2007 年

ECOM 長期署名フォーマット

相互運用実証実験

XAdES 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

変更履歴

版	更新日	内容
V0.5 draft	2007/1/10	初版発行
	2007/2/19	タイプミスの修正
V0.6 draft	2007/2/28	V1.3.1 の記述が残っている部分を修正。 - リスト１ CMS の記述が残っている部分を修正 - ES-T という記述を XAdES-T へ修正 - 「属性」という記述を「要素」という記述へ修正
V1.0	2007/03/22	以下のテストケースを追加 - 70011 ESA1-ATTACH-ATS-MI-UNMATCH-NG - 70012 ESA1-DETACH-ATS-MI-UNMATCH-NG - 70013 ESA2-ATTACH-NORMAL-OK - 70014 ESA2-ATTACH-ATS-MI-UNMATCH-NG - 70015 ESA2-DETACH-NORMAL-OK - 70016 ESA2-DETACH-ATS-MI-UNMATCH-NG 付録に以下を追加 - 実験用長期署名フォーマットデータプロファイル - 実験用タイムスタンプトークンのプロファイル - 実験用証明書のプロファイル
V1.1	2007/03/28	- テスト項目 10004 をオプショナル項目に移動し、説明を変更。期待値を「有効」から「-」に変更。 - オフラインテストケース<OFF-T-5>の成功条件からテスト項目 10004 を削除
V.1.2 draft	2007/09/27	2007 年オンラインテストについて追加
	2007/09/28	表記を CAdES テストケースに合わせるよう修正
	2007/10/02	オンラインテストについて以下の項目を追加 ・ 合否判定基準 ・ 実施手順詳細 ・ テスト項目における必要なプロパティの表 KeyInfo に関するコメントの反映
	2007/10/05	・ オンラインテストの目視確認について追記 ・ オンラインテスト誤植の修正

	2007/10/09	・ オンラインテスト共通要件のプロパティの補足 ・ オフラインテストの誤植大幅修正
	2007/10/11	・ 3.2.2 署名の入力ファイルを追記
V1.2	2007/10/11	・ V1.2 リリース

1. はじめに

本仕様書は、次世代電子商取引推進協議会(ECOM)の電子署名ワーキンググループの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において実施される実証実験のXAdES長期署名フォーマットに関するテスト内容について記述したものである。

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 1-1）。

表 1-1：表記

表記	説明
<…>	テスト項目
<…OK>	検証結果の期待値が有効であるテスト項目
<…NG>	検証結果の期待値が無効であるテスト項目
[…]	参考文献

1.2. テストの構成

CAdES テストケース設計書に記述されたものと同様の構成とする。

2. オフライン共通データ検証テストカテゴリ

相互運用テストでは、長期署名フォーマットのプロファイルに関する JIS 原案への準拠性を確認する。テストツールより生成された XAdES フォーマットのデータ(XAdES-T、XAdES-A)、証明書、CRL、署名対象データをもとに、実験者のシステムや製品での検証結果が期待値と一致するかどうかを確認する。

2.1. テストの準備

テスト実施する際は、以下の項目の準備が必要となる。

・ CRL の設定

証明書検証時にオンラインで 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

本節では、テストの実施時の設定や条件などを説明する。

・ 署名対象データの設定

内包型署名の場合は、署名対象文字列を”aaa”とし XML 署名の形式として enveloping 形式で署名対象文字列を指定する。ただし、XML 署名の Object 要素として格納するため、base64 で encode された値(YWFh)で格納するもとする。内包型署名の場合の XML 署名文書の例を以下に示す（リスト 1)。

リスト 1：内包型署名の場合の XML 署名文書の例

```
<?xml version="1.0" encoding="UTF-8" ?>
<ds:Signature Id="Signature-ID1" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo> ……</ds:SignedInfo>
  <ds:SignatureValue>……</ds:SignatureValue>
  <ds:KeyInfo >……</ds:KeyInfo >
  <ds:Object Encoding="http://www.w3.org/2000/09/xmldsig#base64"
            Id="signdata">YWFh</ds:Object>
  <ds:Object xmlns:xa="http://uri.etsi.org/01903/v1.3.2#">……</ ds:Object >
</ds:Signature>
```

base64 でエンコードされたテキスト”aaa”

分離署名の場合には、'TARGET_BBB.bin”(ファイルの内容は、0x01-0x09,0x00 の繰り返しで 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、各証明書や 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

テストスィ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の命名規則は、テストケース名と XAdES のバージョンで表され、”<テストケース名>-V132.xml”というファイル名となる。また、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

実施すべき全てのテスト項目について実施する。署名対象データのハッシュ値を base64 でエンコードしたものは以下の通り。

“aaa” ：**fiQN50+x7Qj6CNOAY/amqRRiqBU=**

TARGET_BBB.bin ：**gpGOa0wroxRJGyeXw7tHFbrgtxM=**

2.3. テストデータに共通の情報

・ 有効期間の時刻は、例外ケースを除き 00:00:00 から 23:59:59 に統一する。

・ 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 に統一する

・ 時刻の表記は、特に断りのない限り、UTC 時刻とする。

2.4. XAdES-T フォーマット標準テスト項目

2.4.1. <EST-ATTACH-NORMAL-OK 10001>

署名者証明書および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、XAdES-T データが有効であることを検証する。表 2-1 にテスト結果の期待値とテスト時に利用する時刻や証明書、CRL に関するテストパラメータを示す。

表 2-1：<EST-ATTACH-NORMAL-OK 10001>におけるテスト結果の期待値とテストパラメータ

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	属性なし
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期間	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2001.1.3 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 00:00:00～2001.1.3 23:59:59

2.4.2. <EST-ATTACH-EXPIERED-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 XAdES-T データが無効であることを検証する。表 2-2 にテスト結果の期待値とテスト時に利用する時刻や証明書、CRL に関するテストパラメータを示す。

表 2-2：<EST-ATTACH-EXPIERED-NG 10002>におけるテスト結果の期待値とテストパラメータ

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	属性なし
署名タイムスタンプの時刻	2001.1.3 12:00:00
署名者証明書の有効期間	2001.1.1 00:00:00～2001.1.1 23:59:59
署名者証明書の検証 CRL	2001.1.2 00:00:00～2000.1.2 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

2.4.3. <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、XAdES-T データが無効であることを検証する。表 2-3 にテスト結果の期待値とテスト時に利用する時刻や証明書、CRL に関するテストパラメータを示す。

表 2-3：<EST-ATTACH-REVOKED-NG 10003>におけるテスト結果の期待値とテストパラメータ

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
署名者証明書の有効期間	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 中の失効日時	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

2.4.4. <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、サイニングタイム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、XAdES-T データが無効であることを検証する。

表 2-4：<EST-ATTACH-SIGTS-REVOKED-NG 10005>におけるテスト結果の期待値とテストパラメータ

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
署名者証明書の有効期間	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

2.4.5. <EST-ATTACH-ES-SIG-REVOKED-NG 10006>

XAdES-T フォーマットの Signature 要素にある署名値が改ざんされていた場合に無効であることを検証する。

表 2-5：<EST-ATTACH-EE-SIG-FORGED-NG 10006>におけるテスト結果の期待値とテストパラメータ

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	属性なし
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期間	2001.1.1～2035.12.31
署名者証明書の検証 CRL	2001.1.2 00:00:00～2002.1.4 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

2.4.6. <EST-ATTACH-SIGTS-SIG-FORGED-NG 10007>

XAdES-T フォーマットの SignatureTimeStamp 要素中の 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ざんされていた場合に無効であることを検証する。

表 2-6：<EST-ATTACH-SIGTS-SIG-FORGED-NG 10007>におけるテスト結果の期待値とテストパラメータ

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	属性なし
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期間	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

2.4.7. <EST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG 10008>

XAdES-T フォーマットの SignedInfo 要素の Reference 要素の DigestValue 要素内のハッシュ値が改ざんされていた場合に無効であることを検証する。

表 2-7：<EST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG 10008>におけるテスト結

果の期待値とテストパラメータ

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	属性なし
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期間	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

2.4.8. <EST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG 10009>

XAdES-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 の中の MessageDigest 属性の値が改ざんされていた場合に無効であることを検証する。

表 2-8：<EST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG 10009>におけるテスト結果の期待値とテストパラメータ

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	属性なし
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期間	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

2.4.9. <EST-DETACH-NORMAL-OK 10010>

署名対象文書に対して分離署名を行った XAdES-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。

表 2-9：<EST-DETACH-NORMAL-OK 10010>におけるテスト結果の期待値とテストパラメータ

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	属性なし

署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期間	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 00:00:00～2001.1.2 23:59:59

2.5. XAdES-T フォーマットオプショナルテスト項目

2.5.1. <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、サイニングタイム要素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において、XAdES-T フォーマットを検証する。

なお、XAdES V1.3.2 では、SigningTime 要素の時刻と署名タイムスタンプ時刻の前後関係を規定している。しかし、そのまま実装すると運用上の課題が発生する恐れがあるので、テスト項目に期待値は特に定めない。

表 2-10：<EST-ATTACH-SIGTIME-REVOKED-OK 10004>におけるテスト結果の期待値とテストパラメータ

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	2001.1.4 12:00:00
署名タイムスタンプの時刻	2001.1.1 12:00:00
署名者証明書の有効期間	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	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	2001.1.3 00:00:00～2001.1.3 23:59:59

2.6. XAdES-A フォーマット標準テスト項目

2.6.1. <ESA1-ATTACH-NORMAL-OK 70001>

アーカイブタイムスタンプが一つ付与された XAdES-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。

表 2-11：<ESA 1-ATTACH-NORMAL-OK 70001>におけるテスト結果の期待値とテストパラメータ

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
署名者証明書の有効期間	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
Archiveタイムスタンプ1の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

2.6.2. <ESA1-DETACH-NORMAL-OK 70002>

アーカイブタイムスタンプが一つ付与された XAdES-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。

表 2-12：<ESA1-DETACH-NORMAL-OK 70002>におけるテスト結果の期待値とテストパラメータ

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
署名者証明書の有効期間	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
Archiveタイムスタンプ1の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

2.6.3. <XAdESA1-ATTACH-ATS-MI-UNMATCH-NG 70011>

アーカイブタイムスタンプ要素を一つ含む XAdES-A フォーマットでハッシュ対象より計算したハッシュ値とアーカイブタイムスタンプトークンの TSTInfo の MessageImprint の値が一致せず、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。

表 2-13：＜XAdESA1-ATTACH-ATS-MI-UNMATCH-NG 70011＞におけるテスト結果の期待値とテストパラメータ

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
署名者証明書の有効期間	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

2.6.4. <ESA1-DETACH-ATS-MI-UNMATCH-NG 70012>

アーカイブタイムスタンプ要素を一つ含む XAdES-A フォーマットでハッシュ対象より計算したハッシュ値とアーカイブタイムスタンプトークンの TSTInfo の MessageImprint の値が一致せず、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。

表 2-14：<ESA1-DETACH-ATS-MI-UNMATCH-NG 70012>におけるテスト結果の期待値とテストパラメータ

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
署名者証明書の有効期間	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

2.6.5. <ESA2-V173-ATTACH-NORMAL-OK 70013>

二世代目のアーカイブタイムスタンプが付与された XAdES-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。

表 2-15：<ESA2-V173-ATTACH-NORMAL-OK 70013>のテスト結果の期待値とテストパラメータ

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
署名者証明書の有効期間	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

2.6.6. <ESA2-ATTACH-ATS-MI-UNMATCH-NG 70014>

二世代目のアーカイブタイムスタンプが付与された XAdES-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。

表 2-16：＜ESA2-ATTACH-ATS-MI-UNMATCH-NG 70014＞のテスト結果の期待値とテストパラメータ

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
署名者証明書の有効期間	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

2.6.7. <ESA2-DETACH-NORMAL-OK 70015>

二世代目のアーカイブタイムスタンプが付与された XAdES-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。

表 2-17：＜ESA2-DETACHE-NORMAL-OK 70015＞のテスト結果の期待値とテストパラメータ

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

2.6.8. <ESA2-DETACH-ATS-MI-UNMATCH-NG 70016>

二世代目のアーカイブタイムスタンプが付与された XAdES-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。

表 2-18：＜ESA2-DETACH-ATS-MI-UNMATCH-NG 70016＞のテスト結果の期待値とテストパラメータ

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

2.7. XAdES-T 標準テストケース

本節では XAdES-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。

2.7.1. <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：以下テスト項目が全て期待値通りになること。	
10001	EST-ATTACH-NORMAL-OK

2.7.2. <OFF-T-2>

テストケース名	OFF-T-2
XAdES-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：以下テスト項目が全て期待値通りになること。	
10001	EST-ATTACH-NORMAL-OK
10002	EST-ATTACH-EXPIRED-NG

2.7.3. <OFF-T-3>

テストケース名	OFF-T-3
XAdES-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：以下テスト項目が全て期待値通りになること。	
10001	EST-ATTACH-NORMAL-OK
10003	EST-ATTACH-REVOKED-NG

2.7.4. <OFF-T-4>

テストケース名	OFF-T-4
XAdES-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扱える	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	EST-ATTACH-NORMAL-OK
10002	EST-ATTACH-EXPIRED-NG
10003	EST-ATTACH-REVOKED-NG

2.7.5. <OFF-T-5>

テストケース名	OFF-T-5
XAdES-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：以下テスト項目が全て期待値通りになること。	
10001	EST-ATTACH-NORMAL-OK
10002	EST-ATTACH-EXPIRED-NG
10003	EST-ATTACH-REVOKED-NG
10005	EST-ATTACH-SIGTS-REVOKED-NG

2.7.6. <OFF-T-6>

テストケース名	OFF-T-6
XAdES-T フォーマットの Signature 要素内の署名値の改ざんを検知できる。	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	EST-ATTACH-NORMAL-OK
10006	EST-ATTACH-ES-SIG-FORGED-NG

2.7.7. <OFF-T-7>

テストケース名	OFF-T-7
XAdES-T フォーマットの署名タイムスタンプトークンの SignerInfo の署名値の改ざんを検知できる。	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	EST-ATTACH-NORMAL-OK
10007	EST-ATTACH-SIGTS-FORGED-NG

2.7.8. <OFF-T-8>

テストケース名	OFF-T-8
XAdES-T フォーマットの DigestValue 要素のハッシュ値の改ざんを検知できる。	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	EST-ATTACH-NORMAL-OK
10008	EST-ATTACH-ES-MESSAGEDIGEST-FORGED-NG

2.7.9. <OFF-T-9>

テストケース名	OFF-T-9
XAdES-T フォーマットの署名タイムスタンプトークンの MessageDigest のハッシュ値の改ざんを検知できる。	
成功条件：以下テスト項目が全て期待値通りになること。	
10001	EST-ATTACH-NORMAL-OK
10009	EST-ATTACH-SIGTSTST-MESSAGEDIGEST-FORGED-NG

2.7.10. <OFF-T-10>

テストケース名	OFF-T-10
分離署名の XAdES-T のフォーマットを扱える	
成功条件：以下テスト項目が全て期待値通りになること。	
10010	EST-DETACH-NORMAL-OK

2.8. XAdES-A 標準テストケース

2.8.1. <OFF-A-1>

テストケース名	OFF-A-1
内包署名の第一世代の XAdES-A フォーマットを扱うことができる	
成功条件：以下テスト項目が全て期待値通りになること。	
70001	ESA1-ATTACH-NORMAL-OK
70011	ESA1-ATTACH-ATS-MI-UNMATCH-NG

2.8.2. <OFF-A-2>

テストケース名	OFF-A-2
分離署名の第一世代の XAdES-A フォーマットを扱うことができる	
成功条件：以下テスト項目が全て期待値通りになること。	
70002	ESA1-DETACH-NORMAL-OK
70012	ESA1-DETACH-ATS-MI-UNMATCH-NG

2.8.3. <OFF-A-3>

テストケース名	OFF-A-3
内包署名の第二世代の XAdES-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	
70013	ESA2-ATTACH-NORMAL-OK
70014	ESA2-ATTACH-ATS-MI-UNMATCH-NG

2.8.4. <OFF-A-4>

テストケース名	OFF-A-4
分離署名の第二世代の XAdES-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	
70015	ESA2-DETACH-NORMAL-OK

70016	ESA2-DETACH-ATS-MI-UNMATCH-NG

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)

本テストでは、実験参加組織の持つ実装により、テスト項目で定める生成要件に従い XAdES 署名データを生成し、テスト項目で定める検証要件に従い他の実装が互いに検証を行う実装間の相互運用性を確認するためのテストである。

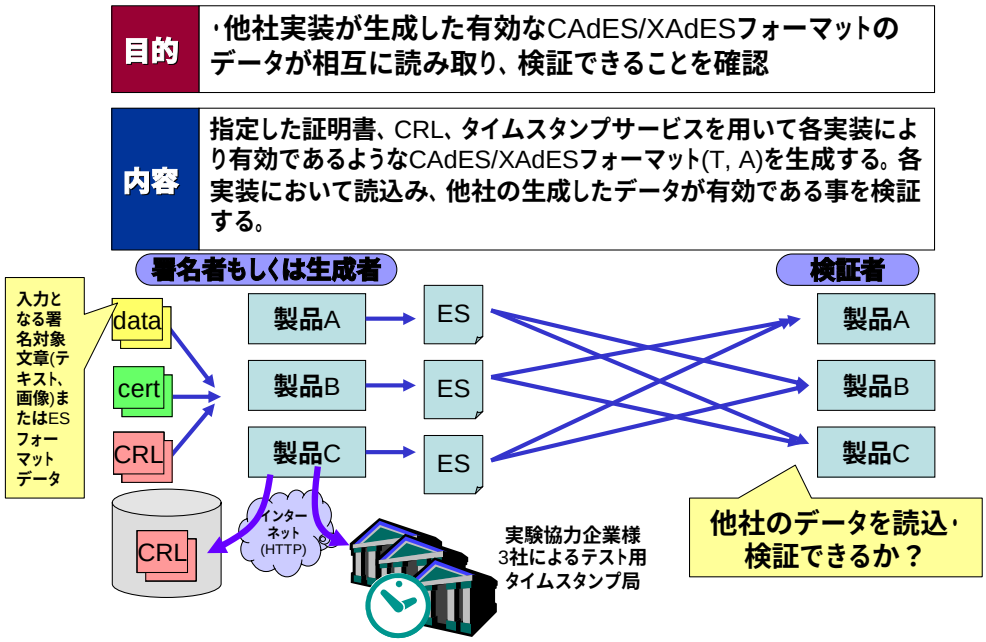

図 3-1　署名データ生成・検証相互運用性テストの概要

XAdES において一般にデータ交換される可能性の高いタイムスタンプ付き署名(XAdES-T)および、アーカイブ署名(XAdES-A)を本テストの対象とする。

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。

- XAdES-T 基本テストケース

XML 署名形態である Enveloping, Enveloped, Detached に対応した XAdES-T の基本テスト

- XAdES-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
- XAdES-T オプショナルプロパティテストケース
  XAdES-T に含めることが可能な QualifyingProperty の対応を確認するテスト
- XAdES-A 基本テストケース
  Enveloping、 Detached、Enveloped 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
- XAdES-A オプショナルプロパティテストケース
  XAdES-A に含めることが可能な QualifyingProperty の対応を確認するテスト

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

XAdES-T 基本テストケース (ON-T-BASIC)	
ON-T-BASIC-ENVELOPING	署名タイムスタンプ付 Enveloping XML 署名
ON-T-BASIC-DETACHED	署名タイムスタンプ付 Detached XML 署名
ON-T-BASIC-ENVELOPED	署名タイムスタンプ付 Enveloped XML 署名
XAdES-T タイムスタンプ局テストケース (ON-T-TSA)	
ON-T-TSA-AMANO-ENVELOPING	AMANO TSA を使用
ON-T-TSA-PFU-ENVELOPING	PFU TSA を使用
ON-T-TSA-SEIKO-ENVELOPING	SEIKO TSA を使用
XAdES-T オプショナルプロパティテストケース (ON-T-PROP)	
ON-T-PROP-SIGNINGTIME	SigningTime を使用
ON-T-PROP-EPES-FREEXML	SignaturePolicyIdentifier を使用。XML フリー形式の Policy ファイルを使用
ON-T-PROP-EPES-TR102038-V111	SignaturePolicyIdentifier を使用。ETSI TR 102 038 v1.1.1 に基づく XML 署名ポリシを使用。
ON-T-PROP-SIGNATUREPRODUCTIONPLACE	SignatureProductionPlace を使用
ON-T-PROP-SIGNERROLE-CLAIMED	ClaimedRole を持つ SignerRole を使用
ON-T-PROP-DATAOBJECTFORMAT	DataObjectFormat を使用
ON-T-PROP-COMMITMENTTYPEINDICATION	CommitmentTypeIndication を使用
ON-T-PROP-ALLDATATS-CLAIMEDTIME	AllDataObjectsTimeStamp と SigningTime を使用
ON-T-PROP-INDVDATATS-CLAIMEDTIME	IndividualDataObjectsTimeStamp と SigningTime を使用
ON-T-PROP-COUNTERSIGNATURE	CounterSignature を使用
ON-T-PROP-SIGNINGCERTIFICATE	SigningCertificate を使用
XAdES-A 基本テストケース (ON-A-BASIC)	
ON-A-BASIC-A1-ENVELOPING	Enveloping 署名で Refs が無く ArchiveTimeStamp を 1 つ付与
ON-A-BASIC-A1-DETACHED	Detached 署名で Refs が無く ArchiveTimeStamp を 1 つ付与
ON-A-BASIC-A1-ENVELOPED	Enveloped 署名で Refs が無く ArchiveTimeStamp を 1 つ付与
ON-A-BASIC-A2-ENVELOPING	ArchiveTimeStamp を 2 つ付与

ON-A-BASIC-A3-ENVELOPING	ArchiveTimeStamp を 3 つ付与
XAdES-A オプショナルプロパティテストケース (ON-A-PROP)	
ON-A-PROP-A1-REFS	Refs、ArchiveTimeStamp を付与
ON-A-PROP-A1-REFS-REFSONLYTS	Refs 、 RefsOnlyTimeStamp 、 ArchivfeTimeStamp を付与
ON-A-PROP-A1-REFS-SIGANDREFSTS	Refs 、 SigAndRefsTimeStamp 、 ArchiveTimeStamp を付与

各テスト項目に必要となる XAdES 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-ENVELOPING	ON-T-BASIC-DETACHED	ON-T-BASIC-ENVELOPED	ON-T-TSA-AMANO-ENVELOPING	ON-T-TSA-PFU-ENVELOPING	ON-T-TSA-SEIKO-ENVELOPING	ON-T-PROP-SIGNINGTIME	ON-T-PROP-EPES-FREEXML	ON-T-PROP-EPES-TR102038-V111	ON-T-PROP-SIGNATUREPRODUCTIONPLACE	ON-T-PROP-SIGNERROLE-CLAIMED	ON-T-PROP-DATAOBJECTFORMAT	ON-T-PROP-COMMITMENTTYPEINDICATION	ON-T-PROP-ALLDATATS-CLAIMEDTIME	ON-T-PROP-INDVDATATS-CLAIMEDTIME	ON-T-PROP-COUNTERSIGNATURE	ON-T-PROP-SIGNINGCERTIFICATE	ON-A-BASIC-A1-ENVELOPING	ON-A-BASIC-A1-DETACHED	ON-A-BASIC-A1-ENVELOPED	ON-A-BASIC-A2-ENVELOPING	ON-A-BASIC-A3-ENVELOPING	ON-A-PROP-A1-REFS	ON-A-PROP-A1-REFS-REFSONLYTS	ON-A-PROP-A1-REFS-SIGANDREFSTS
Signed Signature Properties	SigningTime							✓							✓	✓										
	SigningCertificate	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	✓	C1	C1	C1	C1	C1	C1	C1	C1
	KeyInfo.X509Data.X509Cert with Ref	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1		C1	C1	C1	C1	C1	C1	C1	C1
	SignaturePolicyIdentifier								✓	✓																
	SignatureProductionPlace										✓															
	SignerRole											✓														
Signed Data Object Properties	DataObjectFormat												✓													
	CommitmentTypeIndication													✓												
	AllDataObjectsTimeStamp														✓											
	IndividualDataObjectsTimeStamp															✓										
Unsigned Signature Properties	CounterSignature																✓									
	SignatureTimeStamp	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	CompleteCertificateRefs																							✓	✓	✓
	CompleteRevocationRefs																							✓	✓	✓
	AttributeCertificateRefs																									
	AttributeRevocationRefs																									
	SigAndRefsTimeStamp																									✓
	RefsOnlyTimeStamp																								✓	
	CertificateValues																		✓	✓	✓	✓	✓	✓	✓	✓
	RevocationValues																		✓	✓	✓	✓	✓	✓	✓	✓
	AttrAuthoritiesCertValues																									
	AttributeRevocationValues																									
	ArchiveTimeStamp																		1	1	1	2	3	1	1	1
Unsigned Data Object Property																										

C?: Choice

3.2. テスト実施手順

テスト実施の大まかな流れを以下に示す。

- 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
  - 検証必要なデータの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
  - Enveloping 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_CCC.bin
  - Detached 署名のテストに用いる 10K バイトのバイナリの署名対象ファイル。0x01020304050607080900 の並びで構成される。
- TARGET_DDD.xml
  - Enveloped 署名のテストに用いる XML データの署名対象ファイル。

- TARGET-SIGPOL-FREEXML.xml
  - ETSI TR 102 038 に準拠しないフリーフォーマットの XML 形式の署名ポリシ。署名ポリシの OID は 1.2.3.4.5.3 とする。
- TARGET-SIGPOL-TR2038.xml
  - ETSI TR 102 038 v1.1.1 に基づく XML フォーマットの署名ポリシ。署名ポリシの OID は 1.2.3.4.5.2 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 101 903 v1.3.2 に基づく XAdES 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
	QualifyingProperties 中のプロパティ		
		SignatureTimeStamp が含まれなければならない。	MUST
		SigningCertificate が含まれるか、KeyInfo の中に署名者証明書の X509Data.X509Certificate が含まれ、この KeyInfo が SignedInfo.Reference で参照されなければならない。	MUST
		他のプロパティ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 101 903 v1.3.2 に基づく XAdES を検証しなければならない		MUST
	証明書検証を除き XML 署名の有効性を検証しなければならない		MUST
	証明書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プロパティを含んでよい。例えば、複数のプロパティ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. XAdES-T 署名基本テストケース (ON-T-BASIC)

3.4.1. <ON-T-BASIC-ENVELOPING>

テキストファイルに対し、Enveloping 署名による XAdES-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		
	Enveloping 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
	SignedInfo.Reference	
	署名対象文書 ds:Object が対象でなければならない	MUST
	署名対象文書の Reference の Transforms は Base64 であることが望ましい	RECOMMEND

3.4.2. <ON-T-BASIC-DETACHED>

インターネット上で URI により参照されるバイナリデータに対し、Detached 署名による XAdES-T の生成および検証を行う。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。		
生成要件		
	Detached 署名を生成しなければならない	MUST
	署名対象文書は http://ecom-es-test.ath.cx/repository/TARGET_CCC.bin でなければならない	MUST
	SignedInfo.Reference	
	署名対象文書の Reference の URI は上記 URI でなければならない。	MUST

3.4.3. <ON-T-BASIC-ENVELOPED>

ローカルにある XML データファイルに対し、Enveloped 署名による XAdES-T の生成および検証を行う。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。			
生成要件			
	Enveloped 署名を生成しなければならない		MUST
	署名対象文書は ./TARGET_DDD.xml でなければならない		MUST
	SignedInfo.Reference		
		署名対象文書の Reference の URI は空文字列でなければならない。	MUST

3.5. XAdES-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-ENVELOPING>

アマノタイムビジネスの TSA を用いた Enveloping 署名による XAdES-T の生成および検証を行う。

<ON-T-BASIC-ENVELOPING>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 TSA を用いる	MUST

3.5.2. <ON-T-TSA-PFU-ENVELOPING>

PFU の TSA を用いた Enveloping 署名による XAdES-T の生成および検証を行う。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。		
生成要件		
	TSA は PFU の TSA を用いる	MUST

3.5.3. <ON-T-TSA-SEIKO-ENVELOPING>

セイコープレシジョンの TSA を用いた Enveloping 署名による XAdES-T の生成および検証を行う。

<ON-T-BASIC-ENVELOPING>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 TSA を用いる	MUST

3.6. XAdES-T オプショナルプロパティテストケース (ON-T-PROP)

本テストケースでは XAdES-T に付与することが可能なオプションのプロパティへの対応を確認する。

3.6.1. <ON-T-PROP-SIGNINGTIME>

本テスト項目では比較的一般的な SigningTime プロパティへの対応を確認する。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。			
生成要件			
	QualifyingProperties 中のプロパティ		
		SigningTime を含まれなければならない	MUST
		ETSI TS 101 903 v1.3.2 G.2.2.16 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 101 903 v1.3.2 G.2.2.16 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-PROP-EPES-FREEXML>

XAdES-EPES として、フリーフォーマットの XML 文書による SignaturePolicyIdentifier プロパティを持つ XAdES-T の対応を確認する。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。
生成要件

	QualifyingProperties 中のプロパティ	
	SignaturePolicyIdentifier を含まれなければならない	MUST
	本ポリシの OID は uri:oid:1.2.3.4.5.3 でなければならない。	MUST
	XML 署名ポリシファイルは http://ecom-es-test.ath.cx/repository/TARGET-SIGPOL-FREEXML.xml でなければならない。	MUST
検証要件		
	SignaturePolicyIdentifier の有無および署名ポリシの情報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。

3.6.3. <ON-T-PROP-EPES-TR102038-V111>

XAdES-EPES として、ETSI TR 102 038 v1.1.1 に準拠した XML 形式の署名ポリシによる SignaturePolicyIdentifier プロパティを持つ XAdES-T の対応を確認する。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。		
生成要件		
	QualifyingProperties 中のプロパティ	
	SignaturePolicyIdentifier を含まれなければならない	MUST
	本ポリシの OID は urn:oid:1.2.3.4.5.2 でなければならない。	MUST
	対象となる XML 署名ポリシファイルは http://ecom-es-test.ath.cx/repository/TARGET-SIGPOL-XML2038.xml でなければならない。	MUST
検証要件		
	SignaturePolicyIdentifier の有無および署名ポリシの情報を何らかの方法で目視確認しなければならない	MUST

3.6.4. <ON-T-PROP-SIGNATUREPRODUCTIONPLACE>

SignatureProductionPlace プロパティを持つ XAdES-T の対応を確認する。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。		
生成要件		
	QualifyingProperties 中のプロパティ	
	SignatureProductionPlace を含まれなければならない	MUST
検証要件		
	SignatureProductionPlace 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

3.6.5. <ON-T-PROP-SIGNERROLE-CLAIMED>

ClaimedRole を持つ SignerRole プロパティを持つ XAdES-T の対応を確認する。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。		
生成要件		
	QualifyingProperties 中のプロパティ	
	ClaimedRole を持つ SignerRole が含まれなければならない	MUST
検証要件		
	SignerRole 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-PROP-DATAOBJECTFORMAT>

DataObjectFormat プロパティを持つ XAdES-T の対応を確認する。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。
生成要件

	QualifyingProperties 中のプロパティ	
	MimeType に"text/plain"を持つ DataObjectFormat が含まれなければならない	MUST
検証要件		
	DataObjectFormat の有無および情報が目視確認できるか、もしくは記載された MimeType により、適切なビューアーが使用されなければならない	MUST

3.6.7. <ON-T-PROP-COMMITMENTTYPEINDICATION>

CommitmentTypeIndication プロパティを持つ XAdES-T の対応を確認する。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。		
生成要件		
	QualifyingProperties 中のプロパティ	
	CommitmentTypeIndication が含まれなければならない	MUST
検証要件		
	CommitmentTypeIndication の有無および情報が何らかの方法で目視確認できなければならない	MUST

3.6.8. <ON-T-PROP-ALLDATATS-CLAIMEDTIME>

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

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。		
生成要件		
	QualifyingProperties 中のプロパティ	
	AllDataObjectsTimeStamp および SigningTime が含まれなければならない	MUST

	ETSI TS 101 903 v1.3.2 G.2.2.16 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 101 903　v1.3.2 G.2.2.16 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

3.6.9. <ON-T-PROP-INDVDATATS-CLAIMEDTIME>

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

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。		
生成要件		
	QualifyingProperties 中のプロパティ	
	IndividualDataObjectsTimeStamp および SigningTime が含まれなければならない	MUST
	ETSI TS 101 903 v1.3.2 G.2.2.16 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 101 903　v1.3.2 G.2.2.16 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

3.6.10. <ON-T-PROP-COUNTERSIGNATURE>

CounterSignature プロパティを持つ XAdES-T の対応を確認する。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。
生成要件

	QualifyingProperties 中のプロパティ	
	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-PROP-SIGNINGCERTIFICATE>

SigningCertificate プロパティを持つ XAdES-T の対応を確認する。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。		
生成要件		
	QualifyingProperties 中のプロパティ	
	SigningCertificate が含まれなければならない	MUST
検証要件		
	SigningCertificate の情報と署名者証明書との一致確認を行わなければならない。	MUST

3.7. XAdES-A 基本テストケース (ON-A-BASIC)

3.7.1. <ON-A-BASIC-A1-ENVELOPING>

Enveloping 署名による第一世代の XAdES-A への対応を確認する。

<ON-T-BASIC-ENVELOPING>の要件を基礎とする。	
生成要件	
QualifyingProperties 中のプロパティ	
署名者証明書の検証に必要な証明書情報を持つ CertificateValues を含まなければならない	MUST
署名者証明書の検証に必要な失効情報を持つ RevocatoinValues を含まなければならない	MUST
ETSI TS 101 903 v1.3.2 に基づく ArchiveTimeStamp を 1 つ含まなければならない	MUST
ArchiveTimeStamp 以外の TimeStampToken の TSA 証明書の検証に必要な情報は TimeStampToken の certificates および crls フィールドに格納することを推奨する	RECOMMEND
TimeStampToken に TSA 証明書の検証情報を含めない場合、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 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>

Detached 署名による第一世代の XAdES-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		
	QualifyingProperties 中のプロパティ	
	署名者証明書の検証に必要な証明書情報を持つ CertificateValues を含まなければならない	MUST
	署名者証明書の検証に必要な失効情報を持つ RevocationValues を含まなければならない	MUST
	ETSI TS 101 903 v1.3.2 に基づく ArchiveTimeStamp を 1 つ含まなければならない	MUST
	ArchiveTimeStamp 以外の TimeStampToken の TSA 証明書の検証に必要な情報は TimeStampToken の certificates および crls フィールドに格納することを推奨する	RECOMMEND
	TimeStampToken に TSA 証明書の検証情報を含めない場合、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 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-A1-ENVELOPED>

Enveloped 署名による第一世代の XAdES-A への対応を確認する。

<ON-T-BASIC-ENVELOPED>の要件を基礎とする。		
生成要件		
	QualifyingProperties 中のプロパティ	
	署名者証明書の検証に必要な証明書情報を持つ CertificateValues を含まなければならない	MUST
	署名者証明書の検証に必要な失効情報を持つ RevocationValues を含まなければならない	MUST
	ETSI TS 101 903 v1.3.2 に基づく ArchiveTimeStamp を 1 つ含ま	MUST

	なければならない	
	ArchiveTimeStamp 以外の TimeStampToken の TSA 証明書の検証に必要な情報は TimeStampToken の certificates および crls フィールドに格納することを推奨する	RECOMMEND
	TimeStampToken に TSA 証明書の検証情報を含めない場合、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 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

3.7.4. <ON-A-BASIC-A1-ENVELOPING>

Enveloping 署名による第二世代の XAdES-A への対応を確認する。

<ON-A-BASIC-A1-ENVELOPING>の要件を基礎とする。		
生成要件		
QualifyingProperties 中のプロパティ		
	ETSI TS 101 903 v1.3.2 に基づく ArchiveTimeStamp を 2 つ含まなければならない	MUST
	ArchiveTimeStamp の時間間隔は 1 日程度以上空けることを推奨する	RECOMMEND

3.7.5. <ON-A-BASIC-A3-ENVELOPING>

Enveloping 署名による第三世代の XAdES-A への対応を確認する。

<ON-A-BASIC-A2-ENVELOPING>の要件を基礎とする。		
生成要件		
	QualifyingProperties 中のプロパティ	
		ETSI TS 101 903 v1.3.2 に基づく ArchiveTimeStamp を 3 つ含まなければならない	MUST

3.8. XAdES-A オプショナルプロパティテストケース (ON-A-PROP)

3.8.1. <ON-A-PROP-A1-REFS>

CompleteCertificateRefs および CompleteRevocationRefs を含む XAdES-A の対応を確認する。

<ON-A-BASIC-A1-ENVELOPING>の要件を基礎とする。		
生成要件		
	QualifyingProperties 中のプロパティ	
		CompleteCertifiacteRefs, CompleteRevocationRefs を含まなければならない	MUST
検証要件		
	署名者証明書検証の際、検証情報と Refs との一致確認を行わなければならない	MUST

3.8.2. <ON-A-PROP-A1-REFS-REFSONLYTS>

RefsOnlyTimeStamp プロパティを含む XAdES-A の対応を確認する。

<ON-A-PROP-A1-REFS>の要件を基礎とする。		
生成要件		
	QualifyingProperties 中のプロパティ	
		RefsOnlyTimeStamp を含まなければならない	MUST

3.8.3. <ON-A-PROP-A1-REFS-SIGANDREFSTS>

SigAndRefsTimeStamp プロパティを含む XAdES-A の対応を確認する。

<ON-A-PROP-A1-REFS>の要件を基礎とする。		
生成要件		
	QualifyingProperties 中のプロパティ	
		SigAndRefsTimeStamp を含まなければならない	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：実験データ用プロファイル

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。なお、証明書およびタイムスタンプトークンのプロファイルは CAdES の実験に利用したものを用いる。

4.1. オフラインテスト用長期署名フォーマットデータプロファイル

長期署名フォーマットのデータは、全て XAdES の仕様に基づいている。

4.1.1. XAdES-BES

要素	内容
ds:Signature	
ds:SignedInfo	あり
ds:CanonicalizationMethod	Canonical XML(REC-xml-c14n-20010315)
ds:SignatureMethod	RSAwithSHA1(http://www.w3.org/2000/09/xmldsig#rsa-sha1)
ds:Reference	複数の場合も考慮する（署名形式はテスト項目に依存）
ds:Transforms	署名対象がXMLの場合は、Canonical XMLを使用する。
ds:DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1
ds:DigestValue	署名対象文書のダイジェスト値
ds:SignatureValue	署名値
ds:KeyInfo	有り(ds:X509Data要素のds:X509Certificate要素 に署名者証明書を格納)
ds:Object	有り(SingingCertificateの有無に依存する)
QualifyingProperties	有り(SingingCertificateの有無に依存する)
SignedProperties	有り(SingingCertificateの有無に依存する)
SignedSignatureProperties	有り(SingingCertificateの有無に依存する)
SigningCertificate	発行者名、シリアル番号、SHA1フィンガープリント

4.1.2. XAdES-T

要素	内容
ds:Signature	
ds:SignedInfo	あり
ds:CanonicalizationMethod	Canonical XML(REC-xml-c14n-20010315)
ds:SignatureMethod	RSAwithSHA1(http://www.w3.org/2000/09/xmldsig#rsa-sha1)
ds:Reference	複数の場合も考慮する（署名形式はdetached形式とする）
ds:Transforms	署名対象文書のフォーマットに依存する。 署名対象がXMLの場合は、Canonical XMLを使用する。
ds:DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1
ds:DigestValue	署名対象文書のダイジェスト値
ds:SignatureValue	署名値
ds:KeyInfo	有り(ds:X509Data要素のds:X509Certificate要素 に署名者証明書を格納)
ds:Object	有り
QualifyingProperties	有り
SignedProperties	有り(SingingCertificateの有無に依存する)
SignedSignatureProperties	有り(SingingCertificateの有無に依存する)
SigningCertificate	発行者名、シリアル番号、SHA1フィンガープリント
UnSignedProperties	有り
UnSignedSignatureProperties	有り
SignatureTimeStamp	トークンは実験用データプロファイルに従う

4.1.3. XAdES-A(第一世代)

要素	内容
ds:Signature	
ds:SignedInfo	あり
ds:CanonicalizationMethod	Canonical XML(REC-xml-c14n-20010315)
ds:SignatureMethod	RSAwithSHA1(http://www.w3.org/2000/09/xmldsig#rsa-sha1)
ds:Reference	複数の場合も考慮する（署名形式はdetached形式とする）
ds:Transforms	署名対象文書のフォーマットに依存する。 署名対象がXMLの場合は、Canonical XMLを使用する。
ds:DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1
ds:DigestValue	署名対象文書のダイジェスト値
ds:SignatureValue	署名値
ds:KeyInfo	有り(ds:X509Data要素のds:X509Certificate要素 に署名者証明書を格納)
ds:Object	有り
QualifyingProperties	有り
SignedProperties	有り(SingingCertificateの有無に依存する)
SignedSignatureProperties	有り(SingingCertificateの有無に依存する)
SigningCertificate	発行者名、シリアル番号、SHA1フィンガープリント
UnSignedProperties	有り
UnSignedSignatureProperties	有り
SignatureTimeStamp	トークンは実験用データプロファイルに従う
CompleteCertificateRefs	無し
CompleteRevocationRefs	無し
CertificateValues	有り
RevocationValues	有り(CRLのみ)
ArchiveTimeStamp	トークンは実験用データプロファイルに従う

4.1.4. XAdES-A(第二世代)

要素	内容
ds:Signature	
ds:SignedInfo	あり
ds:CanonicalizationMethod	Canonical XML(REC-xml-c14n-20010315)
ds:SignatureMethod	RSAwithSHA1(http://www.w3.org/2000/09/xmldsig#rsa-sha1)
ds:Reference	複数の場合も考慮する（署名形式はdetached形式とする）
ds:Transforms	署名対象文書のフォーマットに依存する。 署名対象がXMLの場合は、Canonical XMLを使用する。
ds:DigestMethod	http://www.w3.org/2000/09/xmldsig#sha1
ds:DigestValue	署名対象文書のダイジェスト値
ds:SignatureValue	署名値
ds:KeyInfo	有り(ds:X509Data要素のds:X509Certificate要素 に署名者証明書を格納)
ds:Object	有り
QualifyingProperties	有り
SignedProperties	有り
SignedSignatureProperties	有り
SigningCertificate	発行者名、シリアル番号、SHA1フィンガープリント）
UnSignedProperties	有り
UnSignedSignatureProperties	有り
SignatureTimeStamp	トークンは実験用データプロファイルに従う
CompleteCertificateRefs	無し
CompleteRevocationRefs	無し
CertificateValues	有り
RevocationValues	有り(CRLのみ)
ArchiveTimeStamp	トークンは実験用データ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

4.2. 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。JIS 原案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	検証情報としてTSA証明書およびパスを含みうる
crls	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(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

※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. 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