長期署名フォーマット
ECOM 相互運用実証実験
CAdES テストケース設計書

2007 年 10 月 11 日

V1.2

次世代電子商取引推進協議会(ECOM)
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

図表番号

更新履歴

バージョン	日付	変更内容
V0.9	2006.3.9	ECOM プロファイルに基づく実証実験
V1.0	2007.3.5	JIS 原案に基づいたテストケースを追加 ・ 追加テスト項目番号(20012 - 20019, 70003 - 70010) ・ テストケース追加(OFF-T-OP-11～OFF-T-OP-13, OFF-A-3～OFF-A-6) ・ TSTInfo のプロファイルに追記
V1.2draft	2007.9.28	2007 年署名データ生成・検証相互運用性テスト(旧オンラインテスト)を再設計、追記 ドラフト版を実験参加者に公開しレビュー依頼
	2007.10.2	オンラインテストについて以下を追加 ・ テスト実施手順の詳細（ファイル名のガイドラインも含む） ・ 合否判定基準 今回は使用しないため ETSI TS 101 733 v1.5.1 の ECOM テスト用に定めた ArchiveTS 計算法の記述を削除
	2007.10.5	オンラインテストの「目視確認」について追記 オンラインテストに ArchiveTimeStampV1 を追加 オンラインテスト用署名ポリシのプロファイルの追加 オンラインテストの 2005 年資料から流用していた部分(署名対象、生成、検証)を削除 誤植の修正
	2007.10.9	オンラインテストの属性の追加について共通要件で補足
	2007.10.11	3.2.2 署名生成の入力ファイルについて追記
V1.2	2007.10.11	V1.2 リリース

1 はじめに

本書では、長期署名フォーマットおよび JIS 原案への準拠性を確認するためのテストの内容を示したテストケース設計書である。

1.1 本書における表記

本仕様書では以下の表記を用いることとする。

表記	説明
<…>	テスト項目
<…-OK>	検証結果の期待値が有効のテスト項目
<…-NG>	検証結果の期待値が無効のテスト項目
<… 00000>	テスト項目名の末尾の 5 桁の数字はテスト項目番号
[…]	参考文献

1.2 テストの構成

・テストカテゴリ（今回のテストではオフラインテストカテゴリとオンラインテストカテゴリに大別される）

・テストケース（個々のテストケースであり機能評価判定の単位となる。複数のテスト項目を含む）

・テスト項目（テストの最小単位であり、検証の結果として期待値通りかそうでないかを成功・失敗として表現する。）

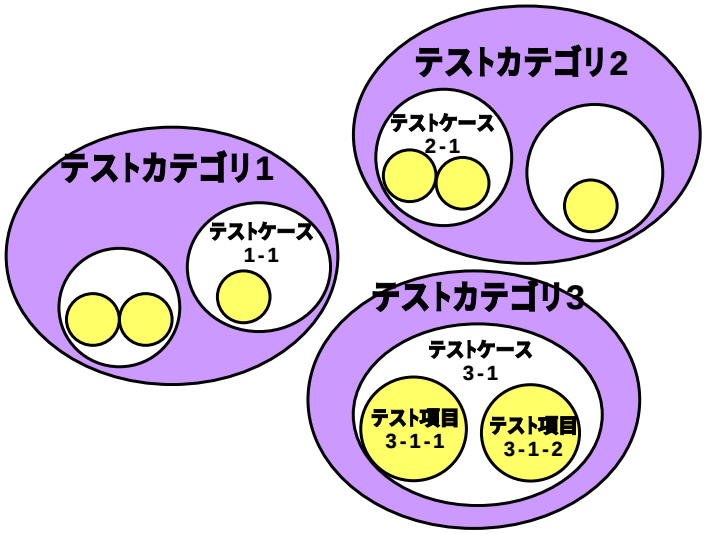

図 1-1 テストの構成

2 オフライン 共通データ検証テストカテゴリ

長期署名フォーマット及びJIS原案に基づく共通のESフォーマットデータを用いて正しく検証することができるかを確認する。テストツールにより生成されたCAdES フォーマットのデータ(CAdES-BES, CAdES-EPES, CAdES-T, CAdES-C, CAdES-X long, CAdES-A)、証明書、CRL、署名対象データをもとに、検証結果が期待値と一致するかどうかを確認する。

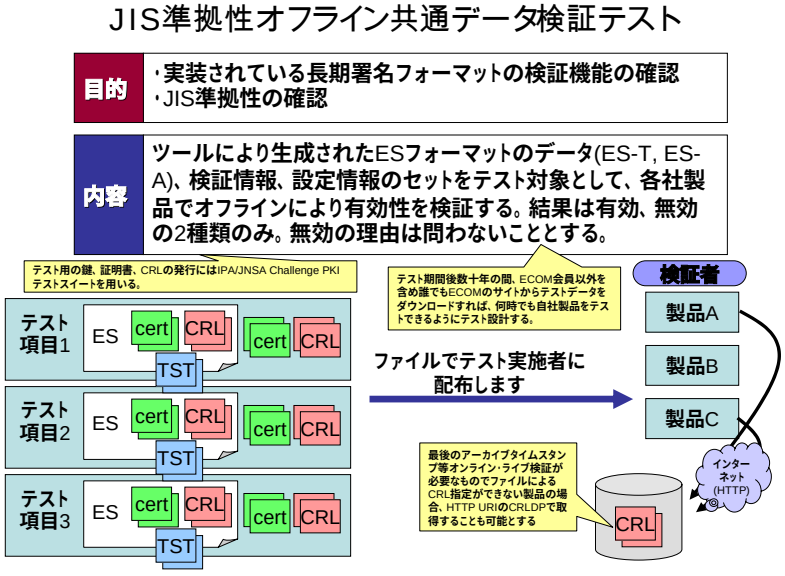

図 2-1 オフライン検証テスト

2.1 テストの準備

- **CRL のための設定**

オンラインで CRL を取得する場合には、検証環境におけるインターネット接続環境の準備。実験期間終了後にはホスト名を同じくする HTTP リポジトリの立ち上げと設定。もしくは、ファイルによる CRL の設定。

- **トラストアンカの設定**

テストスイートで配布されるオフラインテスト用の署名者用ルート証明書、TSA 用ルート証明書をトラストアンカとして設定する。

2.2 テストの実施

- **署名対象データの設定**

内包署名の場合にはファイル'TARGET_AAA.txt'(ファイルの内容は"aaa"という 3 文字 3 バイトの文字列のみ)、分離署名の場合には'TARGET_BBB.bin'(ファイルの内容は 0x01-0x09,0x00 の繰り返し 1024000 バイトのバイナリファイル)を設定する。

- **検証時刻の設定**

検証時刻はフォーマット毎に異なる。フォーマットに応じ検証時刻の設定を行う。検証可能な現在時刻の範囲は UTC2002 年 1 月 1 日 0 時 0 分 0 秒より UTC2035 年 12 月 31 日 23 時 59 分 59 秒までとし、各証明書、CRL もまたこれが可能なように設定されている。

- **検証対象の長期署名フォーマットデータの設定**

テストスイートにおいて長期署名フォーマットの検証対象テストデータは'data.der'というファイル名となっており、テスト項目毎に別々のディレクトリに保存されている。

- **検証の実施**

これを実施すべき全てのテスト項目について実施する。

署名対象データの SHA1 ハッシュ値は以下の通り。

- TARGET_AAA.txt
  SHA-1: 7e240de74fb1ed08fa08d38063f6a6a91462a815
- TARGET_BBB.bin
  SHA-1: 82918e6b4c2ba314491b2797c3bb4715bae0b713

2.3 テストデータに共通の情報

- **有効期限の時刻は例外ケースを除き** 00:00:00 **から** 23:59:59 **に統一**
- **署名時刻、タイムスタンプ時刻は例外ケースを除き** 12:00:00 **に統一**
- **時刻の表記は特に断りの無い限り、**UTC **時刻であるとする。**

2.4 オフライン検証テストのテスト項目の概要

オフライン検証テストのテストケースは以下の内容を含んでいる。

- ES-T, ES-C, ES-X Long, ES-A **フォーマットの検証**
- **内包署名と分離署名**
- **ハッシュアルゴリズム** (SHA-1, SHA-256, SHA-512)
- BES **と** EPES
- RFC3126**、**ETSI TS 101733 v1.5.1/v1.6.3**、**v1.7.3 **のアーカイブハッシュ**
- SigningTime, SignatureTimeStamp **時刻による失効、期限切れ検証**
- **各種ハッシュ値の改竄の検証**

- **コンテンツタイムスタンプ**
- **並列署名(=独立署名)**
- **カウンタ署名**
- **署名ポリシファイルを考慮した検証**
- ESS SigningCertificateV2

全 30 テスト項目のリストを以下に示す。

番号	テスト項目名	期待値
10001	EST-ATTACH-NORMAL-OK	有効
BES 内包署名による ES-T フォーマットのデータが有効となることを検証する。		
10002	EST-ATTACH-EXPIRED-NG	無効
ES-T フォーマットで署名者証明書が期限切れの場合、無効となることを検証する。		
10003	EST-ATTACH-REVOKED-NG	無効
期限切れではないが署名タイムスタンプの genTime の値よりも前に署名者証明書が失効している場合に ES-T データが無効であることを検証する。		
10004	EST-ATTACH-SIGTIME-REVOKED-OK	有効
SigingTime 属性の値の時点では失効しているが、署名タイムスタンプの時点では失効していない場合に、SigningTime 属性の値に関わらず ES-T データが有効であることを検証する。		
10005	EST-ATTACH-SIGTS-REVOKED-NG	無効
SigningTime 属性の値の時点では失効してないが、署名タイムスタンプの時点で失効している場合に、署名タイムスタンプを考慮して ES-T データが無効であることを検証する。		
10006	EST-ATTACH-ES-SIG-FORGED-NG	無効
signerInfo の signature フィールドが改竄されている場合に ES-T データが無効であることを検証する。		
10007	EST-ATTACH-ES-SIGTS-SIG-FORGED-NG	無効
署名タイムスタンプのタイムスタンプトークンの signature フィールドが改竄されている場合に、ES-T データが無効であることを検証する。		
10008	EST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG	無効
signedAttrs フィールド中の MessageDigest CMS 属性の値が改竄されている場合に、ES-T データが無効であることを検証する。		
10009	EST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG	無効
署名タイムスタンプのタイムスタンプトークンの MessageDigest CMS 属性が改竄されている場合に、ES-T データが無効であることを検証する。		
10010	EST-DETACH-NORMAL-OK	有効
BES 分離署名による ES-T フォーマットのデータが有効であることを検証する。		
20001	EST-OTHERCERT-SHA256-OK	有効
SHA-256 アルゴリズムによる OtherSigningCertificate CMS 属性がある場合に、ES-T フォーマットのデータが有効であることを検証する。		
20002	EST-SIGTS-SHA256-OK	有効
TSTInfo の MessageImprint および SignerInfo の DigestAlgorithm フィールドが SHA-256 アルゴリズムであり、signatureAlgorithm が SHA256withRSA であるようなタイムスタンプトークンの署名タイムスタンプである場合に、ES-T フォーマットデータが有効であることを検証する。		
20003	EST-SIGTS-SHA512-OK	有効
TSTInfo の MessageImprint および SignerInfo の DigestAlgorithm フィールドが SHA-512 アルゴリズムであり、signatureAlgorithm が SHA512withRSA であるようなタイムスタンプトークンの署名タイムスタンプである場合に、ES-T フォーマットデータが有効であることを検証する。		
20004	EST-CONTENT-TIMESTAMP-OK	有効

signedAttributes フィールドに ContentTimeStamp CMS 属性がある場合に、ES-T フォーマットデータが有効であることを検証する。		
20005	EST-INDEPENDENT-SIGNATURES-OK	有効
2 つの signerInfo を持つような並列署名(独立署名)である ES-T フォーマットデータが有効であることを検証する。		
20006	EST-EPES-WITHOUT-HASHCHECK-OK	有効
signaturePolicyIdentifier の CMS 属性があるような EPES に基づく ES-T フォーマットデータが有効であることを検証する。		
20007	EST-EPES-NORMAL-OK	有効
SignaturePolicyIdentifier CMS 属性がある EPES に基づく ES-T フォーマットデータにおいて、署名ポリシファイルを参照しながら有効であることを検証する。		
20008	EST-EPES-POLICY-HASH-NOT-MATCH-NG	無効
SignaturePolicyIdentifier CMS 属性のハッシュ値が署名ポリシと一致しない場合に ES-T フォーマットが無効であることを検証する。		
20009	EST-EPES-NOT-BEFORE-VIOLATION-NG	無効
署名ポリシファイルの signingPeriod の notBefore フィールドの時刻が遠い将来であり、まだ有効期間内に無い場合、署名ポリシが無効であるために ES-T フォーマットが現時点で無効であることを検証する。		
20010	EST-EPES-MANDATED-SIGNEDATTRS-VIOLATION-NG	無効
署名ポリシファイルの mandatedSignedAttr フィールドで必須とされている SigningTime 属性が無い場合に、ES-T フォーマットデータが無効であることを検証する。		
20011	EST-EPES-EXTERNAL-SIGNEDDATA-VIOLATION-NG	無効
署名ポリシファイルにおいて externalSignedData が TRUE、即ち分離署名を要求しているにも関らず、内包署名である場合に、ES-T フォーマットデータが無効であることを検証する。		
20012	EST-ESSCERTV2-SHA256-OK	有効
SHA-256 アルゴリズムによる ESSSigningCertificateV2 CMS 属性がある場合に、ES-T フォーマットのデータが有効であることを検証する。		
20013	EST-ESSCERTV2-SHA256-FORGED-NG	無効
SHA-256 アルゴリズムによる ESSSigningCertificateV2 CMS 属性のハッシュ値が改竄されている場合に、ES-T データが無効であることを検証する。		
20014	EST-ESSCERTV2-SHA512-OK	有効
SHA-512 アルゴリズムによる ESSSigningCertificateV2 CMS 属性がある場合に、ES-T フォーマットのデータが有効であることを検証する。		
20015	EST-ESSCERTV2-SHA512-FORGED-NG	無効
SHA-512 アルゴリズムによる ESSSigningCertificateV2 CMS 属性のハッシュ値が改竄されている場合に、ES-T データが無効であることを検証する。		
20016	EST-COUNTER-SIGNATURE1-OK	有効
一人の署名タイムスタンプ付きカウンタ署名を付与した ES-T フォーマットデータが有効であることを検証する。		
20017	EST-COUNTER-SIGNATURE1-FORGED-NG	無効
カウンタ署名の signature フィールドが改竄されている場合に、ES-T データが無効であることを検証する。		
20018	EST-COUNTER-SIGNATURE2-OK	有効
二人の署名タイムスタンプ付きカウンタ署名を付与した ES-T フォーマットデータが有効であることを検証する。		
20019	EST-COUNTER-SIGNATURE2-FORGED-NG	無効
二人目のカウンタ署名の signature フィールドが改竄されている場合に、ES-T データが無効であることを検証する。		
40001	ESC-ATTACH-NORMAL-OK	有効
内包署名の BES に基づく ES-C フォーマットデータが有効であることを検証する。		
40002	ESC-DETACH-NORMAL-OK	有効
分離署名の BES に基づく ES-C フォーマットデータが有効であることを検証する。		
50001	ESXL-ATTACH-NORMAL-OK	有効
内包署名の BES に基づく ES-X Long フォーマットデータが有効であることを検証する。		
50002	ESXL-DETACH-NORMAL-OK	有効
分離署名の BES に基づく ES-X Long フォーマットデータが有効であることを検証する		
60001	ESXL-ATTACH-SIGTS-VALIDATIONINFO-NOT-INCLUDED-OK	有効

署名タイムスタンプの TSA 証明書のための懸賞情報がトークンに含まれず、ファイルなどの別の方法で検証情報が提供される場合に、ES-X Long フォーマットのデータが有効であることを検証する。		
70001	ESA1-ATTACH-NORMAL-OK	有効
内包署名による第一世代、即ち 1 つしかアーカイブタイムスタンプ CMS 属性が無い ES-A フォーマットデータが有効であることを検証する。		
70002	ESA1-DETACH-NORMAL-OK	有効
分離署名による第一世代、即ち 1 つしかアーカイブタイムスタンプ CMS 属性が無い ES-A フォーマットデータが有効であることを検証する。		
70003	ESA1-V173-ATTACH-NORMAL-OK	有効
ETSI TS 101 733 v1.7.3 アーカイブタイムスタンプの検証。 内包署名による第一世代、即ち 1 つしかアーカイブタイムスタンプ CMS 属性が無い ES-A フォーマットデータが有効であることを検証する。		
70004	ESA1-V173-DETACH-NORMAL-OK	有効
ETSI TS 101 733 v1.7.3 アーカイブタイムスタンプの検証。 分離署名による第一世代、即ち 1 つしかアーカイブタイムスタンプ CMS 属性が無い ES-A フォーマットデータが有効であることを検証する。		
70005	ESA1-V173-ATTACH-ATS-FORGED-NG	無効
ETSI TS 101 733 v1.7.3 アーカイブタイムスタンプの検証。 内包署名による第一世代 ES-A フォーマットデータでアーカイブタイムスタンプのハッシュ値が一致しない場合に、ES-A データが無効であることを検証する。		
70006	ESA1-V173-DETACH-ATS-FORGED-NG	無効
ETSI TS 101 733 v1.7.3 アーカイブタイムスタンプの検証。 分離署名による第一世代 ES-A フォーマットデータでアーカイブタイムスタンプのハッシュ値が一致しない場合に、ES-A データが無効であることを検証する。		
70007	ESA2-V173-ATTACH-NORMAL-OK	有効
ETSI TS 101 733 v1.7.3 アーカイブタイムスタンプの検証。 内包署名による第二世代、即ち 2 つのアーカイブタイムスタンプ CMS 属性を持つ ES-A フォーマットデータが有効であることを検証する。		
70008	ESA2-V173-DETACH-NORMAL-OK	有効
ETSI TS 101 733 v1.7.3 アーカイブタイムスタンプの検証。 分離署名による第二世代、即ち 2 つのアーカイブタイムスタンプ CMS 属性を持つ ES-A フォーマットデータが有効であることを検証する。		
70009	ESA2-V173-ATTACH-ATS-FORGED-NG	無効
内包署名による第二世代 ES-A フォーマットデータで、二世代目のアーカイブタイムスタンプのハッシュ値が一致しない場合に、ES-A データが無効であることを検証する。		
70010	ESA2-ETSI173-DETACH-ATS-FORGED-NG	無効
分離署名による第二世代 ES-A フォーマットデータで、二世代目のアーカイブタイムスタンプのハッシュ値が一致しない場合に、ES-A データが無効であることを検証する。		
80001	ESA1-ATTACH-ETSI151-OK	有効
ESTI TS 101 733 v1.5.1 以降のアーカイブハッシュ計算方法による内包署名による第一世代の ES-A フォーマットデータが有効であることを検証する。		
80002	ESA1-DETACH-ETSI151-OK	有効
ESTI TS 101 733 v1.5.1 以降のアーカイブハッシュ計算方法による分離署名による第一世代の ES-A フォーマットデータが有効であることを検証する。		

2.5 ES-T フォーマット標準テスト項目

2.5.1 <EST-ATTACH-NORMAL-OK 10001>

署名者証明書、署名タイムスタンプの TSA 証明書が有効期間内にあり、共に失効しない場合。ES-T データが有効であることを検証する。本テストケースは ES-T フォーマットの標準テストである。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.5.2 <EST-ATTACH-EXPIRED-NG 10002>

署名タイムスタンプの TSA 証明書は有効であるが、署名証明書が期限切れの時点で署名タイムスタンプを付した場合、署名者証明書を検証する CRL に記載されていないとき ES-T データが無効であることを検証する。

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.3 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.3 12:00:00
署名者証明書	2001.1.1 00:00:00～2001.1.1 23:5959
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.5.3 <EST-ATTACH-REVOKED-NG 10003>

署名者証明書、署名タイムスタンプの TSA 証明書が有効期間内にあり、サイニングタイム属性の時刻および署名タイムスタンプ時刻において、署名者証明書が失効して CRL に記載されている場合、ES-T データが無効であることを検証する。

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.2 12:00:00
サイニングタイム属性の時刻	2001.1.2 12:00:00
署名タイムスタンプの時刻	2001.1.2 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.4 00:00:00-2001.1.4 23:59:59
署名者証明書 CRL 中失効日時	2005.1.1 12:00
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.4 00:00:00-2001.1.4 23:59:59

2.5.4 <EST-ATTACH-SIGTIME-REVOKED-OK 10004>

署名者証明書、署名タイムスタンプの TSA 証明書が有効期間内にあり、署名タイムスタンプ時刻では失効していないが、サイニング属性の時刻において署名者証明書が失効して CRL に記載されている場合、署名時刻は無視し、署名タイムスタンプ時刻での証明書有効性を検証することにより、ES-T データが有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00 (=SignatureTS)
サイニングタイム属性の時刻	2001.1.4 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.3 00:00:00-2001.1.3 23:59:59
署名者証明書 CRL 中失効日時	2001.1.2 12:00:00
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31

署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00-2001.1.3 23:59:59

2.5.5 <EST-ATTACH-SIGTS-REVOKED-NG 10005>

署名者証明書、署名タイムスタンプの TSA 証明書が有効期間内にあり、SigningTime 属性の時刻では失効していないが、署名タイムスタンプ時刻において署名者証明書が失効して CRL に記載されている場合、署名時刻は無視し、署名タイムスタンプ時刻での証明書有効性を検証することにより、ES-T データが無効であることを検証する。

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.3 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.4 00:00:00-2001.1.4 23:59:59
署名者証明書 CRL 中失効日時	2005.1.2 12:00:00
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.4 00:00:00-2001.1.4 23:59:59

2.5.6 <EST-ATTACH-ES-SIG-FORGED-NG 10006>

ES-T フォーマットの CMS SignedData の SignerInfo において signature フィールドにある署名値が改竄されていた場合に無効であることを検証する。

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31

署名 TS TSA 証明書検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

2.5.7 <EST-ATTACH-SIGTS-SIG-FORGED-NG 10007>

ES-T フォーマットの SignatureTimeStamp 属性中の TimeStampToken の CMS SignedData 構造の SignerInfo において signature フィールドにある署名値が改竄されていた場合に無効であることを検証する。

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

2.5.8 <EST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG 10008>

ES-T フォーマットの CMS SignedData の signedAttributes 中の MessageDigest 属性の値が改竄されていた場合に無効であることを検証する。

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.5.9 <EST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG 10009>

ES-T フォーマットの SignatureTimeStamp 属性に含まれるタイムスタンプトークンの signedAttributes 中の MessageDigest 属性の値が改竄されていた場合に無効であることを検証する。

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.5.10 <EST-DETACH-NORMAL-OK 10010>

署名対象文書に対して分離署名を行った ES-T フォーマットにおいてデータが有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6　ES-T フォーマットオプショナルテスト項目

2.6.1 <EST-OTHERCERT-SHA256-OK 20001>

テスト項目<EST-ATTACH-NORMAL-OK>と比較して、署名者証明書を特定するための情報として、ESSSigningCertificate 属性ではなく、ハッシュアルゴリズムに SHA256 を用いた場合で証明書のハッシュ値が一致している場合に、有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6.2 <EST-SIGTS-SHA256-OK 20002>

ES-T フォーマットの署名タイムスタンプのタイムスタンプトークンのハッシュアルゴリズムに SHA256、署名アルゴリズムに SHA256withRSA が用いられた場合に有効であることを検証する。

- TimeStampToken の TSTInfo の MessageImprint は SHA256
- TimeStampToken の SignerInfo の DigestAlgorithm は SHA256
- TimeStampToken の SignerInfo の SignatureAlgorithm は SHA256withRSA

期待値	有効(valid)

署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6.3 <EST-SIGTS-SHA512-OK 20003>

ES-T フォーマットの署名タイムスタンプのタイムスタンプトークンのハッシュアルゴリズムに SHA512、署名アルゴリズムに SHA512withRSA が用いられた場合に有効であることを検証する。

- TimeStampToken の TSTInfo の MessageImprint は SHA512
- TimeStampToken の SignerInfo の DigestAlgorithm は SHA512
- TimeStampToken の SignerInfo の SignatureAlgorithm は SHA512withRSA

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6.4 <EST-CONTENT-TIMESTAMP-OK 20004>

ES-T フォーマットのデータの CMS 署名属性に有効なコンテンツタイムスタンプが含まれている場合に有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
コンテンツタイムスタンプの時刻	2001.1.1 09:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6.5 <EST-INDEPENDENT-SIGNATURES-OK 20005>

二人の署名者による並列署名(独立署名とも言う)の双方に有効な署名タイムスタンプが付与された ES-T フォーマットのデータが有効であることを検証する。

二人の署名者用証明書は同一のサブ CA から発行されているとする。

期待値	有効(valid)
署名 1 を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性 1 の時刻	属性無し
署名タイムスタンプ 1 の時刻	2001.1.1 12:00:00
署名者証明書 1 の有効期限	2001.1.1～2035.12.31
署名 2 を実施したとする時刻	2001.1.1 13:00:00
サイニングタイム属性 2 の時刻	属性無し
署名タイムスタンプ 2 の時刻	2001.1.1 13:00:00
署名者証明書 2 の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6.6 <EST-EPES-WITHOUT-HASHCHECK-OK 20006>

signedAttributes フィールドに署名ポリシ識別子を明示的に持つ EPES(Explicit Policy Electronic Signatures)フォーマットに対し署名タイムスタンプを付与した ES-T データを読み込みエラーとならないことを検証する。
署名ポリシを厳密に扱う実装では、テストデータとして配布される署名ポリシファイルを共に検証に用いる。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59
署名ポリシ OID	1.2.3.4.5
署名ポリシ SHA1 ハッシュ値	af1d3ea7aef706a898191dd257218f5e9acafaa1

2.6.7 <EST-EPES-NORMAL-OK 20007>

signedAttributes フィールドに署名ポリシ識別子を明示的に持つ EPES フォーマットに対し署名タイムスタンプを付与した ES-T データおよび署名ポリシファイルを読み込み EPES フォーマットより生成された ES-T データが有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59
署名ポリシ OID	1.2.3.4.5.20000
署名ポリシ SHA1 ハッシュ値	90490e8e411bd495415988298d07ab45922e8bff

2.6.8 <EST-EPES-POLICY-HASH-NOT-MATCH-NG 20008>

EPES より生成された ES-T フォーマットのデータにおいて、その SignaturePolicyIdentifier CMS 署名属性の持つハッシュ値が署名ポリシファイルのハッシュ値と一致しない場合に、その ES-T データが無効であることを検証する。

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59
署名ポリシ OID	1.2.3.4.5.20000
署名ポリシ SHA1 ハッシュ値	90490e8e411bd495415988298d07ab45922e8bff
CMS 署名ポリシ識別子属性のハッシュ値	1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f1f

2.6.9 <EST-EPES-NOT-BEFORE-VIOLATION-NG 20009>

EPES より生成された ES-T フォーマットのデータの使用する署名ポリシデータにおいて、signingPeriod の notBefore フィールドの値が常に無効となるような値(2035 年 12 月 31 日)に設定されていた場合に、署名ポリシが有効期間内に無いために、関連付けられた ES-T データが無効となることを検証する。

期待値	無効(invalid)

署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59
署名ポリシ OID	1.2.3.4.5.20009
署名ポリシ SHA1 ハッシュ値	eab88babb6ffc05343fc8ef0ca6a7dd4920b7e02
署名ポリシの signingPeriod.notBefore フィールド	2035.12.31 23:59:59

2.6.10 <EST-EPES-MANDATED-SIGNEDATTRS-VIOLATION-NG 20010>

EPES より生成された ES-T フォーマットのデータに関連付けられた署名ポリシデータにおいて、commonRules の signerAndVerifierValue の signerRules の mandatedSignedAttr に signingTime の OID が含まれているにもかかわらず、ES-T フォーマットのデータには signingTime CMS 属性が含まれていない場合に、署名ポリシに違反するため ES-T データが無効となることを検証する。

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59
署名ポリシ OID	1.2.3.4.5.20010
署名ポリシ SHA1 ハッシュ値	5a6c1d137ca139771adbd8d41c868d682ded8b20
mandatedSignedAttr	1.2.840.113549.1.9.4 1.2.840.113549.1.9.5(signingTime)

	1.2.840.113549.1.9.16.2.15

2.6.11 <EST-EPES-EXTERNAL-SIGNEDDATA-VIOLATION-NG 20011>

EPES より生成された ES-T フォーマットのデータに関連付けられた署名ポリシデータにおいて、commonRules の signerAndVerifierValue の signerRules の externalSignedData フィールドの値が TRUE、即ち署名ポリシが分離署名であることを要求している場合に、ES-T フォーマットのデータが内包署名であったとき、署名ポリシに違反するため ES-T データが無効となることを検証する。

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59
署名ポリシ OID	1.2.3.4.5.20011
署名ポリシ SHA1 ハッシュ値	b363f51a65438136d26ce87f3078657df52b5dc4
externalSignedData	TRUE

2.6.12 <EST-ESSCERTV2-SHA256-OK 20012>

署名者証明書を特定するための情報として、ESSSigningCertificateV2 属性を用い、ハッシュアルゴリズムに SHA256 を用いた場合で証明書のハッシュ値が一致している場合に、有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00

署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6.13 <EST-ESSCERTV2-SHA256-FORGED-NG 20013>

署名者証明書を特定するための情報として、ESSSigningCertificateV2 属性を用い、ハッシュアルゴリズムに SHA256 を用いた場合で証明書のハッシュ値が一致しない場合に、無効であることを検証する。

期待値	無効 (invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6.14 < EST-ESSCERTV2-SHA512-OK 20014>

署名者証明書を特定するための情報として、ESSSigningCertificateV2 属性を用い、ハッシュアルゴリズムに SHA512 を用いた場合で証明書のハッシュ値が一致している場合に、有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6.15 < EST-ESSCERTV2-SHA512-FORGED-NG 20015>

署名者証明書を特定するための情報として、ESSSigningCertificateV2 属性を用い、ハッシュアルゴリズムに SHA512 を用いた場合で証明書のハッシュ値が一致しない場合に、無効であることを検証する。

期待値	無効 (invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6.16 < EST-COUNTER-SIGNATURE1-OK 20016>

一人の署名者によるカウンタ署名に有効な署名タイムスタンプが付与された ES-T フォーマットのデータが有効であることを検証する。

署名者、カウンタ署名者の証明書は同一のサブ CA から発行されているとする。

期待値	有効(valid)
署名 0 を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプ 0 の時刻	2001.1.1 12:00:00
署名者証明書 0 の有効期限	2001.1.1～2035.12.31
カウンタ署名 1 を実施したとする時刻	2001.1.1 13:00:00
カウンタ署名 1 の署名タイムスタンプ 1 の時刻	2001.1.1 13:00:00
署名者証明書 1 の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31

署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6.17 < EST-COUNTER-SIGNATURE1-FORGED-NG 20017>

一人の署名者によるカウンタ署名に有効な署名タイムスタンプが付与された ES-T フォーマットのデータで、カウンタ署名の signature フィールドが無効であることを検証する。

署名者、カウンタ署名者の証明書は同一のサブ CA から発行されているとする。

期待値	無効(invalid)
署名 0 を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプ 0 の時刻	2001.1.1 12:00:00
署名者証明書 0 の有効期限	2001.1.1～2035.12.31
カウンタ署名 1 を実施したとする時刻	2001.1.1 13:00:00
カウンタ署名 1 の署名タイムスタンプ 1 の時刻	2001.1.1 13:00:00
署名者証明書 1 の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6.18 < EST-COUNTER-SIGNATURE2-OK 20018>

二人の署名者によるカウンタ署名に有効な署名タイムスタンプが付与された ES-T フォーマットのデータが有効であることを検証する。

署名者、二人のカウンタ署名者の証明書は同一のサブ CA から発行されているとする。

期待値	有効(valid)
署名 0 を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプ 0 の時刻	2001.1.1 12:00:00
署名者証明書 0 の有効期限	2001.1.1～2035.12.31

カウンタ署名１を実施したとする時刻	2001.1.1 13:00:00
カウンタ署名１の署名タイムスタンプ１の時刻	2001.1.1 13:00:00
カウンタ署名２を実施したとする時刻	2001.1.1 14:00:00
カウンタ署名２の署名タイムスタンプ２の時刻	2001.1.1 14:00:00
署名者証明書 0 の有効期限	2001.1.1～2035.12.31
カウンタ署名者証明書１の有効期限	2001.1.1～2035.12.31
カウンタ署名者証明書２の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.6.19 < EST-COUNTER-SIGNATURE2-FORGED-NG 20019>

二人の署名者によるカウンタ署名に有効な署名タイムスタンプが付与された ES-T フォーマットのデータで、二人目のカウンタ署名の signature フィールドが無効であることを検証する。

署名者、二人カウンタ署名者の証明書は同一のサブ CA から発行されているとする。

期待値	無効(invalid)
署名 0 を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプ 0 の時刻	2001.1.1 12:00:00
署名者証明書 0 の有効期限	2001.1.1～2035.12.31
カウンタ署名１を実施したとする時刻	2001.1.1 13:00:00
カウンタ署名１の署名タイムスタンプ１の時刻	2001.1.1 13:00:00
カウンタ署名２を実施したとする時刻	2001.1.1 14:00:00
カウンタ署名２の署名タイムスタンプ２の時刻	2001.1.1 14:00:00

署名者証明書 0 の有効期限	2001.1.1～2035.12.31
カウンタ署名者証明書１の有効期限	2001.1.1～2035.12.31
カウンタ署名者証明書２の有効期限	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.1 00:00:00～2035.12.31 23:59:59

2.7　ES-C フォーマット標準テスト項目

ES-C フォーマットは ECOM プロファイルにおいてオプショナルであるため、標準テスト項目は無いこととする。

2.8　ES-C フォーマットオプショナルテスト項目

2.8.1 <ESC-ATTACH-NORMAL-OK 40001>

署名者証明書、署名タイムスタンプの TSA 証明書が有効期間内にあり、共に失効しない場合。ES-C データが有効であることを検証する。本テストケースは ES-C フォーマットの標準テストである。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

2.8.2 <ESC-DETACH-NORMAL-OK 40002>

署名対象文書に対して分離署名を行った ES-C フォーマットにおいてデータが有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

2.9 ES-X Long フォーマット標準テスト項目

2.9.1 <ESXL-ATTACH-NORMAL-OK 50001>

署名者証明書、署名タイムスタンプの TSA 証明書が有効期間内にあり、共に失効しておらず、これらの検証情報を含む ES-X Long データが有効であることを検証する。本テストケースは ES-X Long フォーマットの標準テストである。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

2.9.2 <ESXL-DETACH-NORMAL-OK 50002>

署名対象文書に対して分離署名を行った ES-X Long フォーマットにおいてデータが有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

2.10 ES-X Long フォーマットオプショナルテスト項目

2.10.1 <ESXL-ATTACH-SIGTS-VALIDATIONINFO-NOT-INCLUDED-OK 60001>

ES-X Long フォーマットを検証する際、署名タイムスタンプ属性のタイムスタンプトークンの TSA 証明書の検証情報がトークン無いに含まれず、別の手段により渡される場合、この ES X-Long フォーマットが有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
サイニングタイム属性の時刻	属性無し
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59

2.11 ES-A フォーマット標準テスト項目

2.11.1 <ESA1-ATTACH-NORMAL-OK 70001>

ECOM 長期署名フォーマットプロファイル 2005 で定めた RFC3126 に基づくアーカイブタイムスタンプのハッシュ計算方法により付与されたアーカイブタイムスタンプ属性を一つ含む ES-A フォーマットが有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archive タイムスタンプ 1 の時刻	2001.1.3 12:00:00
Archive タイムスタンプ 1 TSA 証明書	2001.1.1～2035.12.31
Archive TS TSA 証明書検証 CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.11.2 <ESA1-DETACH-NORMAL-OK 70002>

署名対象文書に対して分離署名を行った第一世代の ArchiveTimeStamp のみを持つ ES-A フォーマットにおいてデータが有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31

署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archive タイムスタンプ 1 の時刻	2001.1.3 12:00:00
Archive タイムスタンプ 1 TSA 証明書	2001.1.1～2035.12.31
Archive TS TSA 証明書検証 CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.11.3 <ESA1-V173-ATTACH-NORMAL-OK 70003>

ETSI TS 101 733 v1.7.3 に基づくアーカイブタイムスタンプのハッシュ計算方法により付与されたアーカイブタイムスタンプ属性を一つ含む ES-A フォーマットが有効であることを検証する。内包署名に対するアーカイブタイムスタンプを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
Archive タイムスタンプ 1 の時刻	2001.1.3 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archive TS TSA 証明書検証 CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.11.4 <ESA1-V173-DETACH-NORMAL-OK 70004>

ETSI TS 101 733 v1.7.3 に基づくアーカイブタイムスタンプのハッシュ計算方法により付与されたアーカイブタイムスタンプ属性を一つ含む ES-A フォーマットが有効であることを検証する。分離署名に対するアーカイブタイムスタンプを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
Archive タイムスタンプ 1 の時刻	2001.1.3 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archive TS TSA 証明書検証 CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.11.5 <ESA1-V173-ATTACH-ATS-FORGED-NG 70005>

ETSI TS 101 733 v1.7.3 に基づくアーカイブタイムスタンプのハッシュ計算方法により付与されたアーカイブタイムスタンプ属性を一つ含む ES-A フォーマットでハッシュ値が不一致し、無効であることを検証する。内包署名に対するアーカイブタイムスタンプを検証する。

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
Archive タイムスタンプ 1 の時刻	2001.1.3 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archive TS TSA 証明書検証 CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.11.6 <ESA1-ETSI173-DETACH-ATS-FORGED-NG 70006>

ETSI TS 101 733 v1.7.3 に基づくアーカイブタイムスタンプのハッシュ計算方法により付与されたアーカイブタイムスタンプ属性を一つ含む ES-A フォーマッ

トでハッシュ値が不一致し、無効であることを検証する。分離署名に対するアーカイブタイムスタンプを検証する。

期待値	無効(invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
Archive タイムスタンプ 1 の時刻	2001.1.3 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archive TS TSA 証明書検証 CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.11.7 <ESA2-V173-ATTACH-NORMAL-OK 70007>

二世代目のアーカイブタイムスタンプが付与された ES-A フォーマットが有効であることを検証する。内包署名に対するアーカイブタイムスタンプを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
Archive タイムスタンプ 1 の時刻	2001.1.3 12:00:00
Archive タイムスタンプ 2 の時刻	2001.1.4 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archive TS1 TSA 証明書検証 CRL	2001.1.4 00:00:00～2002.1.3 23:59:59
Archive TS2 TSA 証明書検証 CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.11.8 < ESA2-V173-DETACH-NORMAL-OK 70008>

二世代目のアーカイブタイムスタンプが付与された ES-A フォーマットが有効であることを検証する。分離署名に対するアーカイブタイムスタンプを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
Archive タイムスタンプ 1 の時刻	2001.1.3 12:00:00
Archive タイムスタンプ 2 の時刻	2001.1.4 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archive TS1 TSA 証明書検証 CRL	2001.1.4 00:00:00～2002.1.3 23:59:59
Archive TS2 TSA 証明書検証 CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.11.9 <ESA2-V173-ATTACH-ATS-FORGED-NG 70009>

二世代目のアーカイブタイムスタンプが付与された ES-A フォーマットで、二世代目のアーカイブタイムスタンプのハッシュが不一致し、無効であることを検証する。内包署名に対するアーカイブタイムスタンプを検証する。

期待値	無効 (invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
Archive タイムスタンプ 1 の時刻	2001.1.3 12:00:00
Archive タイムスタンプ 2 の時刻	2001.1.4 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archive TS1 TSA 証明書検証 CRL	2001.1.4 00:00:00～2002.1.3 23:59:59
Archive TS2 TSA 証明書検証 CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.11.10 <ESA2-V173-DETACH-ATS-FORGED-NG 70010>

二世代目のアーカイブタイムスタンプが付与された ES-A フォーマットで、二世代目のアーカイブタイムスタンプのハッシュが不一致し、無効であることを検証する。分離署名に対するアーカイブタイムスタンプを検証する。

期待値	無効 (invalid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
Archive タイムスタンプ 1 の時刻	2001.1.3 12:00:00
Archive タイムスタンプ 2 の時刻	2001.1.3 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archive TS1 TSA 証明書検証 CRL	2001.1.4 00:00:00～2002.1.3 23:59:59
Archive TS2 TSA 証明書検証 CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.12 ES-A フォーマットオプショナルテスト項目

2.12.1 <ESA1-ATTACH-ETSI151-OK 80001>

ECOM 長期署名フォーマットプロファイルの範囲外ではあるが、ETSI TS 101 733 v1.5.1 以降で定めている新しいアーカイブハッシュ計算方法に本設計書付録で示した正規化法を用いたアーカイブタイムスタンプ属性を一つ含む ES-A フォーマットが有効であることを検証する。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31

署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archive タイムスタンプ 1 の時刻	2001.1.3 12:00:00
Archive タイムスタンプ 1 TSA 証明書	2001.1.1～2035.12.31
Archive TS TSA 証明書検証 CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.12.2 <ESA1-DETACH-ETSI151-OK 80002>

テスト項目<ESA1-ATTACH-ETSI151-OK>と同じ条件で分離署名であった場合に ES-A フォーマットが有効であることを検証する。最初のハッシュ対象 encapContentInfo はコンテンツを含め内部まで DER 正規化されていなければならない。署名対象データは<ESA1-ATTACH-ETSI151-OK>と同じデータとし、他の分離署名の署名対象とは異なる。

期待値	有効(valid)
署名を実施したとする時刻	2001.1.1 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.2 23:59:59
署名タイムスタンプ TSA 証明書	2001.1.1～2035.12.31
署名 TS TSA 証明書検証 CRL	2001.1.3 00:00:00～2001.1.3 23:59:59
Archive タイムスタンプ 1 の時刻	2001.1.3 12:00:00
Archive タイムスタンプ 1 TSA 証明書	2001.1.1～2035.12.31
Archive TS TSA 証明書検証 CRL	2001.1.4 00:00:00～2035.12.31 23:59:59

2.13 ES-T 標準テストケース

本節では ES-T フォーマットを扱う実装が満足すべきテストケースを示す。

2.13.1 <OFF-T-1>

テストケース名	OFF-T-1
一般的な内包署名の ES-T フォーマットを読み込むことができる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK

2.13.2 <OFF-T-2>

テストケース名	OFF-T-2
ES-T フォーマットの署名者証明書の期限切れを扱える	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10002	EST-ATTACH-EXPIRED-NG

2.13.3 <OFF-T-3>

テストケース名	OFF-T-3
ES-T フォーマットの署名者証明書の失効を扱える	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10003	EST-ATTACH-REVOKED-NG

2.13.4 <OFF-T-4>

テストケース名	OFF-T-4

ES-T フォーマットの署名者証明書の認証パス検証を正しく行える	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10002	EST-ATTACH-EXPIRED-NG
10003	EST-ATTACH-REVOKED-NG

2.13.5 <OFF-T-5>

テストケース名	OFF-T-5
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	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10003	EST-ATTACH-REVOKED-NG
10004	EST-ATTACH-SIGTIME-REVOKED-OK
10005	EST-ATTACH-SIGTS-REVOKED-NG

2.13.6 <OFF-T-6>

テストケース名	OFF-T-6
ES-T フォーマットの SignerInfo の署名値の改竄を検知できる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10006	EST-ATTACH-ES-SIG-FORGED-NG

2.13.7 <OFF-T-7>

テストケース名	OFF-T-7
ES-T フォーマットの署名タイムスタンプのタイムスタンプトークンの SignerInfo の	

署名値の改竄を検知できる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10007	EST-ATTACH-SIGTS-SIG-FORGED-NG

2.13.8 <OFF-T-8>

テストケース名	OFF-T-8
ES-T フォーマットの MessageDigest のハッシュ値の改竄を検知できる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10008	EST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG

2.13.9 <OFF-T-9>

テストケース名	OFF-T-8
ES-T フォーマットの署名タイムスタンプのタイムスタンプトークンの MessageDigest のハッシュ値の改竄を検知できる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
10009	EST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG

2.13.10 <OFF-T-10>

テストケース名	OFF-T-10
分離署名の ES-T フォーマットを扱える	
成功条件：以下のテスト項目が全て期待値通り	
10010	EST-DETACH-NORMAL-OK

2.14 ES-T オプショナルテストケース

本節では ES-T フォーマットを扱う実装の機能を確認するために行うことが可能はオプショナルテストケースを示す。

2.14.1 <OFF-T-OP-1>

テストケース名	OFF-T-OP-1
OtherSigningCertificate 属性において SHA-256 である ES-T フォーマットを扱える	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20001	EST-OTHERCERT-SHA256-OK

2.14.2 <OFF-T-OP-2>

テストケース名	OFF-T-OP-2
署名タイムスタンプのタイムスタンプトークンのハッシュや署名に SHA-256 アルゴリズムが使われている ES-T フォーマットを扱える	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20002	EST-SIGTS-SHA256-OK

2.14.3 <OFF-T-OP-3>

テストケース名	OFF-T-OP-3
署名タイムスタンプのタイムスタンプトークンのハッシュや署名に SHA-512 アルゴリズムが使われている ES-T フォーマットを扱える	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20003	EST-SIGTS-SHA512-OK

2.14.4 <OFF-T-OP-4>

テストケース名	OFF-T-OP-4
CMS 署名属性にコンテンツタイムスタンプ属性が含まれる ES-T フォーマットを正しく検証できる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20004	EST-CONTENT-TIMESTAMP-OK

2.14.5 <OFF-T-OP-5>

テストケース名	OFF-T-OP-5
独立署名(並列署名)、即ち signerInfo が 2 つあり、署名に用いたそれらの署名者証明書が同一の信頼点である ES-T フォーマットを正しく検証できる	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20005	EST-INDEPENDENT-SIGNATURES-OK

2.14.6 <OFF-T-OP-6>

テストケース名	OFF-T-OP-6
EPES フォーマットに基づく ES-T フォーマットにおいて読み込み時エラーとならないことを検証する。	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20006	EST-EPES-WITHOUT-HASHCHECK-OK

備考：署名ポリシを正しく扱う実装は、テストデータに含まれる署名ポリシを用いて検証を行う。署名ポリシを処理しない実装はエラーが発生しないことのみを確認する。

2.14.7 <OFF-T-OP-7>

テストケース名	OFF-T-OP-7
EPES フォーマットに基づく ES-T フォーマットにおいて署名ポリシのハッシュ値の一致確認を行い正しく署名ポリシが扱えることを検証する。	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20007	EST-EPES-NORMAL-OK
20008	EST-EPES-POLICY-HASH-NOT-MATCH-NG

2.14.8 <OFF-T-OP-8>

テストケース名	OFF-T-OP-8
EPES に基づく ES-T フォーマットにおいて、署名ポリシの notBefore を正しく扱うことができる。	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20007	EST-EPES-NORMAL-OK
20009	EST-EPES-NOT-BEFORE-VIOLATION-NG

2.14.9 <OFF-T-OP-9>

テストケース名	OFF-T-OP-9
EPES に基づく ES-T フォーマットにおいて、署名ポリシの signerRules の mandatedSignedAttr を正しく扱うことができる。	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20007	EST-EPES-NORMAL-OK
20010	EST-EPES-MANDATED-SIGNEDATTRS-VIOLATION-NG

2.14.10 <OFF-T-OP-10>

テストケース名	OFF-T-OP-10
EPES に基づく ES-T フォーマットにおいて、署名ポリシの externalSignedData が TRUE,即ち分離署名を要求しているのに内包署名であるような ES-T データを正しく扱うことができる。	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20007	EST-EPES-NORMAL-OK
20011	EST-EPES-EXTERNAL-SIGNEDDATA-VIOLATION-NG

2.14.11 <OFF-T-OP-11>

テストケース名	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	
成功条件：以下のテスト項目が全て期待値通り	
20012	EST-ESSCERTV2-SHA256-OK
20013	EST-ESSCERTV2-SHA256-FORGED-NG

2.14.12 <OFF-T-OP-12>

テストケース名	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	
成功条件：以下のテスト項目が全て期待値通り	
20014	EST-ESSCERTV2-SHA512-OK
20015	EST-ESSCERTV2-SHA512-FORGED-NG

2.14.13 <OFF-T-OP-13>

テストケース名	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。	
成功条件：以下のテスト項目が全て期待値通り	
10001	EST-ATTACH-NORMAL-OK
20016	EST-COUNTER-SIGNATURE1-OK
20017	EST-COUNTER-SIGNATURE1-FORGED-NG
20018	EST-COUNTER-SIGNATURE2-OK
20019	EST-COUNTER-SIGNATURE2-FORGED-NG

2.15 ES-C オプショナルテストケース

2.15.1 <OFF-C-OP-1>

テストケース名	OFF-C-OP-1
一般的な内包署名の ES-C フォーマットを読み込むことができる	
成功条件：以下のテスト項目が全て期待値通り	
40001	ESC-ATTACH-NORMAL-OK

2.15.2 <OFF-C-OP-2>

テストケース名	OFF-C-OP-2
分離署名の ES-C フォーマットを扱える	
成功条件：以下のテスト項目が全て期待値通り	
40001	ESC-ATTACH-NORMAL-OK
40002	ESC-DETACH-NORMAL-OK

2.16 ES-X Long 標準テストケース

2.16.1 <OFF-X-1>

テストケース名	OFF-X-1
一般的な内包署名の ES-X Long フォーマットを読み込むことができる	
成功条件：以下のテスト項目が全て期待値通り	
50001	ESXL-ATTACH-NORMAL-OK

2.16.2 <OFF-X-2>

テストケース名	OFF-X-2
分離署名の ES-X Long フォーマットを扱える	
成功条件：以下のテスト項目が全て期待値通り	
50002	ESXL-DETACH-NORMAL-OK

2.17 ES-X Long オプショナルテストケース

2.17.1 <OFF-X-OP-1>

テストケース名	OFF-X-OP-1
ES-X Long フォーマットで署名タイムスタンプの検証情報がそのタイムスタンプトークン内に含まれていない場合に別途与えられる検証情報を元に検証できる	
成功条件：以下のテスト項目が全て期待値通り	
50001	ESXL-ATTACH-NORMAL-OK
60001	ESXL-ATTACH-SIGTS-VALIDATIONINFO-NOT-INCLUDED-OK

2.18 ES-A 標準テストケース

2.18.1 <OFF-A-1>

テストケース名	OFF-A-1
ECOM プロファイルに基づく内包署名の第一世代の ES-A フォーマットを扱うことができる	
成功条件：以下のテスト項目が全て期待値通り	

70001	ESA1-ATTACH-NORMAL-OK

2.18.2 <OFF-A-2>

テストケース名	OFF-A-2
ECOM プロファイルに基づく分離署名の第一世代の ES-A フォーマットを扱うことができる	
成功条件：以下のテスト項目が全て期待値通り	
70002	ESA1-DETACH-NORMAL-OK

2.18.3 <OFF-A-3>

テストケース名	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 フォーマットを扱うことができる	
成功条件：以下のテスト項目が全て期待値通り	
70003	ESA1-V173-ATTACH-NORMAL-OK
70005	ESA1-V173-ATTACH-ATS-FORGED-NG

2.18.4 <OFF-A-4>

テストケース名	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 フォーマットを扱うことができる	
成功条件：以下のテスト項目が全て期待値通り	
70004	ESA1-V173-DETACH-NORMAL-OK
70006	ESA1-V173-DETACH-ATS-FORGED-NG

2.18.5 <OFF-A-5>

テストケース名	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 フォーマットを扱うことができる	
成功条件：以下のテスト項目が全て期待値通り	
70007	ESA2-V173-ATTACH-NORMAL-OK
70009	ESA2-V173-ATTACH-ATS-FORGED-NG

2.18.6 <OFF-A-6>

テストケース名	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 フォーマットを扱うことができる	
成功条件：以下のテスト項目が全て期待値通り	
70008	ESA2-V173-DETACH-NORMAL-OK
70010	ESA2-V173-DETACH-ATS-FORGED-NG

2.19 ES-A オプショナルテストケース

2.19.1 <OFF-A-OP-1>

テストケース名	OFF-A-OP-1
ETSI TS 101 733 v1.5.1 以降のハッシュ計算法に基づく内包署名の第一世代の ES-A フォーマットを扱うことができる	
成功条件：以下のテスト項目が全て期待値通り	
80001	ESA1-ATTACH-ETSI151-OK

2.19.2 <OFF-A-OP-2>

テストケース名	OFF-A-OP-2
ETSI TS 101 733 v1.5.1 以降のハッシュ計算法に基づく分離署名の第一世代の ES-A フォーマットを扱うことができる	
成功条件：以下のテスト項目が全て期待値通り	
80002	ESA1-DETACH-ETSI151-OK

3　署名データ生成・検証相互運用性テストカテゴリ(旧オンラインテスト)

ある実装が生成した有効な長期署名フォーマットのデータが相互に読み込みおよび検証ができることを確認するためのテストを行う。あらかじめ指定された署名対象データ、証明書、CRL、タイムスタンプサービスを用いて参加企業全ての製品により長期署名フォーマットデータを生成する。各社で生成されたデータをお互いに交換し、参加企業の各製品において、他社製品の生成したデータが有効であることを検証する。CRL およびタイムスタンプトークンはオンラインで取得する。

ここで長期署名フォーマットデータは流通性が高く JIS の要件にもなっている CAdES-T および CAdES-A を対象とする。

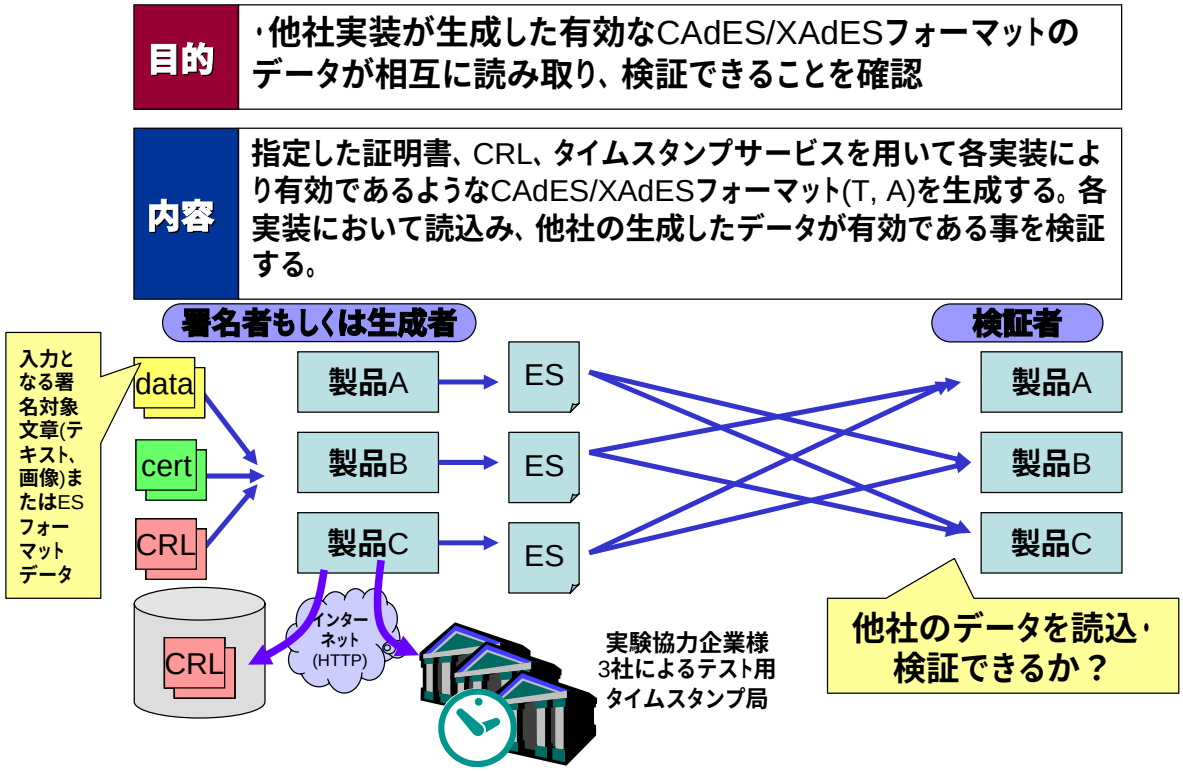

図 3-1 署名データ生成・検証相互運用性テストの概要

3.1 テストケースの概要

テスト項目は以下の 5 つのテストケースに分類される。

- CAdES-T 基本テストケース
  - CMS 署名形態である Attached, Detached に対応した CAdES-T の基本テスト
- CAdES-T タイムスタンプ局テストケース
  - 実験に協力頂いた 3 つのタイムスタンプ局への対応を確認するテスト
- CAdES-T オプショナル属性テストケース
  - CAdES-T に含めることが可能な署名属性、非署名属性の対応を確認するテスト
- CAdES-A 基本テストケース
  - Attached, Detached 署名のアーカイブ署名、複数世代に渡るアーカイブタイムスタンプへの対応を確認するアーカイブ署名の基本テスト
- CAdES-A オプショナル属性テストケース
  - CAdES-A に含めることが可能な非署名属性の対応を確認するテスト

テストケースには、それぞれ規定された要件に基づいて署名データを作成するテスト項目が含まれている。参加組織の実装がサポートする内容についてのみテスト項目を実施してよい。以下に各テストケースを構成するテスト項目の概要をまとめる。

表 3-1　署名データ生成・検証相互運用テスト テスト項目一覧

CAdES-T 基本テストケース (ON-T-BASIC)	
ON-T-BASIC-ATTACHED	署名タイムスタンプ付 CMS 内包署名
ON-T-BASIC-DETACHED	署名タイムスタンプ付 CMS 分離署名
CAdES-T タイムスタンプ局テストケース (ON-T-TSA)	
ON-T-TSA-AMANO-ATTACHED	AMANO TSA を使用
ON-T-TSA-PFU-ATTACHED	PFU TSA を使用
ON-T-TSA-SEIKO-ATTACHED	SEIKO TSA を使用
CAdES-T オプショナル属性テストケース (ON-T-ATTR)	
ON-T-ATTR-SIGNINGTIME	SigningTime を使用
ON-T-ATTR-EPES-RFC3125	SignaturePolicyIdentifier を使用。RFC 3125 に基づく ASN.1 形式の署名ポリシファイルを使用
ON-T-ATTR-SIGNERLOCATION	SignerLocation を使用
ON-T-ATTR-SIGNERATTRIBUTES-CLAIMED	ClaimedAttributes を持つ SignerAttributes を使用
ON-T-ATTR-CONTENTHINTS	ContentHints を使用
ON-T-ATTR-COMMITMENTTYPEINDICATION	CommitmentTypeIndication を使用
ON-T-ATTR-CONTENTTS-CLAIMEDTIME	ContentTimeStamp と SigningTime を使用
ON-T-ATTR-CONTENTREFERENCE	ContentReference を使用
ON-T-ATTR-CONTENTIDENTIFIER	ContentIdentifier を使用
ON-T-ATTR-COUNTERSIGNATURE	CounterSignature を使用
ON-T-ATTR-ESSCERTV2	ESSCertV2 を使用
CAdES-A 基本テストケース (ON-A-BASIC)	
ON-A-BASIC-A1-ATTACHED	内包署名で 1 つの ArchiveTimeStampV2
ON-A-BASIC-A1-DETACHED	分離署名で 1 つの ArchiveTimeStampV2
ON-A-BASIC-A2-ATTACHED	内包署名で 2 つの ArchiveTimeStampV2
ON-A-BASIC-A3-ATTACHED	内包署名で 3 つの ArchiveTimeStampV2
CAdES-A オプショナル属性テストケース (ON-A-ATTR)	
ON-A-ATTR-A1-ARCTSV1-ATTACHED	内包署名で 1 つの ArchiveTimeStampV1
ON-A-ATTR-A1-TIMESTAMPEDCERTSCRLS	TimestampedCertsCRLs、ArcTS を付与
ON-A-ATTR-A1-ESCTIMESTAMP	ESCTimeStamp、ArcTS を付与

各テスト項目に必要となる CAdES のプロパティを以下にまとめる。

表 3-2　テスト項目と必要なプロパティ

	TEST CASE ID	ON-T-BASIC ATTACHED	ON-T-BASIC DETACHED	ON-T-TSA AMANO-ATTACHED	ON-T-TSA PFU-ATTACHED	ON-T-TSA SEIKO-ATTACHED	ON-T-ATTR SIGNINGTIME	ON-T-ATTR EPES-RFC3125	ON-T-ATTR SIGNERLOCATION	ON-T-ATTR SIGNERATTRIBUTES-CLAIMED	ON-T-ATTR CONTENTHINTS	ON-T-ATTR COMMITMENTTYPEINDICATION	ON-T-ATTR CONTENTS-CLAIMEDTIME	ON-T-ATTR CONTENTREFERENCE	ON-T-ATTR CONTENTIDENTIFIER	ON-T-ATTR COUNTERSIGNATURE	ON-T-ATTR ESSCERTV2	ON-A-BASIC A1-ATTACHED	ON-A-BASIC A1-DETACHED	ON-A-BASIC A2-ATTACHED	ON-A-BASIC A3-ATTACHED	ON-A-ATTR A1-ARCTS1-ATTACHED	ON-A-ATTR A1-TIMESTAMPEDCERTSCRLS	ON-A-ATTR A1-ESCTIMESTAMP
Signed Attributes	ContentType	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	MessageDigest	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	ESSSigningCertificate	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1		C1	C1	C1	C1	C1	C1	C1
	ESSSigningCertificateV2	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	✓	C1	C1	C1	C1	C1	C1	C1
	OtherSigningCertificate	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1		C1	C1	C1	C1	C1	C1	C1
	SigningTime						✓						✓											
	SignaturePolicyIdentifier							✓														✓		
	SignerLocation								✓															
	SignerAttributes									✓														
	ContentHints										✓													
	CommitmentTypeIndication											✓												
	ContentTimeStamp												✓											
	ContentReference													✓										
	ContentIdentifier														✓									
Unsigned Signature Properties	CounterSignature															✓								
	SignatureTimeStamp	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	CompleteCertificateRefs																	✓	✓	✓	✓	✓	✓	✓
	CompleteRevocationRefs																	✓	✓	✓	✓	✓	✓	✓
	AttributeCertificateRefs																							
	AttributeRevocationRefs																							
	ESCTimeStamp																							✓
	TimestampedCertsCRLs																						✓	
	CertificateValues																	✓	✓	✓	✓	✓	✓	✓
	RevocationValues																	✓	✓	✓	✓	✓	✓	✓
	ArchiveTimeStampV1																					1		
	ArchiveTimeStampV2																	1	1	2	3		1	1

C1: Choice however ESSSigningCertificate is recommende BLANK: Option ✓ :Mandatory 123: Number of ArcTS

3.2 テスト実施手順

- テスト準備
  - タイムスタンプ局との疎通確認
  - 認証局リポジトリとの疎通確認
- 署名データの生成
  - 署名用鍵(PKCS#12 or JKS)をダウンロードし署名データ生成アプリケーションのために設定する
  - 生成データテンプレートアーカイブ(結果データフォルダ構成、入力データ、要件情報を含む) をダウンロードする
  - 検証必要なデータをコピーやリンクなど張る
  - 要件に合わせデータを生成する
  - 必要ならばハッシュ対象、使用した証明書、CRL など参考情報として置く
  - また検証に必要な(自動コピーされない)データは直下に置く
  - 生成データデータのセットの圧縮アーカイブファイルを作成する
  - 共有スペース(ECOM 会議室)に生成したデータをアップロードする
  - 生成データに問題があった場合には、期間内ならば生成データを再度アップロードできる。
- 署名データの検証
  - 共有スペース(ECOM 会議室)に生成した各社のデータを全てダウンロードする
  - データアーカイブを適当なディレクトリに展開する
  - 認証パス検証に必要な設定を適宜行う
  - 検証結果をエクセルシートに記録する。(検証失敗の場合には失敗理由をメモしておくとよい) (いつのデータセット、実装によるものか記録しておく)
  - 検証結果を共有スペース(ECOM 会議室)にアップデートする。
- 結果が満足なものでない場合、また生成者が新しいアーカイブをアップロードした場合には 1 生成, 2 検証 の手順を繰り返す。

3.2.1 テンプレートアーカイブのダウンロードと解凍

テストデータの生成の際に必要となるテスト項目、証明書や入力となるデータを ZIP アーカイブとしたものをテンプレートアーカイブと呼ぶ。これは ECOM 電子会議室よりダウンロードできる。アーカイブを解凍すると以下のようなディレクトリ構造となっている。

```
02_ONLINE/ 生成・検証相互運用性テスト用のフォルダ
  01_CADES/ CAdES テスト生成用フォルダ      ←これをコピーし結果として提出
    ON-T-BASIC-ATTACHED/ 各テスト項目フォルダ      ←ここに CAdES 署名結果を格納
      :
  02_XADES/ XAdES テスト生成用フォルダ      ←これをコピーし結果として提出
    ON-T-BASIC-ENVELOPING/ 各テスト項目フォルダ      ←ここに XAdES 署名結果を格納
      :
  03_CERTS/   ←署名に用いる証明書と鍵(PKCS#12 と JKS)
  99_WORK/ 検証用の作業領域として使用するディレクトリ   ←他組織の署名を置き検証
    CADES_1_社名_生成日付/      ↑最初は空ディレクトリ
    CADES_2_社名_生成日付/
    XADES_1_社名_生成日付/
```

3.2.2 署名生成の入力ファイル

署名生成の入力として以下のファイルを用いる。

- TARGET_AAA.txt
  - **内包**(attached)**署名のテストに用いるプレーンテキストの署名対象ファイル。**"aaa"**の** ASCII **テキストで構成される。**
- TARGET_BBB.bin
  - **分離**(detached)**署名のテストに用いる** 1M **バイトのバイナリの署名対象ファイル。**0x0102030405060708090**0 の並びで構成される。**

- TARGET-SIGPOL-RFC3125.der
  - ETSI TR 101 272 v1.1.1 もしくは RFC 3125 に基づく ASN.1 DER 形式の署名ポリシファイル。署名ポリシの OID は 1.2.3.4.5.1 とする。

3.2.3 署名の生成

01_CADES もしくは 02_XADES フォルダの下の各テスト項目のフォルダに対し、テスト設計書の生成要件に従い署名データを作成する。

3.2.4 生成するファイル名に関する要件

各テスト項目ディレクトリの中のファイル名は以下に従う。

- 生成された署名ファイルは "sig.der" もしくは "sig.xml" とする。
- 検証に必要な証明書、CRL を各テスト項目ディレクトリに含める。
- 検証の際に必要とはならないが、参考となるようなハッシュ対象データ、証明書、CRL などがあれば DATA/ フォルダの下に置く。
- ChangeLog.ja.txt (SJIS) もしくは ChangeLog.en.txt に生成の変更履歴を記入する。

3.2.5 生成アーカイブに含める証明書、CRL のファイル名について

生成側は検証側がある程度処理を自動化できるように証明書検証に必要なデータのファイル名のガイドラインを与える。各テスト項目フォルダの下に以下のガイドラインに従ったファイル名の証明書、CRL を含める。

署名者、カウンタ署名者の証明書は以下のファイル名とする。

CERT-SIG-EE.cer ←署名者証明書(参加企業により異なる)

CERT-SIG-EE-CS1.cer	←カウンタ署名者証明書(共通)
CERT-SIG-SUB1.cer	←署名用サブ CA 証明書(共通)
CERT-SIG-ROOT.cer	←署名用ルート CA 証明書(共通)

署名者証明書、カウンタ署名者証明書の検証に必要な CRL のファイル名は以下に従う。ファイルは生成者が作成する。

EE 検証の CRL はオンライン取得が可能
EE 証明書の CRL を指定のものにしたい場合には

CERT-SIG-SUB1.x.crl	←署名者用の発行時刻を特定した CRL
CERT-SIG-SUB1-CS1.x.crl	←カウンタ署名署名者用の発行時刻を特定した CRL

(注 1) ルート CA など他の CA の発行する CRL も同様にする。
(注 2) 過去発行された CRL には".x.crl"の拡張子をつけることとする。

TSA 証明書は以下のファイル名とする。使用するテスト用タイムスタンプ局により異なるので注意する。<ON-T-TSA>テストケースに含まれるテスト項目のフォルダからコピーしてもよい。

CERT-TSA-EE.cer	←TSA 証明書(参加企業により異なる)
CERT-TSA-SUB1.cer	←TSA 用サブ CA 証明書(参加企業により異なる)
CERT-TSA-ROOT.cer	←TSA 用ルート CA 証明書(参加企業により異なる)

TSA 証明書の検証に必要な CRL のファイル名は以下のガイドラインに従う。

CERT-TSA-SUB1-ST1.x.crl	SignatureTS 用の発行時刻を特定した CRL
CERT-TSA-SUB1-ST1-CS1.x.crl	カウンタ署名の SignatureTS 用の発行時刻を特定した CRL
CERT-TSA-SUB1-CT1.x.crl	ContentTimeStamp 用の発行時刻を特定した CRL
CERT-TSA-SUB1-DT1.x.crl	AllDataObjectsTimeStamp 用の発行時刻を特定した CRL
CERT-TSA-SUB1-IT1.x.crl	IndividualDataObjectsTimeStamp 用の発行時刻を特定した CRL
CERT-TSA-SUB1-ROT1.x.crl	RefsOnlyTimestamp、TimestampedCertsCRLs 用の発行時刻を特定した CRL
CERT-TSA-SUB1-RST1.x.crl	SigAndRefsTimestamp、ESCTimeStamp 用の発行時刻を特定した CRL
CERT-TSA-SUB1-AT1.x.crl	1 つめの ArchiveTimeStamp 用の発行時刻を特定した CRL

CERT-TSA-SUB1-AT2.x.crl	2 つめの ArchiveTimeStamp 用の発行時刻を特定した CRL
CERT-TSA-SUB1-AT3.x.crl	3 つめの ArchiveTimeStamp 用の発行時刻を特定した CRL

署名者証明書の検証情報については CertificateValues、RevocationValues に格納することを推奨し、その場合には検証に不要な証明書、CRL ファイルはテスト項目ディレクトリに含めなくてよい。

3.2.6 生成結果の ZIP アーカイブの作成

生成結果の署名やメモなどを ZIP アーカイブする。以下の手順で行う。

- 01_CADES もしくは 02_XADES ディレクトリの下の ChangeLog.ja.txt もしくは ChangeLog.en.txt ファイルに、変更履歴があれば記入する。
- 生成した 01_CADES もしくは 02_XADES ディレクトリをコピーし、コピー先を以下のディレクトリ名に変更する。

[CADES or XADES]_[グループ分け(1 or 2)]_[社名]_[生成年月日]
(例) CADES_1_ENTRUST_20071024

- 前の手順で作成したディレクトリを ZIP アーカイブにする。
- ECOM 電子会議室にアップロードする。

3.2.7 署名の検証

ECOM 電子会議室より他の参加企業の生成した署名をダウンロードし、99_WORK にて解凍し、その参加企業の署名を検証する。

3.3 共通の要件

署名データ生成・検証相互運用性テストで共通の署名データの生成および検証に関わる要件を示す。

生成要件			
	ETSI TS 101 733 もしくは RFC 3126 に基づく CAdES を生成しなければならない		MUST
	署名者の署名には参加企業毎に実験用に配布された鍵と証明書を用いなければならない		MUST
	署名属性、非署名属性		
		ContentType, MessageDigest を含まなければならない	MUST
		ESSSigningCertificate、ESSSigningCertificateV2、OtherSigningCertificate のいずれかを含まなければならない	MUST
		SignatureTimeStamp を含まなければならない。	MUST
		他の属性を含めることができる(※1)	MAY
	TSA は 3 つのテスト用 TSA 局のうち任意のものを使用できる		MAY
検証要件			
	ETSI TS 101 733 もしくは RFC 3126 に基づく CAdES を検証しなければならない		MUST
	証明書検証を除き CMS 署名の有効性を検証しなければならない		MUST
	署名検証を除きタイムスタンプトークンの有効性を検証しなければならない		MUST
	SignatureTimeStamp の時刻に署名者証明書の有効性を検証しなければならない		MUST

注意※1：次節より個々のテスト項目の生成要件を述べるが、全てのテスト項目において、規定された要件を満足する限り他の属性を含んでよい。例えば、複数の属性を含むよう生成された署名データを、複数のテスト項目の生成結果として利用することができる。

3.4 CAdES-T **署名基本テストケース** (ON-T-BASIC)

3.4.1 <ON-T-BASIC-ATTACHED>

テキストファイルに対し、内包署名(即ち attached もしくは enveloping 署名)による CAdES-T の生成および検証を行う。

共通の要件を基礎とする。		
生成要件		
	encapContentInfo.eContent に署名対象文書を含む内包署名を生成しなければならない	MUST
	署名対象文書は “./TARGET_AAA.txt” でなければならない	MUST

3.4.2 <ON-T-BASIC-DETACHED>

ローカルにあるバイナリデータファイルに対し分離署名(detached 署名)による CAdES-T の生成および検証を行う。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。		
生成要件		
	encapContentInfo.eContent に署名対象文書を含まない分離署名を生成しなければならない	MUST
	署名対象文書は “./TARGET_BBB.bin” でなければならない	MUST

3.5 CAdES-T タイムスタンプ局テストケース (ON-T-TSA)

署名データ生成・検証相互運用性テストでは、実験協力企業による 3 つのテスト用タイムスタンプサービスが利用できる。他のテスト項目では任意の TSA を利用できるとしているが、本テストケースでは、それぞれの TSA への対応を確認する。

3.5.1 <ON-T-TSA-AMANO-ATTACHED>

アマノタイムビジネスのテスト用 TSA を用いた内包署名による CAdES-T の生成および検証を行う。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。		
生成要件		
	TSA はアマノタイムビジネスのテスト用 TSA を用いる	MUST

3.5.2 <ON-T-TSA-PFU-ATTACHED>

PFU のテスト用 TSA を用いた内包署名による CAdES-T の生成および検証を行う。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。		
生成要件		
	TSA は PFU のテスト用 TSA を用いる	MUST

3.5.3 <ON-T-TSA-SEIKO-ATTACHED>

セイコープレシジョンのテスト用 TSA を用いた内包署名による CAdES-T の生成および検証を行う。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。		
生成要件		
	TSA はセイコープレシジョンのテスト用 TSA を用いる	MUST

3.6 CAdES-T **オプショナルプロパティテストケース** (ON-T-ATTR)

本テストケースでは CAdES-T に付与することが可能なオプションの属性への対応を確認する。

3.6.1 <ON-T-ATTR-SIGNINGTIME>

本テスト項目では比較的一般的な SigningTime 属性への対応を確認する。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		SigningTime を含まなければならない	MUST
		ETSI TS 101 733 v1.7.3 C.3.6 に基づく時刻の順序関係に基づき SigningTime およびタイムスタンプを生成できなければならない	MUST
検証要件			
	ETSI TS 101 733 v1.7.3 C.3.6 に基づく時刻の順序関係の検証ができなければならない		MUST
	タイムスタンプおよび SigningTime の時刻が何らかの方法で表示されることが望ましい		RECOMMEND

3.6.2 <ON-T-ATTR-EPES-RFC3125>

CAdES-EPES として ETSI TR 101 272 v1.1.1 もしくは RFC 3125 に準拠した ASN.1 形式の署名ポリシによる SignaturePolicyIdentifier を持つ CAdES-T の対応を確認する。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。		
生成要件		
	署名属性、非署名属性	

		SignaturePolicyIdentifier を含まなければならない	MUST
		署名ポリシは “./TARGET-SIGPOL-RFC3125.der” を用いなければならない。	MUST
		署名ポリシの OID は 1.2.3.4.5.1 でなければならない。	MUST
検証要件			
	署名ポリシ “./TARGET-SIGPOL-RFC3125.der”に基づいて検証ができなければならない。		MUST

3.6.3 <ON-T-ATTR-SIGNERLOCATION>

SignerLocation を持つ CAdES-T の対応を確認する。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		SignerLocation を含まなければならない	MUST
検証要件			
	SignerLocation の有無および記載された内容を何らかの方法で目視確認(※1)しなければならない。		MUST

※１：表示方法は標準出力、ログ、ダイアログ、ウィンドウなど如何なる方法でも構わない。以降、「何らかの方法で目視確認」とある場合には同様とする。

3.6.4 <ON-T-ATTR-SIGNERATTRIBUTES-CLAIMED>

ClaimedAttributes を持つ SignerAttributes が含まれた CAdES-T の対応を確認する。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		ClaimedAttributes を持つ SignerAttributes を含まなければならない	MUST
		ClaimedAttributes を持つ SignerAttributes には CertifiedAttributes を含むことができる	MAY

検証要件		
	SignerAttributes、ClaimedAttributes の有無および記載された内容を何らかの方法で目視確認しなければならない。	MUST
	CertifiedAttributes の属性証明書は検証を省略することができる	MAY

3.6.5 <ON-T-ATTR-CONTENTHINTS>

ContentHints を持つ CAdES-T の対応を確認する。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。		
生成要件		
	署名属性、非署名属性	
	ContentHints を含まなければならない	MUST
検証要件		
	ContentHints の有無および記載された内容を何らかの方法で目視確認しなければならない。	MUST

3.6.6 <ON-T-ATTR-COMMITMENTTYPEINDICATION>

CommitmentTypeIndication を持つ CAdES-T の対応を確認する。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。		
生成要件		
	署名属性、非署名属性	
	CommitmentTypeIndication を含まなければならない	MUST
検証要件		
	CommitmentTypeIndication の有無および記載された内容を何らかの方法で目視確認しなければならない。	MUST

3.6.7 <ON-T-ATTR-CONTENTTS-CLAIMEDTIME>

ContentTimeStamp と SigningTime プロパティを持つ CAdES-T の対応を確認する。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		ContentTimeStamp および SigningTime を含まなければならない	MUST
		ETSI TS 101 733 v1.7.3 C.3.6 に基づく時刻の順序関係に基づき SigningTime およびタイムスタンプを生成できなければならない	MUST
検証要件			
	ETSI TS 101 733 v1.7.3 C.3.6 に基づく時刻の順序関係の検証ができなければならない		MUST
	タイムスタンプおよび SigningTime の時刻が何らかの方法で表示されることが望ましい		RECOMMEND

3.6.8 <ON-T-ATTR-CONTENTREFERENCE>

ContentReference を持つ CAdES-T の対応を確認する。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		ContentReference が含まれなければならない	MUST
検証要件			
	ContentReference で参照される署名との一致検証が行えるか、もしくは、ContentReference の有無および記載される内容が何らかの方法で目視確認できなければならない。		MUST

3.6.9 <ON-T-ATTR-CONTENTIDENTIFIER>

ContentIdentifier を持つ CAdES-T の対応を確認する。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		ContentIdentifier が含まれなければならない	MUST
検証要件			
	ContentIdentifier の有無および記載される内容が何らかの方法で目視確認できなければならない。		MUST

3.6.10 <ON-T-ATTR-COUNTERSIGNATURE>

CounterSignature を持つ CAdES-T の対応を確認する。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		署名者 EE-ON-SIG-ECOMSAMPLE-OK による CounterSignature が含まれなければならない	MUST
		その CounterSignature には SignatureTimeStamp が含まれなければならない	MUST
検証要件			
	CounterSignature に対して、「共通の要件」に記載されたものと同等の検証を行わなければならない		MUST

3.6.11 <ON-T-ATTR-ESSCERTV2>

他の SigningCertificate 属性の代わりに ESSSigningCertificateV2 属性を持つ CAdES-T の対応を確認する。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。

生成要件			
	署名属性、非署名属性		
		ESSSigningCertificateV2 が含まれなければならない	MUST
		ESSSigningCertificateV2 で用いられるハッシュアルゴリズムは SHA1 より強固なアルゴリズムでなければならない。	MUST
		ESSSigningCertificateV2 で用いられるハッシュアルゴリズムは SHA-256 もしくは SHA-512 を推奨する。	RECOMMEND
検証要件			
	署名者証明書と ESSSigningCertificateV2 との一致検証を行わなければならない。		MUST

3.7 CAdES-A **基本テストケース** (ON-A-BASIC)

本テストケースではアーカイブ署名(CAdES-A)への対応を確認する。本テストケースに含まれるテスト項目を次に示す。

3.7.1 <ON-A-BASIC-A1-ATTACHED>

内包署名による第一世代の CAdES-A への対応を確認する。

<ON-T-BASIC-ATTACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		署名者証明書の検証に必要な証明書情報を持つ CertificateValues、CompleteCertificateRefs を含まなければならない	MUST
		ETSI TS 101 733 v1.7.3 に基づきハッシュ計算された ArchiveTimeStamp が 1 つ含まれなければならない	MUST
		最新の ArchiveTimeStamp 以外のタイムスタンプトークンの TSA 証明書の検証に必要な情報はタイムスタンプトークンの certificates および crls フィールドに格納することを推奨する	RECOMMEND
		タイムスタンプトークンに TSA 証明書の検証情報を含めない場合、生成結果の署名データと同じディレクトリに検証データを置かなければならない。	MUST

検証要件		
	署名者証明書は CertificateValues、RevocationValues、CompleteCertificateRefs、CompleteRevocationRefs の検証情報を用い SignatureTimeStamp の時刻における有効性を検証しなければならない	MUST
	タイムスタンプトークン中に検証情報があれば、これを用いて証明書検証することを推奨する	RECOMMEND

3.7.2 <ON-A-BASIC-A1-DETACHED>

分離署名による第一世代の CAdES-A への対応を確認する。

<ON-T-BASIC-DETACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		署名者証明書の検証に必要な証明書情報を持つ CertificateValues、CompleteCertificateRefs を含まなければならない	MUST
		ETSI TS 101 733 v1.7.3 に基づきハッシュ計算された ArchiveTimeStamp が 1 つ含まれなければならない	MUST
		最新の ArchiveTimeStamp 以外のタイムスタンプトークンの TSA 証明書の検証に必要な情報はタイムスタンプトークンの certificates および crls フィールドに格納することを推奨する	RECOMMEND
		タイムスタンプトークンに TSA 証明書の検証情報を含めない場合、生成結果の署名データと同じディレクトリに検証データを置かなければならない。	MUST
検証要件			
	署名者証明書は CertificateValues、RevocationValues、CompleteCertificateRefs、CompleteRevocationRefs の検証情報を用い SignatureTimeStamp の時刻における有効性を検証しなければならない		MUST
	タイムスタンプトークン中に検証情報があれば、これを用いて証明書検証することを推奨する		RECOMMEND

3.7.3 <ON-A-BASIC-A2-ATTACHED>

内包署名による第二世代の CAdES-A への対応を確認する。

<ON-A-BASIC-A1-ATTACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		ETSI TS 101 733 v1.7.3 に基づきハッシュ計算された ArchiveTimeStamp が 2 つ含まれなければならない	MUST
		ArchiveTimeStamp の時間間隔は 1 日程以上空けることを推奨する	RECOMMEND

3.7.4 <ON-A-BASIC-A3-ATTACHED>

<ON-A-BASIC-A2-ATTACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		ETSI TS 101 733 v1.7.3 に基づきハッシュ計算された ArchiveTimeStamp が 3 つ含まれなければならない	MUST

3.8 CAdES-A オプショナル属性テストケース (ON-A-ATTR)

3.8.1 <ON-A-ATTR-A1-ARCTSV1-ATTACHED>

RFC 3126 もしくは ETSI TS 101 733 v1.4.0 に基づく ArchiveTimeStampV1 への対応を確認する。

<ON-A-BASIC-A1-ATTACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		ETSI TS 101 733 v1.7.3 の ArchiveTimeStampV2 の代わりに RFC 3126 もしくは ETSI TS 101 733 v1.4.0 で規定された旧バージョンの ArchiveTimeStamp(V1)を 1 つ含まなければならない。	MUST
		SignaturePolicyIdentifier を含まなければならない。	MUST
		署名ポリシは "./TARGET-SIGPOL-RFC3125.der" を用いなければならない。	MUST
検証要件			
	RFC 3126 もしくは ETSI TS 101 733 v1.4.0 に基づき旧バージョンの ArchiveTimeStamp(V1)の検証ができなければならない。		MUST
	署名ポリシ "./TARGET-SIGPOL-RFC3125.der"に基づいて検証ができなければならない。		MUST

3.8.2 <ON-A-ATTR-A1-TIMESTAMPEDCERTSCRLS>

TimestampedCertsCRLs を持つ CAdES-A への対応を確認する。

<ON-A-BASIC-A1-ATTACHED>の要件を基礎とする。			
生成要件			
	署名属性、非署名属性		
		ETSI TS 101 733 v1.7.3 に基づいた TimestampedCertsCRLs を含まなければならない	MUST

検証要件		
	ETSI TS 101 733 v1.7.3 に基づき TimestampedCertsCRLs を検証しなければならない	MUST

3.8.3 <ON-A-ATTR-A1-ESCTIMESTAMP>

ESCTimeStamp を持つ CAdES-A への対応を検証する。

<ON-A-BASIC-A1-ATTACHED>の要件を基礎とする。		
生成要件		
	署名属性、非署名属性	
	ETSI TS 101 733 v1.7.3 に基づいた ESCTimeStamp を含まなければならない	MUST
検証要件		
	ETSI TS 101 733 v1.7.3 に基づき TimestampedCertsCRLs を検証しなければならない	MUST

3.9 検証の際、インターネット接続環境を持たない場合

検証の際にインターネットに HTTP(TCP/80)で接続できない場合には、http//ecom-es-test.ath.cx/repository/ にあるファイルをダウンロードし、検証に用いてもよい。

3.10 合否判定

本テストにおいては、以下の項目についての合否判定を行う。

- CAdES-T/XAdES-T の生成
- CAdES-T/XAdES-T の検証
- CAdES-A/XAdES-A の生成
- CAdES-A/XAdES-A の検証

この結果は「JIS 適合性宣言書」の「プロファイル実装範囲」を記入するのに参考とすることができる。

3.10.1 生成機能の合否判定基準

- **少なくとも 1 つの生成したテスト項目において、検証を行った 80%以上の実装で検証成功であれば「生成合格」とする。**
- **上記以外を「生成不合格」とする。**
- **但し、標準と照らして不備がある場合には、メーリングリスト上で議論し、問題点を明らかにした上で事務局の協議により「合格」または「不合格」とすることができる。**

3.10.2 検証機能の合否判定基準

- **少なくとも一つのテスト項目に対する参加企業の生成結果に対し、80%以上他社が検証成功としているテスト項目署名データに対して、全て検証成功していれば「検証合格」とする。**

- **上記以外を「検証不合格」とする。**
- **共通データ標準準拠性テスト(旧オフラインテスト)で不合格ならば不合格とする。**
- **但し、標準と照らして不備がある場合には、メーリングリスト上で議論し、問題点を明らかにした上で事務局の協議により「合格」または「不合格」とすることができる。**

4 付録：実験用データプロファイル

本節では実証実験で用いられるデータのプロファイルを示す。

4.1 実験用長期署名フォーマットデータのプロファイル

長期署名フォーマットのデータは全て CMS SignedData フォーマットに基づいており、その中でフォーマット毎に signedAttributes フィールドおよび unsignedAttributes フィールドに必要となる CMS 属性が異なる。

4.1.1 BES (Basic Electronic Signature)

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	内包/分離はテスト項目に依存
certificates	署名者証明書のみ
crls	無
signerInfos	有(要素数=1)
signerInfo	160bit
version	v3(3)
sid	署名者証明書のsubjectKeyIdentifier拡張の値と同じ
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=data(1.2.840.113549.1.7.1)
messageDigest	有
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	無

4.1.2 EPES (Explicit Policy-based Electronic Signature)

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	内包/分離はテスト項目に依存
certificates	署名者証明書のみ
crls	無
signerInfos	有(要素数=1)
signerInfo	160bit
version	v3(3)
sid	署名者証明書のsubjectKeyIdentifier拡張の値と同じ
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=data(1.2.840.113549.1.7.1)
messageDigest	有
sigPolicyId	有(SHA1フィンガープリント)
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	無

4.1.3 ES-T

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	内包/分離はテスト項目に依存
certificates	署名者証明書のみ
crls	無
signerInfos	有(要素数=1)
signerInfo	160bit
version	v3(3)
sid	署名者証明書のsubjectKeyIdentifier拡張の値と同じ
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=data(1.2.840.113549.1.7.1)
messageDigest	有
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	有
signatureTimeStamp	トークンは実験用データプロファイルに従う

4.1.4 ES-X Long

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	内包/分離はテスト項目に依存
certificates	署名者証明書のみ
crls	無
signerInfos	有(要素数=1)
signerInfo	160bit
version	v3(3)
sid	署名者証明書のsubjectKeyIdentifier拡張の値と同じ
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=data(1.2.840.113549.1.7.1)
messageDigest	有
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	有
signatureTimeStamp	トークンは実験用データプロファイルに従う(検証情報を含む)
completeCertificateRefs	ECOMプロファイルに従う
completeRevocationRefs	ECOMプロファイルに従う
certificateValues	ECOMプロファイルに従う
revocationValues	ECOMプロファイルに従う

4.1.5 ES-A (**第一世代**)

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	内包/分離はテスト項目に依存
certificates	署名者証明書のみ
crls	無
signerInfos	有(要素数=1)
signerInfo	160bit
version	v3(3)
sid	署名者証明書のsubjectKeyIdentifier拡張の値と同じ
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=data(1.2.840.113549.1.7.1)
messageDigest	有
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	有
signatureTimeStamp	トークンは実験用データプロファイルに従う(検証情報を含む)
completeCertificateRefs	ECOMプロファイルに従う
completeRevocationRefs	ECOMプロファイルに従う
certificateValues	ECOMプロファイルに従う
revocationValues	ECOMプロファイルに従う
archiveTimeStamp	トークンは実験用データプロファイルに従う

4.1.6 ES-A (第二世代以降)

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	内包/分離はテスト項目に依存
certificates	署名者証明書のみ
crls	無
signerInfos	有(要素数=1)
signerInfo	160bit
version	v3(3)
sid	署名者証明書のsubjectKeyIdentifier拡張の値と同じ
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=data(1.2.840.113549.1.7.1)
messageDigest	有
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	有
signatureTimeStamp	トークンは実験用データプロファイルに従う(検証情報を含む
completeCertificateRefs	ECOMプロファイルに従う
completeRevocationRefs	ECOMプロファイルに従う
certificateValues	ECOMプロファイルに従う
revocationValues	ECOMプロファイルに従う
archiveTimeStamp1	トークンは実験用データプロファイルに従う(検証情報を含む
archiveTimeStamp2 ...	トークンは実験用データプロファイルに従う(署名延長)

4.2 実験用タイムスタンプトークンのプロファイル

4.2.1 TimeStampToken

TimeStampToken は CMS SignedData の構造となっている。ECOM プロファイルの ES-X Long, ES-A の検証情報の格納方法の定義に従い、certificates, crls フィールドに検証情報を持つ場合がある。

フィールド	値
version	v3(3)
digestAlgorithms	{ SHA1 }
encapContentInfo	前述TSTInfoプロファイルに従う
certificates	ECOMプロファイルにより検証情報としてTSA証明書およびパスを含みうる
crls	ECOMプロファイルにより検証情報として全てのCRLを含みうる
signerInfos	有(要素数=1)
signerInfo	160bit
version	v1(1)
sid	TSA証明書のIssuerAndSerialNumber
digestAlgorithm	SHA1
signedAttrs	有
contentInfo	=tSTInfo(1.2.840.113549.1.9.16.1.4)
messageDigest	有
eSSSigningCertificate	有(発行者名、シリアル番号、SHA1フィンガープリント)
signatureAlgorithm	SHA1withRSA
signature	署名値
unsignedAttrs	無

4.2.2 TSTInfo

フィールド	値
バージョン	v1(1)
policy	TSAPolicyId=0.1.2.3.4.5
messageImprint	有
hashAlgorithm	SHA1
hashedMessage	160bit
serialNumber	値はTSA証明書のシリアル番号と同じとする(※1)
genTime	GeneralizedTime(小数点以下最大3桁を含む)
accuracy	500ミリ秒
ordering	TRUE
nonce	0x1234567890(固定)
tsa	directoryName=TSA証明書の主体者名
extensions	無

テスト項目番号 20012 以降、70003 以降は messageImprint のハッシュアルゴリズムに SHA-256 を使用する。

※1：本来は該当 TSA より発行されたトークンのシリアル番号となるがテスト上 TSA からは 1 つのトークンしか発行されないので便宜上 TSA 証明書のシリアル番号と同じとし、テスト項目番号がすぐにわかるようにする。

4.3 実験用証明書のプロファイル

4.3.1 実験用証明書の共通のプロファイル

フィールド	値
バージョン	V3
シリアル番号	5バイトのASN.1 INTEGER(※1)
署名アルゴリズム	SHA1withRSA
発行者DN	PrintableString(全てのDNはPrintableStringとする)
有効期限	UTCTime(使用される時刻は2000/1/1 0:00:00～2035/12/31 23:59:59とする)
主体者DN	PrintableString
公開鍵情報	有
X.509拡張	有
keyUsage	有

4.3.2 RootCA 証明書のプロファイル

フィールド	値	クリティカル
バージョン	V3	
シリアル番号	有	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
有効期限	UTCTime	
主体者DN	PrintableString	
公開鍵情報	2048bit	
X.509拡張	有	
keyUsage	CertSign, CRLSign	TRUE
subjectKeyIdentifier	有 SHA1-160bit	FALSE
basicConstraints	有	TRUE
CAフラグ	TRUE	-

4.3.3 SubCA 証明書のプロファイル

フィールド	値	クリティカル
バージョン	V3	
シリアル番号	有	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
有効期限	UTCTime	
主体者DN	PrintableString	
公開鍵情報	1024bit	
X.509拡張	有	
keyUsage	CertSign, CRLSign	TRUE
subjectKeyIdentifier	有 SHA1-160bit	FALSE
authorityKeyIdentifier	有	FALSE
keyIdentifier	有 SHA1-160bit	-
basicConstraints	有	TRUE
CAフラグ	TRUE	-
cRLDistributionPoints	有	FALSE
DistPt.fullName.URI	http://配布ホスト/**/*.crl	-

4.3.4 署名者用 End Entity 証明書のプロファイル

フィールド	値	クリティカル
バージョン	V3	
シリアル番号	有	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
有効期限	UTCTime	
主体者DN	PrintableString	
公開鍵情報	1024bit	
X.509拡張	有	
keyUsage	digitalSignature, nonRepudiation	TRUE
basicConstraints	有(空シーケンス)	FALSE
CAフラグ	無	-
subjectKeyIdentifier	有 SHA1-160bit	FALSE
authorityKeyIdentifier	有	FALSE
keyIdentifier	有 SHA1-160bit	-
cRLDistributionPoints	有	FALSE
DistPt.fullName.URI	http://配布ホスト/**/*.crl	-

4.3.5 TSA 証明書のプロファイル

フィールド	値	クリティカル
バージョン	V3	
シリアル番号	有	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
有効期限	UTCTime	
主体者DN	PrintableString	
公開鍵情報	1024bit	
X.509拡張	有	
keyUsage	digitalSignature, nonRepudiation	TRUE
subjectKeyIdentifier	有 SHA1-160bit	FALSE
authorityKeyIdentifier	有	FALSE
keyIdentifier	有 SHA1-160bit	-
extKeyUsage	1.3.6.1.5.5.7.3.8(timeStamping)	TRUE
cRLDistributionPoints	有	FALSE
DistPt.fullName.URI	http://配布ホスト/**/*.crl	-

4.3.6 オンライン TSA 用 RootCA 証明書のプロファイル

フィールド	値	クリティカル
バージョン	V3	
シリアル番号	有	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
有効期限	UTCTime	
主体者DN	PrintableString	
公開鍵情報	2048bit	
X.509拡張	有	
keyUsage	CertSign, CRLSign	TRUE
subjectKeyIdentifier	有 SHA1-160bit	FALSE
authorityKeyIdentifier	有	FALSE
keyIdentifier	有 SHA1-160bit	-
authorityCertIssuer	directoryName(PrintableString)	-
authorityCertSerialNumber	(0x00)	-
basicConstraints	有	FALSE
CAフラグ	TRUE	-

4.3.7 オンライン TSA 証明書のプロファイル

フィールド	値	クリティカル
バージョン	V3	
シリアル番号	有	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
有効期限	UTCTime	
主体者DN	PrintableString	
公開鍵情報	1024bit	
X.509拡張	有	
keyUsage	digitalSignature, nonRepudiation	TRUE
subjectKeyIdentifier	有 SHA1-160bit	FALSE
authorityKeyIdentifier	有	FALSE
keyIdentifier	有 SHA1-160bit	-
authorityCertIssuer	directoryName(PrintableString)	-
authorityCertSerialNumber	(0x00)	-
basicConstraints	有(空シーケンス)	FALSE
CAフラグ	無	-
extKeyUsage	1.3.6.1.5.5.7.3.8(timeStamping)	TRUE
cRLDistributionPoints	有	FALSE
DistPt.fullName.URI	https://配布ホスト/**/*.crl	-

4.3.8 オンライン/オフライン/署名者/TSA 共通 CRL プロファイル

フィールド	値	クリティカル
バージョン	V2(1)	
署名アルゴリズム	SHA1withRSA	
発行者DN	PrintableString	
thisUpdate	UTCTime	
nextUpdate	UTCTime	
revokedCertificate		
userCertificate	失効する証明書のシリアル番号	
revocationDate	UTCTime	
crlEntryExtensions		
cRLReason		FALSE
X.509拡張	有	
cRLNumber		FALSE

4.4 オフラインテスト用署名ポリシのプロファイル

フィールド	値
signPolicyHashAlg	SHA1
signPolicyInfo	有
signPolicyIdentifier	1.2.3.4.5*
dateOfIssue	2001.01.01
policyIssuerName	ou=SIGNATURE-POLICY-AUTHORITY,o=ECOM,c=JP
fieldOfApplication	"for …" テスト用ポリシーとしてのメモ
signatureValidationPolicy	
signingPeriod	
notBefore	有
notAfter	無
commonRules	
signerAndVerifierRules[0]	
signerRules	
externalSignedData?	無
mandatedSignedAttr	messageDigest, sigPolicyId
mandatedUnsignedAttr	signatureTimeStamp
mandatedCertificateRef?	無
mandatedCertificateInfo?	無
signPolExtensions?	無
verifierRules	
mandatedUnsignedAttr	空シーケンス
signPolExtensions?	無
signingCertTrustCondition[1]	
signerTrustTrees	署名者用CA証明書
signerRevReq	EE=crlCheck(0), CA=crlCheck(0)
timeStampTrustCondition[2]	
ttsCertificateTrustTrees[0]?	TSA用CA証明書
ttsRevReq[1]?	EE=crlCheck(0), CA=crlCheck(0)
attributeTrustCondition[3]	無
algorithmConstraintSet[4]	無
commitmentRules	空シーケンス
signPolExtensions	無
signPolExtensions	無
signPolicyHash	無

4.5 オンラインテスト用署名ポリシのプロファイル

フィールド	値
signPolicyHashAlg	SHA1
signPolicyInfo	有
signPolicyIdentifier	1.2.3.4.5*
dateOfIssue	2001.01.01
policyIssuerName	ou=SIGNATURE-POLICY-AUTHORITY,o=ECOM,c=JP
fieldOfApplication	"for …" テスト用ポリシーとしてのメモ
signatureValidationPolicy	
signingPeriod	
notBefore	有
notAfter	無
commonRules	
signerAndVerifierRules[0]	
signerRules	
externalSignedData?	無
mandatedSignedAttr	messageDigest, sigPolicyId
mandatedUnsignedAttr	signatureTimeStamp
mandatedCertificateRef?	無
mandatedCertificateInfo?	無
signPolExtensions?	無
verifierRules	
mandatedUnsignedAttr	空シーケンス
signPolExtensions?	無
signingCertTrustCondition[1]	
signerTrustTrees	署名者用CA証明書
signerRevReq	EE=eitherCheck(3), CA=eitherCheck(3)
timeStampTrustCondition[2]	無
attributeTrustCondition[3]	無
algorithmConstraintSet[4]	無
commitmentRules	空シーケンス
signPolExtensions	無
signPolExtensions	無
signPolicyHash	無