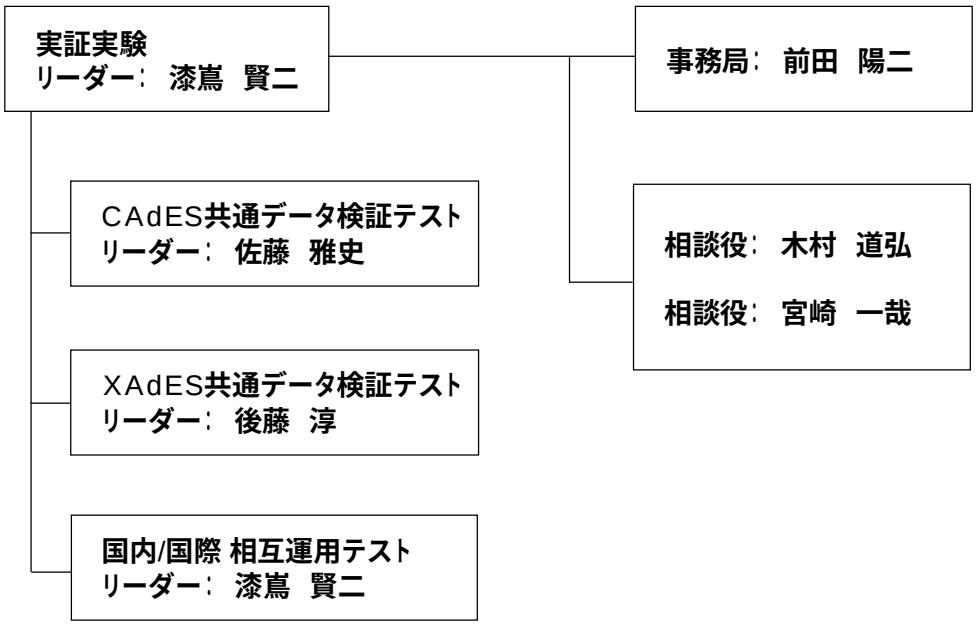


図 2.3　実証実験実施体制図

2.3 参加実装

実証実験に参加した組織とそれらの実装は以下の以下の通り。

表 2.1 実証実験参加組織一覧

組織および実装の名称 (五十音順 全 23 組織)	提供種別	用途種別	CAdES	XAdES	国際実験	事前実験
RSA セキュリティ株式会社						
RSA BSAFE e-文書法対応ライブラリ (version 1.3)	製	開	○			
エントラストジャパン株式会社						
CAdES Add-on for Entrust/IAIK Java Toolkit (build 20071124)+Jython Scripts	試	開	○		○	
XAdES Add-on for Entrust/IAIK Java Toolkit (build 20071207)+Jython Scripts	試	開		○	○	○
関電システムソリューションズ株式会社						
XAdES 長期署名ライブラリ for .NET V2.2	製	開		○		
サートラスト株式会社						
WebSign/FileSign/SignVerifier Ver3.3.0.7	試	ソ	○			
株式会社スカイコム						
SkyPDF Tools for ArchivingSignature (Version 1.6)	製	ソ	○			
大日本印刷株式会社						
SecureStarXML3.0 for Java	試	開		○		
セコム株式会社						
セコム長期署名ライブラリ(バージョン 1.4.5)+テスト用サンプル実装(ver 0.9)	製	開	○		○	
株式会社帝国データバンク						
TDB 長期署名ライブラリ V0.5	試	開	○			
東北インフォメーション・システムズ株式会社						
TOiNX XML 長期署名モジュール(仮称)バージョン 1.0	試	開		○		
日本電気株式会社						
PDF 長期署名プラグイン version2.1 + プロトタイプ	試	ソ	○		○	
PKI サーバ/Carassuit 原本保管サーバ Version 3.0	製	管		○	○	○
株式会社日本電子公証機構						
JN+ (電子署名・タイムスタンプ付与/検証ソフト)長期署名オプション	試	開	○			

株式会社ハイパーギア						
HG/PscanServPro 長期保存署名対応版 Ver0.9.1	試	管	○			
株式会社 PFU						
長期署名ライブラリ（Build：1.0.10.30）	試	開	○		○	
ビーパークテクノロジー株式会社						
DocStamper Version2.0/ESChecker Version2.0	製	ソ	○		○	
富士ゼロックス株式会社						
ArcSuite 2.3 原本性保証オプション	製	管		○	○	
三菱電機株式会社 情報技術総合研究所						
CMS 長期署名ライブラリ Ver 3.0	試	開	○		○	
XML 長期署名ライブラリ Ver 1.0	試	開		○	○	
三菱電機インフォメーションシステムズ株式会社						
三菱署名延長システム MistyGuard<EVERSIGN> V3.00 (改版予定品)	製	管	○			
有限会社ラング・エッジ						
Le-XAdES Library Ver0.98f+XAdEStool クライアントβ40(テスト用ツール)	製	開		○		
株式会社リコー						
長期署名ライブラリ Ver 0.1	試	開	○			
カタルーニャ工科大学(スペイン)	製	開		○		○
A-SIT / グラッツ工科大学(IAIK) (オーストリア)	製	開		○		○
Safelayer Secure Communications, S.A. (スペイン)						
TrustedX Services Platform 2.3.08S1R1	製	開	○		○	
TrustedX Services Platform 2.2.06S2R1_B04	製	開		○	○	
Cryptolog International (フランス)						
cryptolog implementation	試	開	○		○	
cryptolog implementation	試	開		○	○	

凡例：

提供種別：　「製」：製品、「試」：試作品・プロトタイプ

用途種別：　「開」：開発ツールキット、「ソ」：生成・検証ソフト、「管」：文書管理システム

国際実験：ECOM CAdES/XAdES Plugtest 2007 国際実験グループによる実証実験

事前実験：ETSI-ECOM XAdES Plugtest 事前実験(ETSI XAdES Plugtest 2008 の事前準備として)

また、テスト用タイムスタンプ局、テスト設計、テストデータ作成について以下の企業に御協力頂いた。

表 2.2　実証実験協力組織一覧

テスト用タイムスタンプ局提供（五十音順）
・　アマノタイムビジネス株式会社
・　セイコープレシジョン株式会社
・　株式会社 PFU
テスト設計、テストデータ作成（五十音順）
・　エントラストジャパン株式会社
・　セコム株式会社
・　日本電気株式会社

3 テスト結果

署名生成・検証相互運用性テストの生成・検証機能の各テスト項目におけるテスト結果は以下の通りであった。

表 3.1 CAdES 署名生成・検証相互運用性テスト集計結果

CAdES生成・検証相互運用性テスト 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		ピーバーク 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		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	○	○	○	○	○	○	○	○	○	○	–	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
	ON-T-TSA-SEIKO-ATTACHED	○	○	○	○	○	○	○	○	○	○	–	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	任意選択
CAdES-T オプショナル属性テスト	ON-T-ATTR-SIGNINGTIME	–	–	○	○	○	○	–	–	○	○	–	–	–	–	○	○	–	–	–	–	○	–	○	○	×	○	任意選択
	ON-T-ATTR-EPES-RFC3125	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	要別途
	ON-T-ATTR-SIGNERLOCATION	–	–	○	○	–	○	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	要別途
	ON-T-ATTR-SIGNERATTRIBUTES-CLAIMED	–	–	○	○	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	要別途
	ON-T-ATTR-CONTENTHINTS	–	–	○	○	○	○	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	要別途
	ON-T-ATTR-COMMITMENTTYPEINDICATION	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	要別途
	ON-T-ATTR-CONTENTTS-CLAIMEDTIME	–	–	○	○	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	要別途
	ON-T-ATTR-CONTENTREFERENCE	–	–	○	○	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	要別途
	ON-T-ATTR-CONTENTIDENTIFIER	–	–	○	○	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	要別途
	ON-T-ATTR-COUNTERSIGNATURE	–	–	○	○	–	○	–	–	○	○	–	–	–	–	–	–	–	–	–	–	○	○	○	○	–	–	任意選択
	ON-T-ATTR-ESSCERTV2	–	–	○	○	○	○	○	○	○	○	○	○	○	○	○	–	–	–	○	○	○	○	○	○	○	○	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	–	–	○	○	–	–	–	–	○	○	–	–	–	–	–	–	–	–	–	–	○	–	○	–	–	–	任意選択
	ON-A-ATTR-A1-TIMESTAMPEDCERTSCRLS	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	要別途
	ON-A-ATTR-A1-ESCTIMESTAMP	–	–	○	○	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	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		F		F				

表 3.2 XAdES 署名生成・検証相互運用性テスト集計結果

XAdES生成・検証相互運用性テスト 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		TOMX		NEC		富士ゼロックス		三菱電機		ラングエッジ		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	○	○	–	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-T-TSA-PFU-ENVELOPING	○	○	○	○	○	○	○	○	-	-	○	○	○	○	任意選択
	ON-T-TSA-SEIKO-ENVELOPING	○	○	–	○	○	○	○	○	-	-	○	○	○	○	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	○	○	–	–	○	○	-	-	-	-	○	○	-	-	要別途
	ON-T-PROP-COMMITMENTTYPEINDICATION	○	○	○	○	○	○	-	-	-	-	○	○	-	-	要別途
	ON-T-PROP-ALLDATATS-CLAIMEDTIME	○	○	–	○	○	○	-	-	-	-	-	-	-	-	要別途
	ON-T-PROP-INDVDATATS-CLAIMEDTIME	○	○	–	○	○	○	-	-	-	-	-	-	-	-	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	○	○	○	○	○	○	○	○	-	-	○	○	-	–	任意選択
	ON-A-PROP-A1-REFS-REFSONLYTS	○	○	–	○	○	○	○	○	-	-	-	-	-	–	要別途
	ON-A-PROP-A1-REFS-SIGANDREFSTS	○	○	–	○	○	○	○	○	-	-	-	-	-	–	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:
○: 合格:当該テスト項目の生成/検証の結果に相互運用性上の問題が無い
×: 不合格:当該テスト項目の生成/検証の結果に相互運用性上の問題がある
－: 実装が当該テスト項目の生成/検証の機能を提供していない
製品: 有償、無償を問わず2008年までに製品などの形で提供予定の実装
試作品: 社内の試作目的で開発された実装、又は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: 文書管理システムまたはその一部となるサーバーシステムとして提供

CAdES 共通データ検証機能標準準拠性テストの各テストケースにおけるテスト結果は以下の通りであった。

表 3.3　CAdES 共通データ検証機能標準準拠性テスト集計結果

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	ピーバークテクノロジー	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	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
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

XAdES 共通データ検証機能標準準拠性テストの各テストケースにおけるテスト結果は以下の通りであった。

表 3.4　XAdES 共通データ検証機能標準準拠性テスト集計結果

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	ラングエッジ	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

以上、署名生成・検証相互運用性テストと共通データ検証機能標準準拠性テストを集計した結果、参加者実装の合否判定結果は以下となった。

表 3.5　CAdES 総合合否判定結果

CAdESテスト総合合否判定結果 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		ビーバーク 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	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ー	○1
CAdES-Tのオプション機能の提供	ー	ー	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ー	ー	ー	○	○	○	○	○	○	○	ー	ー
CAdES-Aの基本機能の提供	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	ー	○1
CAdES-Aのオプション機能の提供	ー	ー	○	○	ー	ー	ー	ー	○	○	ー	ー	ー	ー	ー	ー	ー	ー	ー	○	ー	○	ー	ー	ー	ー	ー	ー

表 3.6　XAdES 総合合否判定結果

XAdESテスト総合合否判定結果 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		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	○	○	○	○	-	-	○	○	○	○	-	-	○	○	-	-

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
ー 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

基本機能に合格していれば、その実装は CAdES/XAdES 署名の生成または検証において JIS 原案の CAdES/XAdES プロファイルの要件を満たしていると言え、参加した全ての実装がテストに合格した。

個々のテスト項目に関する結果詳細や実装間でのテスト結果、参加者に提出を依頼した JIS プロファイルの供給者適合性宣言書の集計結果はウェブサイト[8]で公開予定の別紙で示す。

4 国際実験の状況

ECOM では、ウェブサイトから問い合わせのあった CAdES / XAdES の実装を有する海外企業 2 社と日本国内有志企業 7 社で実証実験を実施中である。テスト内容は署名生成・検証相互運用性テストのみとし、2007 年 11 月から 2 月末までの期間で行う。テスト結果については実験終了後、別紙としてウェブサイト[8]上で公開する予定である。

また、昨年度より ECOM では ETSI TC ESI にて CAdES / XAdES プラグテストを実施するよう働きかけを行なってきた。2007 年 1 月から 3 月にかけて準備として ETSI 側よりスペインのカタルーニャ工科大、オーストリアの A-SIT、日本電気、エントラストジャパンの 4 組織で XAdES に関する事前実験を行った。ECOM 側よりコストや時間などの面から欧州に集まって行わずテストはリモートでもできることを主張し、事前実験は電話会議、メールなどを活用しリモートで行われた。そしてようやく、2008 年 3 月 3 日から 7 日の期間 ETSI の主催で XAdES REMOTE Interoperability Plugtest[9]が実施される運びとなった。2 月 15 日現在、企業、大学、政府機関を含む欧州 25 組織、日本 1 組織が参加する予定である。ECOM からは、継続的に CAdES と XAdES のテストの両方の共催を呼びかけてきたが XAdES のみしか実現に至らなかったことは残念に思う。

5 考察と課題

本節では、実証実験により得られた知見、相互運用上の課題、テスト内容に関する課題について述べる。

5.1 実験結果に見る日本国内の実装の傾向

生成・検証相互運用テストでは、JIS 原案の要件に含まれるかどうかにかかわらず、実装がどのような機能を持っているのかを客観的に知ることができるよう配慮した。集計された結果により、日本国内における CAdES / XAdES の実装の傾向が伺える。

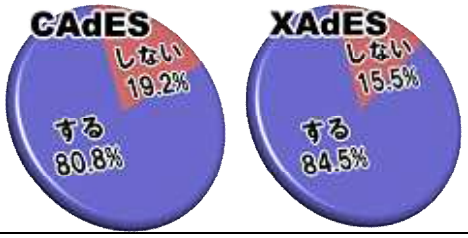
表 5.1　CAdES/XAdES 国内実装の傾向

参加した実装の内訳

国内実験に参加した実装の比率としては、CAdES がやや多く、開発ツールキットに基づく実装が多かった。また、製品としての参加が半数を超えている。

JIS の任意選択の要素をサポートするか

任意選択とは JIS 原案の標準のみでオプションとして利用することが可能な属性もしくはプロパティであり、JIS に準拠する生成者の実装が追加の規定抜きで使用することができる。これに対し、80%以上の実装が生成・検証をサポートしていることがわかった。

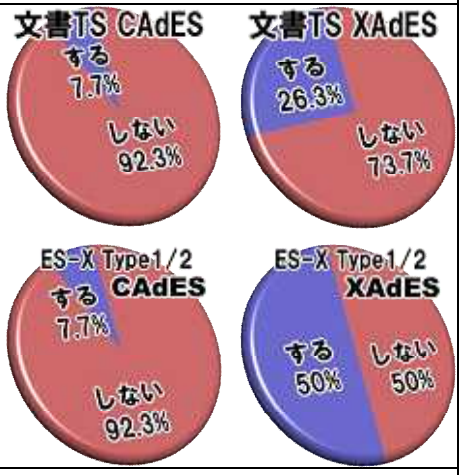


JIS の要別途規定の要素をサポートするか

要別途規定とは ETSI の標準では要素が規定されているものの、利用方法、検証方法に詳しい言及が無いため追加の規定なしには利用してはならない属性もしくはプロパティである。XAdES の 5 割に対し、CAdES では実装している比率が極端に少ない。CAdES では JIS に準拠するための最低限の実装を行うケースが多いようだ。ASN.1 構造と XML との比較で、XAdES の方が要素の追加に柔軟に対応しやすいのかもしれない。

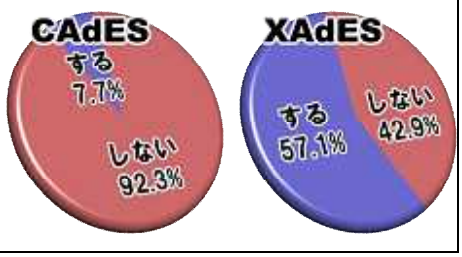
要別途規定のタイムスタンプをサポートするか

JIS で要別途規定となっている署名前に署名対象文書に対し直接付与する ContentTimeStamp, AllDataObjectsTimeStamp などのタイムスタンプの属性およびプロパティのサポート率は予想通り、かなり低いものであった。また、署名や検証参照情報にタイムスタンプを付与する ES-X Type 1 および Type2 の CAdES-C TimeStamp や SigAndRefsTimeStamp 属性およびプロパティについては、CAdES では 1 社しかサポートしていないが、XAdES では半数の実装がサポートしていた。



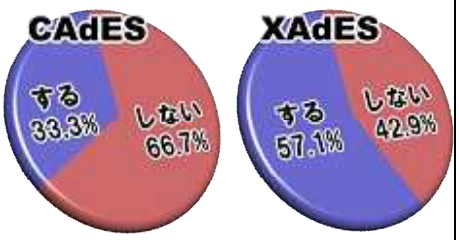
署名ポリシをサポートするか

他の要別途規定の比率と同程度のサポート状況で、日本国内で署名ポリシを利用するには、ハードルが高いことが伺える。数値的には XAdES では使いやすいように勘違いされるかもしれないが、XML 署名ポリシは ETSI 技術標準ではなく技術報告に留まり、スキーマ定義の誤りがあるまま、改訂がされていないなど利用上の障壁はある。



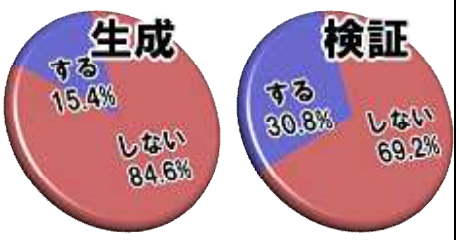
カウンタ署名をサポートするか

CAdES の場合、元の標準である CMS で提供する機能で、JIS では任意選択になっているものの対応する実装は 3 割に留まった。また、XAdES においては XML 署名が持つ任意の対象に対し明示的に署名できる機能により XAdES の CounterSignature プロパティを使用しなくてもカウンタ署名は実現できるが 6 割近くが実装している。



RFC 3126 CAdES ArchiveTimeStampV1 をサポートするか

RFC 3126 が公開されて 7 年であるが、既に V1 形式を検証できる実装は 30%程度である。数 10 年といったスパンで電子文書を保存することを考えると、少なくとも検証についてだけでも過去のバージョンのフォーマットを検証する機能を提供し続けることは重要であり、将来の継続的なフォーマットサポートが危惧される。XAdES についても同様にバージョン間の非互換性の問題を抱えている。



どこに署名生成者は TSA 証明書検証情報を格納するか

特にアーカイブタイムスタンプを付与する場合、タイムスタンプの検証情報をどのように保管するかは重要な問題である。長期署名フォーマットでは署名データ単体で検証が可能な事から、タイムスタンプトークンに含めておいた方が管理しやすい。参加企業の実装はその 100%がトークンに格納する方法をサポートしており、CAdES ではトークンの CertificateValues など非署名属性に格納する方法、XAdES ではトークンの CMS 構造の certificates フィールドに格納する実装の方が多い。XAdES で署名者証明書検証情報の格納領域に TSA 証明書の検証情報を格納する実装もあった。一方、検証については、どこに格納されていても 100%の実装が正しく検証することができた。

5.2 CAdES / XAdES 実装の陥りやすい相互運用性上の誤り

今回 2007 年の実験は前回 2005 年の実験[5]に続いて二度目の実験であり 44%が前回も参加していたり、過去のテストデータをウェブサイト上で公開したりしているため、2007 年の実験では大きな相互運用性上の問題は起きなかった。細かな障害は発生したものの、多くの参加者が実験期間中に修正版を実装し問題解決している。

そこで本節では、実験期間中に起きた実装の誤りによる障害事例を述べる。実装上陥りやすい誤りを示すことにより、今後新規に参入する組織が長期署名フォーマットの実装をする際の参考に資すれば幸いである。

- CAdES で起きやすい誤り
  - アーカイブハッシュ対象が BER であることを想定していないためのハッシュ不一致
    アーカイブタイムスタンプのハッシュ対象である CMS SignedData の eContent、certificates、crls および SignerInfo 中の unsignedAttrs が ASN.1 DER でなく BER を利用可能であることを想定していないためにハッシュ値の不整合を起こしているケースがあった。BER は不定長の OCTET STRING 表現ができ、SET OF 構造をソートしないという特徴があるため、BER、DER の違いに注意する必要がある。
  - signedAttrs の要素がソートされていない
    RFC 3852 で規定されているように CMS SignedData では signedAttrs が ASN.1 DER でエンコードされるため、属性要素を格納する SET OF 構造はソートされなければならない。
  - CompleteRevocationRefs の要素の対応関係の誤り
    CompleteRevocationRefs の要素は CompleteCertificateRefs の要素と対応関係があるように格納しなければならないが、一つの要素の複数の CRL 参照情報を格納しているケースがあった。
  - CompleteCertificateRefs の OtherCertID の issuerSerial の不足
    OtherSigningCertificate 属性を定めた ASN.1 シンタックスの中で、OtherCertID の issuerSerial はオプションとなっているが、CompleteCertificateRefs の中で使用する場合には必須なので注意が必要である。

- XAdES で起きやすい誤り
  - XMLDSIG の Id 属性の重複、不足、入れてはならない場所での使用
    Id 属性は XML ドキュメント中で要素を一意に特定するためのものであり、既存の XML ドキュメントを追加や内包するような場合属性値が重複しないようにしなければならない。また、XAdES においてはスキーマの定義上、要素によって Id 属性が必須であったり、入れてはならない要素があったりするので注意しなければならない。
  - SignedProperties を参照する Reference の Type 属性の値の誤り
    この Type 属性の値は""のように決まっているがそうでないケースがあった。
  - Reference に XPath が使われていると対応できない
    これは誤りではないが、Reference に XPath もしくは XPointer の表現が使われていると対応できない実装がある。可能であれば Id により参照した方が相互運用性は高い。

- CAdES / XAdES に共通の起きやすい誤り
  - TimeStampToken がミリ秒以下の分解能を持つ場合正しくデコードできない
    日本国内の時刻認証事業者はミリ秒の精度でタイムスタンプを発行している事業者が多いが、ミリ秒以下の精度で発行する事業者もある。ミリ秒以下の GeneralizedTime を想定していないために、時刻の比較でエラーとなる実装があった。
  - 検証したい時刻よりも古い CRL、OCSP が格納されているケース

- **検証情報、検証参照情報の不足**
  署名生成時に検証に必要な証明書、CRL、およびこれらの参照情報が不足しているために検証に失敗するケースがあった。
- **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**
  これは誤りではないが、タイムスタンプトークンの TSA 証明書を検証する際に、検証情報はファイルで提供されたりトークンに格納されたりしているが、検証側の実装が、ある格納方法に対応していないために検証に失敗するケースがある。
- **失効情報の猶予期間**
  失効情報を利用する際に猶予期間を厳密に見る実装と、そうでない実装があるので、注意が必要である。
- **SigningTime と TimeStamp 属性の順序関係の不整合**
  CAdES および XAdES の仕様ではコンテントに対するタイムスタンプ、SigningTime および署名タイムスタンプの順序関係が規定されている。この順序に従わないデータを生成しているために検証エラーとなるケースがある。

5.3 タイムスタンプトークンに関する相互運用性上の課題

CAdES および XAdES は、タイムスタンプを用いた署名フォーマットであり、タイムスタンプ局より取得したタイムスタンプトークンを定められた位置に格納するといった処理を行う。今回の実証実験では、日本国内の認定制度による時刻認証認定事業者３社に協力を仰ぎ、テスト用に準備された、ほぼ実サービスと同じプロファイルのタイムスタンプ局を使用した。一部の実装において、以下の問題が発生した。

- **時刻監査証の格納場所に関する問題**
  時刻認証局(TSA)の機器と時刻配信局(TA)の時刻差を監査した結果を X.509 V2 属性証明書の形式で発行する製品があり、国内の事業者でもタイムスタンプトークンにこの時刻監査証(TAC)を含める実装がある。TAC は V2 属性証明書であるが、タイムスタンプトークンの V1 属性証明書の格納領域に入れているため読み込みエラーになるなどの障害が起きるケースがあった。

- **時刻監査証の整数型フィールドにおける ASN.1 エンコーディングの問題**
  ある事業者のタイムスタンプトークンには、TA より発行された ASN.1 INTEGER のエンコーディングに誤りのある TAC が含まれており、そのため読み込み時にエラーになる実装があった。

- **トークンの PKCS#1 署名値のパディングの問題**
  実サービスと同じテスト用タイムスタンプ局で利用するタイムスタンプを発行する製品にお

いて、PKCS#1 署名に厳密に従っていないものがあり仕様に基づき厳密に検証した場合、タイムスタンプトークンの署名値が一致しないというケースがあった。PKCS#1 のパディング中のダイジェストアルゴリズムのパラメーターを含めるか、含めないかという問題であり、詳細は ECOM の昨年度の報告書(文献[12] 200p)でも述べている。Java などで提供される署名 API では、検証においては相互運用性もしくは後方互換性のためパラメーターの有無に関わらず検証成功としているようだ。ちなみにタイムスタンプサーバーの製品ベンダーからは 2006 年 9 月にこの問題に対する修正[13]が出ている。

署名の生成、延長、検証における相互運用性確保のためには、実装者側は処理の過程で、タイムスタンプトークンの ASN.1 エンコーディングを変更しないことが求められる。また、TA 並びに TSA においては標準に準拠しない箇所の修正が必要となる。TAC は属性証明書であるから一般には検証は不可欠である。その意味内容、提供手段、署名検証者による検証の必要性、検証する側の検証要件について明らかにすると共に長期保存の対象とすべきか、どのように保存する必要があるかについて議論の必要がある。

5.4 CAdES / XAdES における SigningTime の時刻比較

CAdES および XAdES においては SigningTime とタイムスタンプ要素との時刻の比較の検証要件(文献[1] C.3.6 および [2] G.2.2.16)が定められており、コンテンツに対するタイムスタンプ、SigningTime、署名タイムスタンプの順序でなければならないとしている。時刻が全て厳密に正確ならば論理的にこのような順序であることが保証されるが、SigningTime は署名を付与する機器のローカル時刻に基づく時刻であるため調時が正確でなかったりすると、往々にして時刻の順序関係が前述の検証要件を満たさないこととなる。

SigningTime は CMS 署名や S/MIME 署名メールにおいて一般的な属性であり、頻繁に使われるが、署名デバイスは必ずしもオンラインの環境で NTP 等により調時できるとは限らないため順序関係の要件を満足するのは非常に難しい。そこで、ETSI TC ESI 会議や IETF S/MIME ワーキングループの議論の場で、SigningTime の比較の要件を緩和することを ECOM より提言し、2008 年上旬には公開される RFC 3126 の後継となる CAdES の RFC では「前後関係は問わず、ある事前に取り決められた範囲内であることを確認する」というような表現に変更された。同様に、2008 年に改定される ETSI TS 101 733 v1.7.4 でも同様に反映される。XAdES においても同様の改定がなされるよう ECOM より提言を継続する。

5.5 CAdES / XAdES に関連するセキュリティ勧告

CAdES 署名に直接関連するセキュリティ勧告としては、現状把握している限りにおいて、OpenSSL や Microsoft CryptoAPI に関する脆弱性報告のみであり、報告から数年が経過していることから概ねの実装が対策を施していると思われる。

一方、XAdES においては、2007 年 6 月に XML 署名に関してセキュリティ勧告[14]があった。XML 署名では Reference 要素や KeyInfo の RetrievalMethod 要素の中に Transform 要素を含むことができ、この中では XML スタイルシートを記述することができる。過去の Apache Xalan に基づく XSLT の実装では、extension を有効にしていた場合スタイルシートの中で任意の Java クラスのメソッドを実行ができるようになっていたため、攻撃者がコマンド実行や DoS 攻撃を受ける可能性がある。署名検証よりも前にこれらの処理が行われることが多いため、送信者が不特定であったり、中間者が XML メッセージの改竄ができたりするような環境では確認が必要である。Microsoft 系の実装でも独自の拡張によりスクリプト(msxsl:script)を実行やコマンドが実行できる可能性があるので、調査ならびに確認が必要である。

5.6 将来に向けた標準仕様の改定案

実証実験を踏まえ、サービス側、実装側で対処するのではなく、CAdES、XAdES のみならず CMS、XMLDSIG などの標準仕様そのものを変更が望まれる箇所があった。これを今後の課題としてまとめる。

- ETSI TS 101 733 XAdES
  - ♦ 名前空間にバージョンが含まれている問題
    XAdES の規定する XML 要素は XML の名前空間を持っているが、これは "http://uri.etsi.org/01903/v1.3.2#"のようにバージョン番号を含んだ表現となっている。XAdES は 2～3 年毎に改定されているが、その度に名前空間が変っている。XAdES の実装では名前空間が変わると、基本的には実装を分ける必要があり、今回の実験参加した実装も、そのほとんどが最新版の v1.3.2 のみにしか対応しない実装がほとんどであり、前回実験のバージョンをサポートするものは無かった。この事は、XML 署名文書を長期保存する上で重大な問題である。10 年後、20 年後、過去のバージョンの XAdES を検証できない可能性が非常に高いのである。バージョンの差異によって生成、検証のアルゴリズムが変わる場合に名前空間を分けることは重要だが、XAdES のバージョンの違いで個々の要素の処理内容には変更が無いようなバージョン更新が多い。今後は、名前空間のバージョンを変更しないか、含めずに、要素の構造や処理内容に変更があった場合には、別の名前の要素として(例 SigningTime, SigningTimeV2)仕様追加し、将来的に後方互換性をある程度保証できるような仕様にしなければならないと考える。

  - ♦ タイムスタンプトークンの検証情報格納領域の追加
    タイムスタンプトークンを検証するのに必要な証明書や失効情報は長期署名フォーマッ

トの中に含めてアーカイビングした方が、署名データ単体で検証できるため望ましい。しかしながら、CAdES/XAdES ではトークンの検証情報の格納の属性やプロパティを持たないため、現在では仕方なくトークンの CMS SignedData 構造の中に格納している。トークン自体が証拠情報であるため、意図しない改ざんを防止する意味でも本来なら手を加えずそのまま格納しておくことが望ましい。そのためにも、タイムスタンプトークンの検証情報を格納する領域に関する規定を追加することが望ましい。XAdES の実装者は、この問題がなければタイムスタンプ以外で CMS SignedData を細かく扱う必要が無いので、特に XAdES においてトークン検証情報の格納用のプロパティの追加が強く求められる。

- ETSI TS 101 733 CAdES
  - ♦ ArchiveTimeStamp の計算方法に関する注釈の曖昧性
    CAdES の ArchiveTimeStamp のハッシュ対象となる非署名属性群の ASN.1 エンコーディングについて ETSI TS 101 733 v1.7.3 では以下のような記述がある。

> 6.4.1 Archive time-stamp attribute definition
> NOTE 5: Whilst it is recommended that unsigned attributes are DER encoded it cannot generally be so guaranteed except by prior arrangement.
> (訳) 非署名属性は DER でエンコードされることが推奨されるが、事前の調整がある場合を除いて、一般にそのようには保証できない。
> -- 出典：ETSI TS 101 733 v1.7.3

    CAdES の元となっている CMS SignedData の仕様では、CMS 自体は DER ではなく BER エンコーディングであり、非署名属性群もまた属性要素がソートされない BER エンコーディングでよい。この注釈自体、仕様の不整合を生じてまで誰が DER を推奨しているのか明らかではないし、本来正しいはずの BER が、例外であるような印象を受ける。実験参加者の中にも非署名属性群が DER であることを想定した実装があり相互運用性に問題があった。eContent, certificates, crls など他のハッシュ対象も BER エンコーディングでよいことから、非署名属性群についてのみこのような制限を加えるのは適切でない。この注釈を修正し、非署名属性が BER であることを踏まえた実装を行う必要があることを明記する必要がある。

  - ♦ タイムスタンプトークンの検証情報の格納用属性の追加
    CAdES についても XAdES と同様にトークンの検証情報の格納用の属性が望まれる。

- IETF RFC 3852 CMS
  - ♦ OCSP 応答を格納するための OID の規定
    CMS SignedData の RevocationInfoChoices では、CRL やその他の任意の形式の

失効情報を格納することができる。OCSP 応答を格納したい場合、その他の形式を利用するわけだが、現状 RFC では OCSP 応答の形式であるということを特定するためのオブジェクト識別子(OID)の規定が無い。例えば、タイムスタンプの検証情報が OCSP のみでしか提供されない場合に備え、早期にこの OID の規定を追加する必要がある。

- W3C XMLDSIG
  - ♦ **名前空間にバージョン(年月)が含まれている問題**
    前述の名前空間による後方互換性の問題は、XAdES だけでなく、XML 署名(XMLDSIG)についても同じ問題である。XMLDSIG の現行バージョンは "http://www.w3.org/2000/09/xmldsig#"のような名前空間となっている。将来にわたって現行の XMLDSIG の名前空間に対応した実装が存在し続けられるか懸念される。何らかの対策、方針が必要であると考える。

以上の点は、ETSI TC ESI、IETF S/MIME WG、W3C を通じて今後、継続的に提言を続けていく必要がある。

5.7 CAdES / XAdES 実証実験内容に関する今後の課題

今回の実証実験を踏まえた残課題をまとめる。

- **共通データ検証機能標準準拠性テストのテストケースの充実**
  テストデータの準備期間が十分でなかったことから 2005 年に実施したテストと比較してテスト項目数ベースで 25%程度減っている。また、CAdES と比較して XAdES の方が、よりテストケースが少ない。今回実施した生成･検証相互運用性テストで利用したツールを用いて相互運用性テストのテスト項目程度にテスト内容を充実させることが望まれる。OCSP に関するテストなども必要である。
- XAdES 共通データ検証機能標準準拠性テストのテストケース
  近年、SHA1 ハッシュアルゴリズムの危殆化が危惧されているが、XML 署名においては CMS と比較してアルゴリズムの移行が遅れており、対応する実装が少ないようである。一つにアルゴリズム URI の登録機関が明確でない点もあるかと思う。長期保存の観点から SHA2 を用いた署名のテストは急務であると考える。また、Enveloped 署名、署名ポリシなどのテストも必要となるだろう。
- **後方互換性を確認するテスト**
  CAdES、XAdES の長期署名フォーマットの実装が現れてほんの数年であるが、CAdES

では ArchiveTimeStamp V1 と V2 があったり、XAdES では仕様のバージョン毎に名前空間が異なるなど後方互換性の問題が懸念される。今回の実証実験では、現時点で最新の仕様のみに準拠し、過去の版をサポートしない実装が多かったようだ。少なくとも署名検証だけでも過去の版のテストケースを提供しておく必要がある。

6 謝辞

本実証実験を実施するにあたり快く無償でテスト用 TSA を提供して頂いたアマノタイムビジネス株式会社様、セイコープレシジョン株式会社様、株式会社 PFU 様、また、時刻監査証(TAC)に関し情報提供頂いたセイコーインスツル様に心より感謝の意を表します。

7 参考文献

[1] ETSI TS 101 733 V1.7.3 (2007-01) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES), Jan 2007, ETSI

[2] ETSI TS 101 903 V1.3.2 (2006-03) XML Advanced Electronic Signatures (XAdES), Mar 2006, ETSI

[3]CMS 長期署名プロファイル, 2005 年 8 月, 次世代電子商取引推進協議会(ECOM), http://www.ecom.jp/report/electronic_signatures/CMSformat.pdf

[4]XAdES 長期署名プロファイル, 2005 年 8 月, 次世代電子商取引推進協議会(ECOM), http://www.ecom.jp/report/electronic_signatures/XAdESLong-TermSignatureFormatProfile_V0.6pub_.pdf

[5]長期署名フォーマット相互運用性実験報告書,平成 18 年 3 月,電子商取引推進協議会 セキュリティワーキンググループ

[6] 暗号メッセージ構文を利用した電子署名(CAdES)の長期署名プロファイルに関する要求事項 JIS 原案, 2006 年 12 月, 次世代電子商取引推進協議会(ECOM), http://www.ecom.jp/report/JIS_CAdES_Profile.pdf

[7] 拡張可能なマーク付け言語を利用した電子署名(XAdES)の長期署名プロファイルに関する要求事項 JIS 原案, 2006 年 12 月, 次世代電子商取引推進協議会(ECOM), http://www.ecom.jp/report/JIS_XAdES_Profile.pdf

[8] ECOM CAdES / XAdES Plugtest 2007 ウェブサイト, 2007 年 10 月, 次世代電子商取引推進協議会(ECOM), http://www.ecom.jp/LongTermStorage/interoptest2007.html

[9] Plugtest Portal for Electonic Signature 3 - 7 March 2008, 2007 年 11 月, ETSI, http://www.etsi.org/plugtests/XAdES/XAdES.htm

[10] 日本工業規格(JIS) JIS X 5092:2008 CMS 利用電子署名(CAdES)の長期署名プロファイル, 2008 年, 日本規格協会

[11] 日本工業規格(JIS) JIS X 5093:2008 XML 署名利用電子署名(XAdES)の長期署名プロファイル, 2008 年, 日本規格協会

[12] 電子文書長期保存ハンドブック, 平成 19 年 3 月, 電子商取引推進協議会 セキュリティワーキンググループ, http://www.ecom.jp/results/results18.html

[13] nCipher DSE 200 Release Notes, 2006 年 9 月, nCipher PLC, http://active.ncipher.com/documentation/nCDSE/win/user/dse_rnot.txt

[14] XML Digital Signature Command Injection, iSEC Partners Security Advisory - 12 Jul 2007, 2007 年 6 月, iSEC Partners, Inc., http://www.isecpartners.com/advisories/2007-04-dsig.txt

8 変更履歴

日付	変更内容
2008.02.25	ウェブ公開用初版 (漆嶌)
2008.02.22	・メンバー一覧、実施体制図を追加
2008.02.18	電子署名普及ワーキンググループ報告書版 (漆嶌)