

OpenXML 長期署名 システム設計書 (詳細)

2008年 3月24日版

国立情報学研究所
学術ネットワーク研究開発センター

山地一禎, 片岡俊幸, 曾根原登

■ 目次

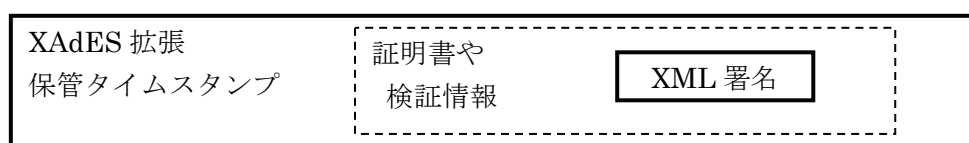
■ 目次	1 -
1 - 1. 目的	2 -
1 - 2. XML署名と長期署名 (XAdES) の違い	2 -
1 - 3. XML署名の長期署名 (XAdES) 化の問題点	4 -
1 - 4. OpenXMLにおける長期署名 (XAdES) 化の方針	5 -
2 - 1. OpenXMLとODFのXML署名仕様解析結果 1 (署名対象の指定)	6 -
2 - 2. OpenXMLとODFのXML署名仕様解析結果 2 (複数署名)	8 -
3 - 1. OpenXML仕様 1 (Package-Specific Object)	9 -
3 - 2. OpenXML仕様 2 (Application-Specific Object)	12 -
4 - 1. プロジェクト構成	13 -
4 - 2. インストールキット	13 -
付録 1. MS-Office2007 で作成したOpenXML署名ファイル (sig1.xml)	14 -
付録 2. 標準長期署名仕様のOpenXML署名ファイル (sig1.xml)	17 -

1-1. 目的

本システム設計書はMicrosoftのOffice 2007より採用されたOffice Open XML(OOXMLとも略すが本資料中では以後OpenXML)フォーマットによるWord文書に対する電子署名(Office用語ではデジタル署名)の仕様を明確にし、その上でXML署名の上位互換フォーマットである長期署名(XAdES)フォーマットへの対応を検討する目的を持つ。なおOpenXMLフォーマットと似たフォーマットとしてよく対比さえるOpen Document Format(ODFと略す)フォーマットにおける長期署名の仕様と比較する。また実装例としてのOpenXML長期署名ツールOOXmlSignToolの仕様をまとめる。

1-2. XML署名と長期署名(XAdES)の違い

最初にXMLによる署名とXAdESによる長期署名の違いを解説する。XML署名はW3C勧告またはRFC3075にて規格化されている。XAdES署名はXML署名の上位互換規格であり、長期保管に必要となる各種情報(証明書や検証情報等)をタイムスタンプ(RFC3161)により長期保証する仕組みを提供する。



まず以下にXML署名の基本的な構造を示す。

<Signature>	// XML 署名開始タグ
<SignedInfo>	// 署名対象要素
<CanonicalizationMethod/>	// 署名対象正規化手法指定
<SignatureMethod/>	// 署名アルゴリズム指定
<Reference/>	// 署名対象への URI 指定 1 とオプション変換手法指定
:	// 署名対象は複数指定可能
<Reference/>	// 署名対象への URI 指定 n
</SignedInfo>	// 署名対象要素終了
<SignatureValue/>	// 署名値 (Base64)
<KeyInfo/>	// 署名者の秘密鍵情報
<Object/>	// 署名対象内包時のオブジェクト要素 (オプション)
</Signature>	// XML 署名終了タグ

XML 署名の標準的な要素

次に XAdES 署名の基本的な構造を示す。

```

<Signature> // XML 署名開始タグ
  <SignedInfo> // 署名対象要素
    <CanonicalizationMethod/> // 署名対象正規化手法指定
    <SignatureMethod/> // 署名アルゴリズム指定
    <Reference/> // 署名対象への URI 指定 1 とオプション変換手法指定
    : // 署名対象は複数指定可能
    <Reference URI=" #xades" /> // XAdES 署名対象への URI 指定
  </SignedInfo> // 署名対象要素終了
  <SignatureValue/> // 署名値 (Base64)
  <KeyInfo/> // 署名者の秘密鍵情報
  <Object/> // 署名対象内包時のオブジェクト要素 (オプション)
  <Object> // 長期署名用オブジェクト (必須)
    <QualifyingProperties> // XAdES 要素開始
      <SignedProperties Id=" xades" > // XAdES 署名対象要素
        <SignedSignatureProperties/> // XAdES 署名要素 (例: <SigningTime>等)
      </SignedProperties> // XAdES 署名対象要素終了
      <UnsignedProperties> // XAdES 非署名対象要素
        <UnsignedSignatureProperties> // XAdES 非署名要素
          <SignatureTimeStamp/> // XAdES-T 署名タイムスタンプ要素
          <CertificateValues/> // XAdES-X-Long 証明書一覧要素
          <RevocationValues/> // XAdES-X-Long 検証情報一覧要素
          <ArchiveTimeStamp/> // XAdES-A 保管タイムスタンプ要素 (複数回可能)
          :
        </UnsignedSignatureProperties> // XAdES 非署名要素
      </UnsignedProperties> // XAdES 非署名対象要素終了
    </QualifyingProperties> // XAdES 要素終了
  </Object> // 長期署名用オブジェクト終了タグ
</Signature> // XML 署名終了タグ

```

XAdES 署名の標準的な要素

先の XML 署名と比較すると太字になっている**長期署名用 Object 要素**が追加され、その中の<SignedProperties>へ対する<Reference>要素が追加されている点が異なる。特に<SignedProperties>を含む<Object>は署名時には用意されている必要がある。この為に最初に XML 署名されてしまったファイルに対しては XAdES 要素を追加できない問題がある。つまり **XAdES 長期署名を付与するには最初から XAdES 長期署名として署名をする必要がある**。XML 署名と XAdES オブジェクトの署名要素のみの形式を XAdES-BES と呼び、単なる XML 署名とは区別している。なお XAdES ファイルを XML 署名として検証する事は何も問題が無い。

1-3. XML署名の長期署名 (XAdES) 化の問題点

前ページまでに説明にあるように、既存のXML署名ファイルを後から長期署名(XAdES)化することは出来ない。署名時から長期署名用に署名付与して XAdES-BES 形式にしておく必要がある。

OpenXMLを採用している Office2007 や、ODFを採用している OpenOffice.org では標準の署名形式がXML署名である。しかしながら XAdES形式の長期署名を付与するには標準の署名機能を使わずに、別途署名時に長期署名形式の XAdES-BES を作成する必要がある。生成された長期署名ファイルはXML署名として検証が可能なので基本的には Office2007 や OpenOffice.org のアプリケーションでの検証も可能であるはずである。

ただし例えば OpenOffice.org のワープロアプリケーションを使った場合には ODF 独自の Object 要素が署名対象に入っていないと ODF の署名として扱われない。

```
<Object>
  <SignatureProperties xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignatureProperty Id="ODF-ADD" Target="#Signature">
      <dc:date xmlns:dc="http://purl.org/dc/elements/1.1/">2007-12-20T18:28:17</dc:date>
    </SignatureProperty>
  </SignatureProperties>
</Object>
```

ODF 署名に必要な Object 要素

ODF 署名では上記署名日時を記述した Object 要素を署名対象として追加する事で長期署名化した署名ファイルも OpenOffice.org にて検証が可能となった。なお実際の署名対象としては直接 ODF ファイル内でのファイルパスを Reference 要素にて指定している。

調査した結果、OpenXMLにおいては必須の Object 要素 (Package-Specific Object : Id は "idPackageObject" 固定) と、オプションの Object 要素 (Application-Specific Object) を追加すれば良い事が判明している。長期署名対応とするにはこの2種類の Object 要素に加えて長期署名用 Object 要素を追加した場合に Office2007 が検証を通してくれるかと言う問題がある。実際に試してみたところ Office2007 では長期署名仕様の XML 署名ファイルの検証は通らなかった。

ECMA による ISO に対する OpenXML の仕様書 (Final Draft) では「Part2: Open Packaging Conventions」の「1 2. Digital Signature」では OpenXML 独自の Package-Specific と Application-Specific が指定可能とあるものの、他のタイプの Object 要素に関しては何も記載が無い (駄目だとも書いてない)。少なくとも Office2007 で長期署名 Object が許されないと OpenXML ではそのままの形式での長期署名 (XAdES) 化は困難だと言える。

1-4. OpenXMLにおける長期署名 (XAdES) 化の方針

OpenXML の長期署名 (XAdES) 化が現在は実現できない状況にある。この場合に対応可能な方針としては以下の2通りが考えられる。

1) Microsoft に交渉して長期署名 Object を OpenXML の仕様に追加して貰う

正直言ってかなり難しいと思われるが、長期的視点に立てば可能であればトライすべき方針である。現在の OpenXML および Office2007 では長期署名の可能性を全く考慮していないように見える。長期署名は欧州及び日本では検討や標準化が進んでいるが米国は熱心では無い。ODF 署名に関しても長期署名が考慮されていると言うよりも仕様に無い冗長な記述も許されているだけとも言える。「ODF では長期署名が可能である」と言えば Microsoft も興味を持つかもしれない。

2) OpenXML 標準の署名ファイルに対して別途長期署名を付与する

次善の策ではあるが、OpenXML 標準で作成される XML 署名ファイル (sig1.xml 等) を署名対象にした長期署名ファイル (sig1-xades.xml 等) を作成して OpenXML の中に埋め込む。署名対象となる XML 署名ファイルは、Office2007 で署名したファイルでも構わないし独自に XML 署名したファイルでも構わない。独自に生成した XML 署名ファイルが Office2007 で検証可能である事は確認をした。また余分な長期署名ファイルを埋め込んでもエラーにはならない事も確認をした。

今回の実装としては1)と2)の両方に署名と検証の両方で対応する。ただし署名時のデフォルトは2)の方式とする。1)と2)の方式に加え元々OpenXMLの仕様であるXML署名を加えた3方式を実装した。以下に3方式の種類と名称を列挙する。

種類	動作
標準 XML 署名	sig1.xml を生成 (標準の XML 署名)
標準長期署名	sig1.xml を生成 (sig1.xml を長期署名化)
拡張長期署名	sig1.xml (標準の XML 署名) と sig1-xades.xml (長期署名) を生成

2-1. OpenXMLとODFのXML署名仕様解析結果 1 (署名対象の指定)

ここからは長期署名からは一旦離れて、OpenXMLとODFの署名に関して比較しつつ解説を行う。なおODF署名に関しては現在ODFの1.1と呼ばれる仕様では記載されていない。ODFの1.2から署名機能の仕様が明らかにされる予定である。本資料は独自にOpenOffice.orgのアプリケーションで署名した結果から解析をした仕様を説明する。

まず署名対象の指定方法にOpenXMLとODFでは明確に違いがある。ODFでは直接的にSignedInfo要素内のReference要素からODFファイル内のファイルパスとして署名対象を指定している。OpenXMLではSignedInfo要素内のReference要素はOpenXML独自形式であるObject要素(Package-Specific Object: Idは"IdPackageObject"固定)を参照しており、Package-Specific Object要素内のReference要素からOpenXMLファイル内のファイルパスを指定している。ODF署名が直接指定ならOpenXML署名は間接指定と言える。

```
<document-signatures>
  <Signature> // XML 署名開始タグ
    <SignedInfo> // 署名対象要素
      <Reference URI=" content.xml" /> // 署名対象 content.xml への URI 指定 (外部ファイル)
      <Reference URI=" meta.xml" /> // 署名対象 meta.xml への URI 指定 (外部ファイル)
      <Reference URI=" settings.xml" /> // 署名対象 settings.xml への URI 指定 (外部ファイル)
      <Reference URI=" styles.xml" /> // 署名対象 styles.xml への URI 指定 (外部ファイル)
      <Reference URI=" #ID-DATE" /> // 署名対象 content.xml への URI 指定 (内包 Id 指定)
    </SignedInfo> // 署名対象要素終了
    <SignatureValue/> // 署名値 (Base64)
    <KeyInfo/> // 署名者の秘密鍵情報
    <Object>
      <SignatureProperties>
        <SignatureProperty Id=" ID-DATE" >
          <dc:date/> // 署名日時要素 (PURLS 指定)
        </SignatureProperty>
      </SignatureProperties>
    </Object>
  </Signature> // XML 署名終了タグ
</document-signatures>
```

ODF 署名の標準的な要素

ODF署名では署名対象として直接ファイル名が指定される。ただし署名日時のdate要素に対しての内包データとしてId指定も必要となる。date要素を除けば全てXML署名仕様の範囲内であり、シンプルなXML署名形式と言える。

```

<Signature> // XML 署名開始タグ
  <SignedInfo> // 署名対象要素
    <Reference URI="#idPackageObject" /> // Package-Specific Object への URI 指定 (内包 Id 指定)
    <Reference URI="#idOfficeObject" /> // Application-Specific Object への URI 指定 (内包 Id
指定)
  </SignedInfo> // 署名対象要素終了
  <SignatureValue/> // 署名値 (Base64)
  <KeyInfo/> // 署名者の秘密鍵情報
  <Object Id=" idPackageObject" > // Package-Specific Object
    <Manifest>
      <Reference URI=" /_rels/.rels" /> // 署名対象 .rels への URI 指定 (外部ファイル)
      <Reference URI=" /word/_rels/document.xml.rels" />
// 署名対象 document.xml.rels への URI 指定 (外部ファイル)
      <Reference URI=" /word /document.xml" />
// 署名対象 document.xml への URI 指定 (外部ファイル)
      <Reference URI=" /word /fontTable.xml" />
// 署名対象 fontTable.xml への URI 指定 (外部ファイル)
      <Reference URI=" /word /settings.xml" />
// 署名対象 settings.xml への URI 指定 (外部ファイル)
      <Reference URI=" /word /styles.xml" />
// 署名対象 styles.xml への URI 指定 (外部ファイル)
      <Reference URI=" /word/theme/theme1.xml" />
// 署名対象 theme1.xml への URI 指定 (外部ファイル)
      <Reference URI=" /word /webSettings.xml" />
// 署名対象 webSettings.xml への URI 指定 (外部ファイル)
    </Manifest>
    <SignatureProperties>
      <SignatureProperty>
        <mdssi:SignatureTime/> // 署名日時要素 (OpenXML 独自要素)
      </SignatureProperty>
    </SignatureProperties>
  </Object>
  <Object Id=" idOfficeObject" > // Application-Specific Object
    <SignatureComments/> // コメント (オプション)
    <OfficeVersion/> // Office のバージョン番号
    :
  </Object>
</Signature> // XML 署名終了タグ

```

OpenXML 署名の標準的な要素

署名対象の SignedInfo 要素内にある Reference 要素は内包され OpenXML 用に生成された Object 要素を署名対象としている。Package-Specific Object 要素内には Manifest タグがあり、その中から再度 Reference 要素として最終的な OpenXML 構成要素ファイルへのパスが指定されている。Manifest 要素とその中への Reference 要素を指定は XML 署名の仕様範囲内である。

2-2. OpenXMLとODFのXML署名仕様解析結果2（複数署名）

署名は OpenXML でも ODF でも複数を経列署名として付与する事が可能になっている。しかしながらそのやり方はそれぞれ異なる。

OpenXML では最初の署名は `_xmldsignatures` フォルダ下の `sig1.xml` というファイル名として生成される。以後2つ目は `sig2.xml`、3つ目が `sig3.xml` というように XML 署名ファイルが増えて行く方式になっている。

<code>_xmldsignatures</code> フォルダ
<code>origin.sigs</code> ファイル (署名用のダミーデータか?内容はゼロバイト)
<code>sig1.xml</code> ファイル <code><Signature>XML 署名 1 </Signature></code>
<code>sig2.xml</code> ファイル <code><Signature>XML 署名 2 </Signature></code>
<code>sig3.xml</code> ファイル <code><Signature>XML 署名 3 </Signature></code>
:
<code>sign.xml</code> ファイル <code><Signature>XML 署名 n </Signature></code>

OpenXML では Relationship と呼ばれる仕組みでファイル間の関係を定義している。各署名ファイルは `_xmldsignatures` フォルダ下にある `_rels` フォルダ内の `origin.sigs.rels` により定義されている。

ODF では署名ファイルは META-INF フォルダ下の `documentsignatures.xml` だけになる。`documentsignatures.xml` は最初に独自のタグ `document-signatures` 要素があり、その下に複数の XML 署名 Signature 要素を持つ事が出来るようになっている。

META-INF フォルダ
<code>documentsignatures.xml</code> ファイル <code><document-signatures></code> <code><Signature>XML 署名 1 </Signature></code> <code><Signature>XML 署名 2 </Signature></code> <code><Signature>XML 署名 3 </Signature></code> : <code><Signature>XML 署名 n </Signature></code> <code></document-signatures></code>

3-1. OpenXML仕様1 (Package-Specific Object)

XML 署名では Reference 要素の属性として Transform (変換) 要素をセット可能になっている。ODF 署名では XML 署名標準の Transform 要素だけであるが、OpenXML 署名では独自の変換である RelationshipTransform が仕様として設定されている。これは Package-Specific Object 要素内の Manifest 要素内に定義されている Reference 要素にて指定されている。

```

:
<Object Id="idPackageObject" // Package-Specific Object
  <Manifest>
    <Reference URI="/_rels/.rels" // 署名対象.rels への URI 指定 (外部ファイル)
      <Transforms>
        <Transform
          Algorithm="http://schemas.openxmlformats.org/package/2006/RelationshipTransform">
          <mdssi:RelationshipReference SourceId="rId1" />
        </Transform>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <DigestValue>1vWU/YTF/7t6ZjnE44gAFTbZvvA=</DigestValue>
    </Reference>
  </Manifest>
  <SignatureProperties/>
</Object>
:

```

RelationshipTransform 要素

OpenXML では Relationship 署名対象 (拡張子が ".rels" のファイル) に対し、Transform 要素として RelationshipTransform 変換の後で XML 正規化変換 (c14n 変換) を行うことが指定されている。拡張子が ".rels" のファイルも内部は XML となっているので、この2つの変換を順次適応してハッシュ計算対象の XML 情報を取得する。

```

<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId1"
    Type="http://schemas.openxmlformats.org/package/2006/relationships/digital-signature/signature"
    Target="sig1.xml"/>
</Relationships>

```

origin.sigs.rels 例

RelationshipTransform を使った変換は大雑把に言って以下の手順が良い。

1) 必要な Relationship 要素を対象となる .rels より取り出す Transform 要素の SourceId 属性で指定されていない Relationship 要素は削除する
2) 名前空間プレフィックス等があれば削除する Office2007 で生成されたファイルは最初から名前空間プレフィックスを含んでいない
3) Relationship 要素で省略されている属性情報を追加する 通常 TargetMode 属性が省略されているので補う (OpenXML 仕様書説明に記載が無い)
4) Relationship 要素を Id 属性により並べ替え (ソート) する
5) XML 正規化を実施する 余分な余白削除や Id をアルファベット順に並べたり名前空間の処理をする

2) の TargetMode 属性を付けなければならない点が OpenXML 仕様書に記載が無く、試行錯誤により解析をした。本来なら仕様書の手順として明記しておくべき項目であろう。この変換により前ページの origin.sigs.rels を変換した結果が以下となる。なお以下は分かりやすくする為に改行を加えてあるが、実際には改行は入らない。

```
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship
    Id="rId1"
    Target="sig1.xml"
    TargetMode="Internal"
    Type="http://schemas.openxmlformats.org/package/2006/relationships/digital-signature/signature">
  </Relationship>
</Relationships>
```

origin.sigs.rels 変換例

OpenXML 署名はルートフォルダ下の /_rels/.rels により署名対象となる document.xml を指定しており、更に /word/_rels/ document.xml.rels により document.xml と関連付けられているファイルを Relationship を指定しているようである。

参考までに ODF 署名では以下の情報を署名対象としている。Relationship に相当する仕組みが無いので以下のルールとして長期署名対応している。

1) ルートフォルダ直下にある "layout-cache" ファイル。
2) ルートフォルダ直下にある拡張子が ".xml" のファイル全て。
3) Pictures フォルダ下にある全てのファイル。(Pictures フォルダが無い場合あり)
4) デジタル署名ファイル内の Object/SignatureProperties/SignatureProperty/date 情報。

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<xsd:schema xmlns="http://schemas.openxmlformats.org/package/2006/relationships"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://schemas.openxmlformats.org/package/2006/relationships"
  elementFormDefault="qualified" attributeFormDefault="unqualified" blockDefault="#all">

  <xsd:element name="Relationships" type="CT_Relationships" />
  <xsd:element name="Relationship" type="CT_Relationship" />

  <xsd:complexType name="CT_Relationships">
    <xsd:sequence>
      <xsd:element ref="Relationship" minOccurs="0" maxOccurs="unbounded" />
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="CT_Relationship">
    <xsd:simpleContent>
      <xsd:extension base="xsd:string">
        <xsd:attribute name="TargetMode" type="ST_TargetMode" use="optional" />
        <xsd:attribute name="Target" type="xsd:anyURI" use="required" />
        <xsd:attribute name="Type" type="xsd:anyURI" use="required" />
        <xsd:attribute name="Id" type="xsd:ID" use="required" />
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>

  <xsd:simpleType name="ST_TargetMode">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="External" />
      <xsd:enumeration value="Internal" />
    </xsd:restriction>
  </xsd:simpleType>
</xsd:schema>
```

参考 : Relationship の XML スキーマ

3-2. OpenXML仕様2 (Application-Specific Object)

OpenXML 署名において署名日時は Package-Specific Object 要素内の SignatureProperties / SignatureProperty / SignatureTime として指定されるが、その他の情報は全て Application-Specific Object 要素内で指定されている。署名理由を示す SignatureComments 要素は Office2007 の署名時に入力される情報だが、他の Windows や Office のバージョン情報等は自動的に設定されるようだ。以下に Application-Specific Object の例を示す。

```
:
<Object Id="idOfficeObject">
  <SignatureProperties>
    <SignatureProperty Id="idOfficeV1Details" Target="#idPackageSignature">
      <SignatureInfoV1 xmlns="http://schemas.microsoft.com/office/2006/digsig">
        <SetupID />
        <SignatureText />
        <SignatureImage />
        <SignatureComments>LangEdge Test.</SignatureComments>
        <WindowsVersion>5.1</WindowsVersion>
        <OfficeVersion>12.0</OfficeVersion>
        <ApplicationVersion>12.0</ApplicationVersion>
        <Monitors>1</Monitors>
        <HorizontalResolution>1024</HorizontalResolution>
        <VerticalResolution>768</VerticalResolution>
        <ColorDepth>16</ColorDepth>
        <SignatureProviderId>{00000000-0000-0000-0000-000000000000}</SignatureProviderId>
        <SignatureProviderUrl />
        <SignatureProviderDetails>9</SignatureProviderDetails>
        <ManifestHashAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</ManifestHashAlgorithm>
        <SignatureType>1</SignatureType>
      </SignatureInfoV1>
    </SignatureProperty>
  </SignatureProperties>
</Object>
:
```

Application-Specific Object 例

上記例の要素全部を設定する必要は無いようだがまだ未確認である。

4-1. プロジェクト構成

OpenXML 長期署名ツール OOXmlSignTool は Visual Studio 2005 の C++/CLI により構築されている。全体のプロジェクトファイル は以下となる。

```
LeXAdES¥OOXmlSign¥test¥OOXmlSignTest.sln
```

この中には以下のプロジェクトが含まれている。

プロジェクト名	説明
LeXAdES	長期署名ライブラリ
LeZlib	zlib による ZIP 圧縮ライブラリ
OOXmlSign	OpenXML 長期署名拡張ライブラリ
OOXmlSignTool	OpenXML 長期署名ツール本体
Setup	OpenXML 長期署名ツールのインストールキット

通常はアクティブなプロジェクトとして「OOXmlSignTool」を選択しておく。インストールキット生成の「Setup」プロジェクトは「OOXmlSignTool」をフルビルド（リビルド）してもビルドされないので、「OOXmlSignTool」をフルビルド後にマウスにより選択して単独ビルドする。

LeXAdES ライブラリは他に ASN.1 解析ライブラリ LeAsn1Xml も含む。LeAsn1Xml をビルドするには以下のプロジェクトファイルを開く。

```
LeXAdES¥LeAsn1Xml¥src¥ LeAsn1Xml.sln
```

4-2. インストールキット

OpenXML 長期署名ツール OOXmlSignTool のインストールキットは以下のフォルダ下に作成される。この中の Setup.exe を実行する事でインストールが可能。なおインストール時には必要となる Microsoft 社製のモジュールも自動インストールされる。

```
LeXAdES¥OOXmlSign¥test¥Setup¥Release
```

提供される CD-R にはルート直下に OOXmlSignTool フォルダがあり、その中にインストールキットを置いてある。

付録 1. MS-Office2007 で作成したOpenXML署名ファイル (sig1.xml)

```

<?xml version="1.0" encoding="UTF-8"?>
<Signature Id="idPackageSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <Reference URI="#idPackageObject" Type="http://www.w3.org/2000/09/xmldsig#Object">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>bF22T4UPN76bYu3H7Fqwtfstv94=</DigestValue>
    </Reference>
    <Reference URI="#idOfficeObject" Type="http://www.w3.org/2000/09/xmldsig#Object">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>jz3+YeVc9IzgrV35RSRwqTHigPI=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>
    e1UGq0h/07WBNX77dH8K19GsvdsNrZ1e3q04kLIJOBdUsB4Jjvnl doxGedgI9quvW8P83zz0
    :
    VSLYYIyh8qRSvHQjutrRnyvJu5KXfVctZJ7S0k1oZr4j5ZoGEobooQ==
  </SignatureValue>
  <KeyInfo>
    <KeyValue>
      <RSAKeyValue>
        <Modulus>
          yuRXCD/lgIoboSnmEz3kV9iSLqiQ+QG7IpWEgkx7x6kJZ8b9AFCISIH4bZoCZ6ICE2JfKlJ
          :
          0gB2hRQ1d3s2b10GM7dYK1yYHuP6eJ5iOwMXpzmYhsSt6krYDRhOmw==
        </Modulus>
        <Exponent>AQAB</Exponent>
      </RSAKeyValue>
    </KeyValue>
    <X509Data>
      <X509Certificate>
        MIIDYTCCAkmGAWIBAgIKOKnAvKAH45AHATANBgkqhkiG9w0BAQUFADBnMRYwFAYDVQQDEw1J
        :
        KAnqBV4=
      </X509Certificate>
    </X509Data>
  </KeyInfo>
  <Object Id="idPackageObject"
    xmlns:mdssi="http://schemas.openxmlformats.org/package/2006/digital-signature">
    <Manifest>
      <Reference
        URI="/_rels/.rels?ContentType=application/vnd.openxmlformats-package.relationships+xml"
      >
        <Transforms>
          <Transform
            Algorithm="http://schemas.openxmlformats.org/package/2006/RelationshipTransform">
            <mdssi:RelationshipReference SourceId="rId1" />
          </Transform>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>1vWU/YTF/7t6ZjnE44gAFTbZvvA=</DigestValue>
      </Reference>
    </Manifest>
  </Object>

```

```
</Reference>
<Reference
  URI="/word/_rels/document.xml.rels?ContentType=application/vnd.openxmlformats-package.relationships+xml">
  <Transforms>
    <Transform
      Algorithm="http://schemas.openxmlformats.org/package/2006/RelationshipTransform">
      <mdssi:RelationshipReference SourceId="rId3" />
      <mdssi:RelationshipReference SourceId="rId2" />
      <mdssi:RelationshipReference SourceId="rId1" />
      <mdssi:RelationshipReference SourceId="rId5" />
      <mdssi:RelationshipReference SourceId="rId4" />
    </Transform>
    <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
  </Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>zAG0Xkhww/vsV8M3Agd0/+AHFYw=</DigestValue>
</Reference>
<Reference
  URI="/word/document.xml?ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.document.main+xml">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>V8w/ettXsE3Xm+9bDUXxpQf380g=</DigestValue>
</Reference>
<Reference
  URI="/word/fontTable.xml?ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.fontTable+xml">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>avBMPJLJQE4LnLawdOhrJgKo7A4=</DigestValue>
</Reference>
<Reference
  URI="/word/settings.xml?ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.settings+xml">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>TCj0Q1LHssxSbFrNgjFvkJhJDP4=</DigestValue>
</Reference>
<Reference
  URI="/word/styles.xml?ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.styles+xml">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>1kunkUW3bF/09KfcfFszvGuMAE8=</DigestValue>
</Reference>
<Reference
  URI="/word/theme/theme1.xml?ContentType=application/vnd.openxmlformats-officedocument.theme+xml">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>njId7TpxXaw3IGZC2bqGy6DvWRw=</DigestValue>
</Reference>
<Reference
  URI="/word/webSettings.xml?ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.webSettings+xml">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>lsJpQUi3QcTiTVvBBf6+hbXAN/o=</DigestValue>
</Reference>
</Manifest>
<SignatureProperties>
```

```
<SignatureProperty Id="idSignatureTime" Target="#idPackageSignature">
  <mdssi:SignatureTime>
    <mdssi:Format>YYYY-MM-DDThh:mm:ssTZD</mdssi:Format>
    <mdssi:Value>2008-02-29T11:53:14Z</mdssi:Value>
  </mdssi:SignatureTime>
</SignatureProperty>
</SignatureProperties>
</Object>
<Object Id="idOfficeObject">
  <SignatureProperties>
    <SignatureProperty Id="idOfficeV1Details" Target="#idPackageSignature">
      <SignatureInfoV1 xmlns="http://schemas.microsoft.com/office/2006/digsig">
        <SetupID />
        <SignatureText />
        <SignatureImage />
        <SignatureComments>LangEdge Test.</SignatureComments>
        <WindowsVersion>5.1</WindowsVersion>
        <OfficeVersion>12.0</OfficeVersion>
        <ApplicationVersion>12.0</ApplicationVersion>
        <Monitors>1</Monitors>
        <HorizontalResolution>1024</HorizontalResolution>
        <VerticalResolution>768</VerticalResolution>
        <ColorDepth>16</ColorDepth>
        <SignatureProviderId>{00000000-0000-0000-0000-000000000000}</SignatureProviderId>
        <SignatureProviderUrl />
        <SignatureProviderDetails>9</SignatureProviderDetails>
        <ManifestHashAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</ManifestHashAlgorithm>
        <SignatureType>1</SignatureType>
      </SignatureInfoV1>
    </SignatureProperty>
  </SignatureProperties>
</Object>
</Signature>
```

XML 署名形式の OpenXML 署名例

付録 2. 標準長期署名仕様のOpenXML署名ファイル (sig1.xml)

注意：MS-Office2007 における検証には失敗する。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Signature Id="idPackageSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo Id="idPackageSignature-Si-3">
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
    <Reference Id="idPackageSignature-Ref-1"
      URI="#idPackageObject" Type="http://www.w3.org/2000/09/xmldsig#Object">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <DigestValue>bF22T4UPN76bYu3H7FqwtfSTv94=</DigestValue>
    </Reference>
    <Reference Id="idPackageSignature-Ref-2"
      URI="#idOfficeObject" Type="http://www.w3.org/2000/09/xmldsig#Object">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <DigestValue>jz3+YeVc9IzgrV35RSRwqTHigpI=</DigestValue>
    </Reference>
    <Reference Id="idPackageSignature-Ref-7"
      URI="#idPackageSignature-Sp-6" Type="http://uri.etsi.org/01903#SignedProperties">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <DigestValue>Mc7rF9gXhagzK4Rb0I2mP0vhPrU=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue Id="idPackageSignature-Sv-4">
    Aie1tGUp2xDtW4V2y2KG1QtXn+AkDKSV1w5U5zIz6P4c/GiY8yTHaP0gndRxu1ZMymxtcZmwZlWzOT5NHe328JTXT
    :
    mx6PzzIOBrKoHoey7g3cjeFt9kp/54uM69nHF6M0daTCocqYg==
  </SignatureValue>
  <KeyInfo Id="idPackageSignature-Key-5">
    <X509Data>
      <X509Certificate>
        MIIDYTCCAkmGAWIBAgIKOKnAvKAH45AHATANBgkqhkiG9w0BAQUFADBnMRYwFAYDVQQDEw1JY2hpcm8gVGFuYWt
        :
        8qYYZdBHbwQF73N83qybdrlSU29CfKANqBV4=
      </X509Certificate>
    </X509Data>
    <KeyValue>
      <RSAKeyValue>
        <Modulus>
          yuRXCD/lgloboSnMEz3kV9iSLqiQ+QG7IpWEgkx7x6kJZ8b9AfCISIIH4bZoCZ6ICE2JfKLJ3IuJTfa5Kw842R
          :
          eJ5iOwMXpzmYhsSt6krYDRhOmw==
        </Modulus>
      </RSAKeyValue>
    </KeyValue>
  </KeyInfo>
</Signature>
```

```

    <Exponent>AQAB</Exponent>
  </RSAKeyValue>
</KeyValue>
</KeyInfo>
<Object Id="idPackageObject"
  xmlns:mdssi="http://schemas.openxmlformats.org/package/2006/digital-signature">
  <Manifest>
    <Reference
      URI="/_rels/.rels?ContentType=application/vnd.openxmlformats-package.relationships+xml"
    >
      <Transforms>
        <Transform
          Algorithm="http://schemas.openxmlformats.org/package/2006/RelationshipTransform">
          <mdssi:RelationshipReference SourceId="rId1" />
        </Transform>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>1vWU/YTF/7t6ZjnE44gAFTbZvvA=</DigestValue>
      </Reference>
    <Reference
      URI="/word/_rels/document.xml.rels?ContentType=application/vnd.openxmlformats-package.r
relationships+xml">
      <Transforms>
        <Transform
          Algorithm="http://schemas.openxmlformats.org/package/2006/RelationshipTransform">
          <mdssi:RelationshipReference SourceId="rId3" />
          <mdssi:RelationshipReference SourceId="rId2" />
          <mdssi:RelationshipReference SourceId="rId1" />
          <mdssi:RelationshipReference SourceId="rId5" />
          <mdssi:RelationshipReference SourceId="rId4" />
        </Transform>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>zAG0Xkhww/vsV8M3Agd0/+AHFYw=</DigestValue>
      </Reference>
    <Reference
      URI="/word/document.xml?ContentType=application/vnd.openxmlformats-officedocument.wordp
rocessingml.document.main+xml">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <DigestValue>V8w/ettXsE3Xm+9bDUXxpQf380g=</DigestValue>
    </Reference>
    <Reference
      URI="/word/fontTable.xml?ContentType=application/vnd.openxmlformats-officedocument.word
processingml.fontTable+xml">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <DigestValue>avBMPJLJQE4LnLawdOhrJgKo7A4=</DigestValue>
    </Reference>
    <Reference
      URI="/word/settings.xml?ContentType=application/vnd.openxmlformats-officedocument.wordp
rocessingml.settings+xml">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
      <DigestValue>TCj0Q1LHssxSbFrNgjFvkJhJDP4=</DigestValue>
    </Reference>
  </Reference>

```

```

URI="/word/styles.xml?ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.styles+xml">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>1kunkUW3bF/09KfcfFszvGuMAE8=</DigestValue>
</Reference>
<Reference
  URI="/word/theme/theme1.xml?ContentType=application/vnd.openxmlformats-officedocument.theme+xml">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>njId7TpxXaw3IGZC2bqGy6DvWRw=</DigestValue>
</Reference>
<Reference
  URI="/word/webSettings.xml?ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.webSettings+xml">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>lsJpQUi3QcTiTVvBBf6+hbXAN/o=</DigestValue>
</Reference>
</Manifest>
<SignatureProperties>
  <SignatureProperty Id="idSignatureTime" Target="#idPackageSignature">
    <mdssi:SignatureTime>
      <mdssi:Format>YYYY-MM-DDThh:mm:ssTZD</mdssi:Format>
      <mdssi:Value>2008-02-29T11:53:14Z</mdssi:Value>
    </mdssi:SignatureTime>
  </SignatureProperty>
</SignatureProperties>
</Object>
<Object Id="idOfficeObject">
  <SignatureProperties>
    <SignatureProperty Id="idOfficeV1Details" Target="#idPackageSignature">
      <SignatureInfoV1 xmlns="http://schemas.microsoft.com/office/2006/digsig">
        <SetupID />
        <SignatureText />
        <SignatureImage />
        <SignatureComments>LangEdge Test.</SignatureComments>
        <WindowsVersion>5.1</WindowsVersion>
        <OfficeVersion>12.0</OfficeVersion>
        <ApplicationVersion>12.0</ApplicationVersion>
        <Monitors>1</Monitors>
        <HorizontalResolution>1024</HorizontalResolution>
        <VerticalResolution>768</VerticalResolution>
        <ColorDepth>16</ColorDepth>
        <SignatureProviderId>{00000000-0000-0000-0000-000000000000}</SignatureProviderId>
        <SignatureProviderUrl />
        <SignatureProviderDetails>9</SignatureProviderDetails>
        <ManifestHashAlgorithm>http://www.w3.org/2000/09/xmldsig#sha1</ManifestHashAlgorithm>
        <SignatureType>1</SignatureType>
      </SignatureInfoV1>
    </SignatureProperty>
  </SignatureProperties>
</Object>
<Object Id="idPackageSignature-XAdES-Object">
  <QualifyingProperties Target="#idPackageSignature"
    xmlns="http://uri.etsi.org/01903/v1.3.2#">
    <SignedProperties Id="idPackageSignature-Sp-6">
      <SignedSignatureProperties>

```

```
<SigningTime>2008-03-05T11:39:12Z</SigningTime>
<SigningCertificate>
  <Cert>
    <CertDigest>
      <DigestMethod
        Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
        xmlns="http://www.w3.org/2000/09/xmldsig#" />
      <DigestValue xmlns="http://www.w3.org/2000/09/xmldsig#">
        ZgyYb+2T6cEB02owcpCsvuSbzJ0=
      </DigestValue>
    </CertDigest>
    <IssuerSerial>
      <X509IssuerName xmlns="http://www.w3.org/2000/09/xmldsig#">
        C=JP - 日本, E="", OU=Sales, O=Anntena House, CN=Ichiro Tanaka
      </X509IssuerName>
      <X509SerialNumber xmlns="http://www.w3.org/2000/09/xmldsig#">
        985383616336649765521153
      </X509SerialNumber>
    </IssuerSerial>
  </Cert>
</SigningCertificate>
<SignaturePolicyIdentifier>
  <SignaturePolicyImplied />
</SignaturePolicyIdentifier>
</SignedSignatureProperties>
</SignedProperties>
</QualifyingProperties>
</Object>
</Signature>
```

標準長期署名形式の OpenXML 署名例