XAdES 長期署名プロファイル

2005 年 8 月 10 日

次世代電子商取引推進協議会（ECOM）

1. XML 形式の長期署名フォーマット

本稿では、XML 署名に適用する長期署名フォーマットのプロファイルを示す。ここで示す長期署名フォーマットのプロファイルは、ETSI[1] TS 101 903 V1.3.1(2005-05), “XML Advanced Electronic Signatures(XAdES)”に準拠するものであり、CMS 長期署名フォーマットである ETSI TS101 703 V1.5.1(2003-12) “Electronic Signature Formats”とほぼ同等の内容を XML 署名に適用するものである。今回同時に策定する CMS 長期署名フォーマットのプロファイルでは、ETSI TS101 703 V1.5.1(2003-12) “Electronic Signature Formats”から必要なものを抽出したサブセットとして定義したが、XAdES は ETSI TS101 703 V1.5.1(2003-12) “Electronic Signature Formats”と内容的に同等なことから、本稿で示す署名フォーマットのプロファイルも XAdES のサブセットとし、内容的には CMS 長期署名フォーマットのプロファイルに沿った形で定義する。

なお、XAdES には W3C の Note[2]としても公開されている V1.1.1 (2002-02)、既に策定され ETSI 公開されている ETSI TS 101 903 V1.2.2(2004-4)、および現在策定中でありドラフト版である ETSI TS 101 903 V1.3.1(2005-05)、の 3 つのバージョンが存在する。国内の動向を見ると未だそれほど実装が進んでいないが、現在策定中の最新バージョンは V1.1.1 (2002-02)と同様に W3C の Note として公開される予定もあり、今後の実装や普及が見込まれる。そこで本稿では、現在の最新ドラフトである V1.3.1(2005-05)に準拠する形で示す。

2. 署名フォーマット

基本となる電子署名文書の形式として、署名ポリシの有無により”Basic Electronic Signature”(XAdES-BES)、”Explicit Policy based Electronic Signature”(XAdES-EPES)の２通りを利用できる。署名ポリシとは、署名者と検証者がデジタル署名を有効とみなすための、署名の生成と検証に関する一連の規則を定めるものである。署名ポリシについては、ETSI TR 102 038 V1.1.1(2002-04), "XML format for signature policies"にコンピュータ処理可能な XML 形式のフォーマットを規定しており、記述内容は CMS 長期署名フォーマット同様 RFC3125, "Electronic Signature Policies" とまったく同じものである。

電子署名文書の形式は、W3C/IETF Recommendation (February 2002):”XML-Signature Syntax and Processing” （XMLDSIG）の仕様に基づいている。

2.1. XML 署名の基本フォーマット

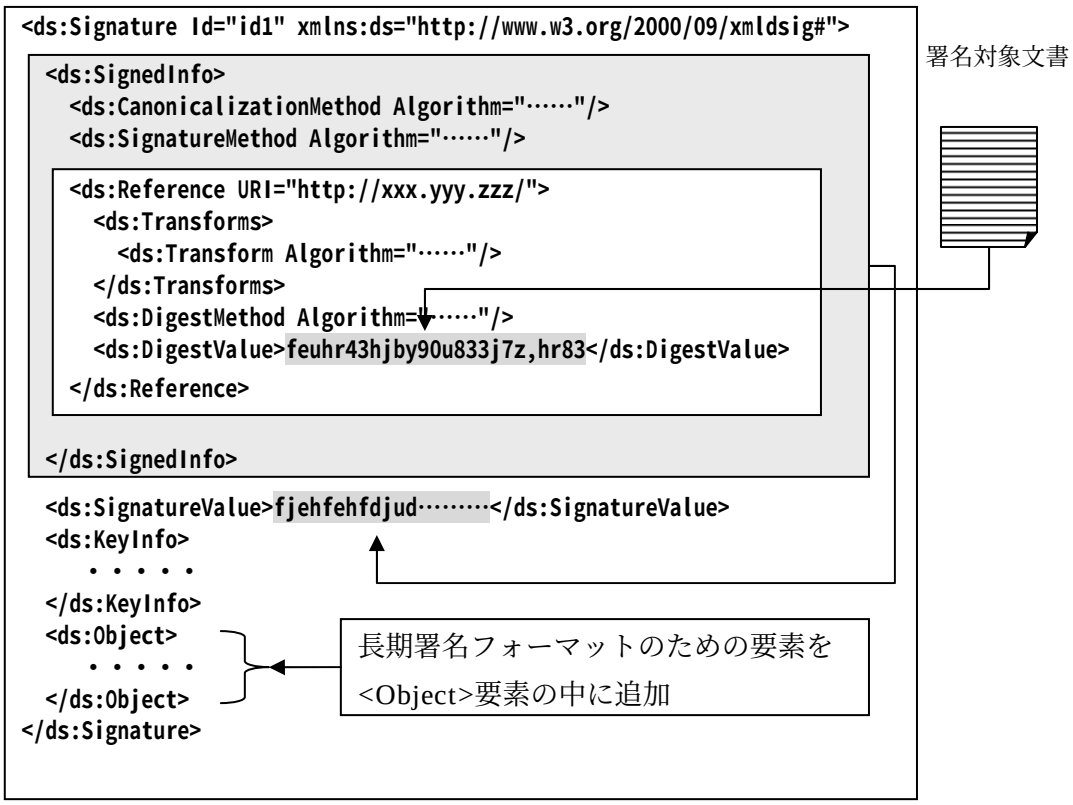
XML 形式の電子署名文書の基本フォーマットは、XMLDSIG に定義されている通りである。リスト 1 に基本的な XML 署名フォーマットの例を示す。

---

[1] http://www.etsi.org/

[2] http://www.w3.org/TR/XAdES/

リスト 1：基本的な XML 署名フォーマットの例



XML 署名では、署名対象を XML 署名文書の<ds:Reference>要素の URI 属性で指定する。署名対象は複数指定することができ、同じ XML 文書内の<ds:Signature>要素より上位の要素（Enveloped 形式）、<ds:Object>要素の中に含まれる要素（Enveloping 形式）、<ds:Signature>要素と親子関係のない要素、および XML 署名文書とは別ファイルの任意のフォーマットの文書（Detached 形式）を指定することができる。XML 署名文書と別ファイルを署名対象文書とする Detached 形式の XML 署名文書を長期保存する場合、署名対象文書は別途保存しておくことを推奨する。

2.2. 長期署名フォーマット

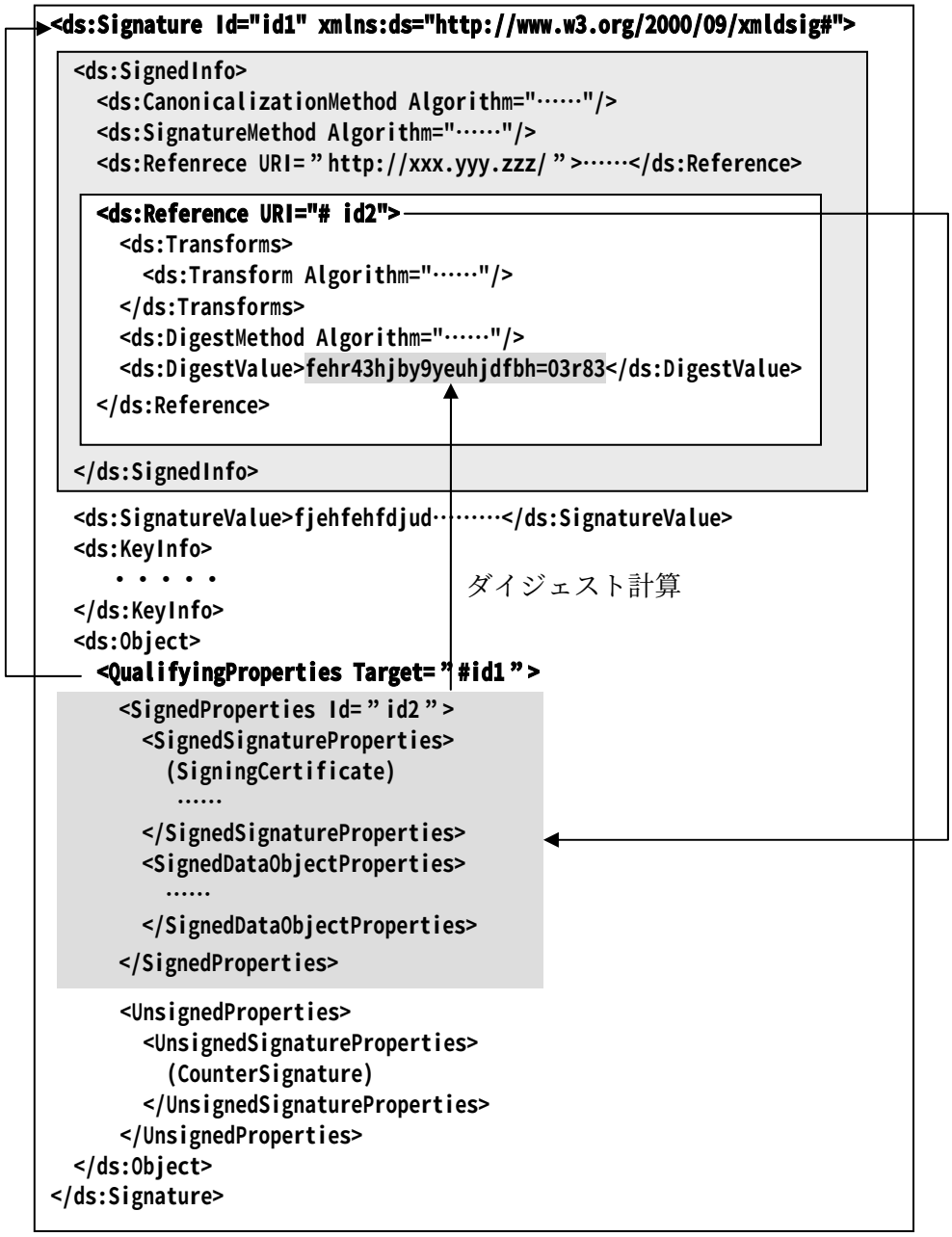
XAdES(V1.3.1)では、基本となる署名形式として”Basic Electronic Signature”(XAdES-BES)、”Explicit Policy based Electronic Signature”(XAdES-EPES)、Electronic Signature with Time(XAdES-T)および Electronic Signature with Complete Validation Data References(XAdES-C)の 4 つが定義されている。

2.2.1. XAdES の基本フォーマット

XAdES の基本となる署名フォーマットは、XMLDSIG の<ds:Object>要素内に必要な情

報が追加された形をとる。リスト 2 に XAdES の基本フォーマットを示し、リスト中の要素について説明する。

リスト 2：XAdES-BES のフォーマット



(1) QualifyingProperties 要素

この要素は、<ds:Object>要素内に含められ長期保存に必要な要素を格納するコンテナの役割を果たす。リスト 3 に QualifyingProperties 要素の XMLSchema 定義を示す。

リスト 3：QualifyingProperties 要素の XMLSchema 定義

```
<xsd:element name="QualifyingProperties" type="QualifyingPropertiesType"/>
<xsd:complexType name="QualifyingPropertiesType">
  <xsd:sequence>
    <xsd:element name="SignedProperties"
                 type="SignedPropertiesType"   minOccurs="0"/>
    <xsd:element name="UnsignedProperties"
                 type="UnsignedPropertiesType" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Target" type="xsd:anyURI" use="required"/>
  <xsd:attribute name="Id"     type="xsd:ID"     use="optional"/>
</xsd:complexType>
```

QualifyingProperties 要素には、署名値の計算対象となる SignedProperties 要素と、署名値の計算対象にはならない UnsignedProperties 要素の二つの要素が含まれる。また、SignedProperties 要素は必ずひとつ存在しなくてはならない。Target 属性は必須属性であり、ds:Signature 要素の Id 属性を参照する必要がある。

(2) SignedProperties 要素

この要素は、XMLDSIG の署名値の計算対象となるよう、ds:Reference タグで参照される。この要素には署名計算の時に一つだけ SignedSignatureProperties 要素を含まなくてはならず、SignedDataObjectProperties 要素を含む場合もある。リスト 4 に SignedProperties 要素の XMLSchema 定義を示す。

リスト 4：SignedProperties 要素の XMLSchema 定義

```
<xsd:element name="SignedProperties" type="SignedPropertiesType" />
<xsd:complexType name="SignedPropertiesType">
  <xsd:sequence>
    <xsd:element name="SignedSignatureProperties"
                 type="SignedSignaturePropertiesType"/>
    <xsd:element name="SignedDataObjectProperties"
                 type="SignedDataObjectPropertiesType" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

また、SignedProperties 要素を参照している ds:Reference 要素の Type 属性に以下の値をセットしなければならない。

http://uri.etsi.org/01903/V1.3.1#SignedProperties

(3) UnsignedProperties 要素

この要素は、署名されない特性を持つ。リスト 5 に UnsignedProperties 要素の XMLSchema 定義を示す。

リスト 5：UnsignedProperties 要素の XMLSchema 定義

```
<xsd:element name="UnsignedProperties" type="UnsignedPropertiesType" />
<xsd:complexType name="UnsignedPropertiesType">
  <xsd:sequence>
    <xsd:element name="UnsignedSignatureProperties"
                 type="UnsignedSignaturePropertiesType" minOccurs="0"/>
    <xsd:element name="UnsignedDataObjectProperties"
                 type="UnsignedDataObjectPropertiesType" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

(4) SignedSignatureProperties 要素

この要素は、QualifyingProperties 要素の Target 属性で指定された XML 署名を限定する特性を子要素に持ち、XML 署名の署名対象として署名計算に含められる。リスト 6 に SignedSignatureProperties 要素の XMLSchema 定義を示す。

リスト 6：SignedSignatureProperties 要素の XMLSchema 定義

```
<xsd:element name="SignedSignatureProperties"
             type="SignedSignaturePropertiesType" />

<xsd:complexType name="SignedSignaturePropertiesType">
  <xsd:sequence>
    <xsd:element name="SigningTime"
                 type="xsd:dateTime" minOccurs="0"/>
    <xsd:element name="SigningCertificate"
                 type="CertIDListType" minOccurs="0"/>
    <xsd:element name="SignaturePolicyIdentifer"
                 type="SignaturePolicyIdentifierType" minOccurs="0"/>
    <xsd:element name="SignatureProductionPlace"
                 type="SignatureProductionPlaceType"  minOccurs="0"/>
    <xsd:element name="SignerRole"
                 type="SignerRoleType" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

(5) UnsignedSignatureProperties 要素

この要素は、QualifyingProperties 要素の Target 属性で指定された XML 署名を限定する特性を子要素に持ち、XML 署名の署名対象として署名計算に含められない。リスト 7 に UnsignedSignatureProperties 要素の XMLSchema を示す。

リスト 7：UnsignedSignatureProperties 要素の XMLSchema 定義

```
<xsd:element name="UnsignedSignatureProperties"
             type="UnsignedSignaturePropertiesType"/>

<xsd:complexType name="UnsignedSignaturePropertiesType">
  <xsd:choice maxOccurs="unbounded">
    <xsd:element name="CounterSignature"
                 type="CounterSignatureType" />
    <xsd:element name="SignatureTimeStamp"
                 type="XAdESTimeStampType/>
    <xsd:element name="CompleteCertificateRefs"
                 type="CompleteCertificateRefsType"/>
    <xsd:element name="CompleteRevocationRefs"
                 type="CompleteRevocationRefsType"/>
    <xsd:element name="AttributeCertificateRefs"
                 type="CompleteCertificateRefsType"/>
    <xsd:element name="AttributeRevocationRefs"
                 type="CompleteRevocationRefsType"/>
    <xsd:element name="SigAndRefsTimeStamp"
                 type="XAdESTimeStampType"/>
    <xsd:element name="RefsOnlyTimeStamp"
                 type="XAdESTimeStampType"/>
    <xsd:element name="CertificateValues"
                 type="CertificateValuesType"/>
    <xsd:element name="RevocationValues"
                 type="RevocationValuesType"/>
    <xsd:element name="ArchiveTimeStamp"
                 type="XAdESTimeStampType"/>
  </xsd:choice>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

この要素には、以降で説明する様々な XAdES の形式で使われる長期保存に必要な要素が含められる。

(6) SignedDataObjectProperties 要素

この要素は、幾つかの署名されたデータオブジェクトを限定するような特性を含み、署名値の計算で計算対象とされる要素である。リスト 8 に SignedDataObjectProperties 要素の XMLSchema 定義を示す。

リスト 8：SignedDataObjectProperties 要素の XMLSchema 定義

```
<xsd:element name="SignedDataObjectProperties"
             type="SignedDataObjectPropertiesType"/>

<xsd:complexType name="SignedDataObjectPropertiesType">
  <xsd:sequence>
    <xsd:element name="DataObjectFormat"
                 type="DataObjectFormatType"
                 minOccurs="0" maxOccurs="unbounded"/>
    <xsd:element name="CommitmentTypeIndication"
                 type="CommitmentTypeIndicationType"
                 minOccurs="0" maxOccurs="unbounded"/>
    <xsd:element name="AllDataObjectsTimeStamp"
                 type="XAdESTimeStampType"
                 minOccurs="0" maxOccurs="unbounded"/>
    <xsd:element name="IndividualDataObjectsTimeStamp"
                 type="XAdESTimeStampType"
                 minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

(7) UnsignedDataObjectProperties 要素

この要素は、幾つかの署名されたデータオブジェクトを限定するような特性を含み、署名値の計算計算対象とされない要素である。リスト 9 に UnsignedDataObjectProperties 要素の XMLSchema 定義を示す。UnsignedDataObjectProperties については、ETSI TS101 703 V1.5.1(2003-12)では記述されていないが、将来の拡張性と完全性のブレを吸収するために定義する。

リスト 9：UnsignedDataObjectProperties 要素の XMLSchema 定義

```
<xsd:element name="UnsignedDataObjectProperties"
             type="UnsignedDataObjectPropertiesType" />

<xsd:complexType name="UnsignedDataObjectPropertiesType">
  <xsd:sequence>
    <xsd:element name="UnsignedDataObjectProperty"
                 type="AnyType" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

2.2.2. データ型定義

(1) AnyType データ型

このデータ型は、要素の内容を特に規定したくない場合に用いる。このデータ型の要素の要素内容には、任意の要素やテキストなどを保持できる。また、任意の属性を制限なく追加することが出来る。リスト 10 に AnyType データ型の XMLShema 定義を示す。

リスト 10：AnyType データ型の XMLSchema 定義

```
<xsd:complexType name="AnyType" mixed="true">
  <xsd:sequence minOccurs="0" maxOccurs="unbounded">
    <xsd:any namespace="##any" processContents="lax"/>
  </xsd:sequence>
  <xsd:anyAttribute namespace="##any"/>
</xsd:complexType>
```

(2) ObjectIdentifierType データ型

このデータ型は、オブジェクト識別子(OID)を格納するためのデータ型である。リスト 11 に ObjectIdentifierType データ型の XMLSchema 定義を示す。Identifier 要素では、ASN.1 におけるオブジェクトを識別する OID と XML のリソースを識別する URI の両方を指定することが出来る。

- XML リソースを指定する場合、Identifier 要素内に URI を記述する。Qualifier 属性は利用しない。
- ASN.1 で利用される OID でリソースを指定する場合は、URN の形式または URI としてエンコードした形で指定する。Qualifier 属性はどちらのエンコードが使われているかを示すために使われ、OIDAsURN、OIDAsURI のどちらかの値を取る。

Description 要素はオプションの要素で、オブジェクト識別子に関する説明文を格納する。また、DocumentationReferences 要素もオプションの要素で、オブジェクト識別子の追加説明への任意の個数の参照が含まれる。

リスト 11：ObjectIdentifier データ型の XMLSchema 定義

```
<xsd:complexType name="ObjectIdentifierType">
  <xsd:sequence>
    <xsd:element name="Identifier" type="IdentifierType"/>
    <xsd:element name="Description" type="xsd:string" minOccurs="0"/>
    <xsd:element name="DocumentationReferences"
                 type="DocumentationReferencesType" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="IdentifierType">
  <xsd:simpleContent>
    <xsd:extension base="xsd:anyURI">
      <xsd:attribute name="Qualifier" type="QualifierType"  use="optional"/>
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>
<xsd:simpleType name="QualifierType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="OIDAsURI"/>
    <xsd:enumeration value="OIDAsURN"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:complexType name="DocumentationReferencesType">
  <xsd:sequence maxOccurs="unbounded">
    <xsd:element name="DocumentationReference" type="xsd:anyURI"/>
  </xsd:sequence>
</xsd:complexType>
```

(3) EncapsulatedPKIDataType データ型

このデータ型は、ASN.1 でエンコードされたデータを XML 文書に格納するために使われる。例えば、X.509 証明書や、失効リスト、属性証明書やタイムスタンプのデータを格納するために使われる。格納時は、これらのデータを base64 でエンコードして格納する。Encoding 属性には、ASN.1 データのエンコード方法を URI で記述する。記述できる URI を表 1 に示す。リスト 12 に EncapsulatedPKIDataType データ型の XMLSchema 定義を示す。

表 1：ASN.1 データのエンコード方法に関する URI

エンコード方法	URI
DER	http://uri.etsi.org/01903#DER
BER	http://uri.etsi.org/01903#BER
CER	http://uri.etsi.org/01903#CER

PER	http://uri.etsi.org/01903#PER
XER	http://uri.etsi.org/01903#XER

リスト 12：EncapsulatedPKIDataType データ型の XMLSchema 定義

```
<xsd:complexType name="EncapsulatedPKIDataType">
  <xsd:simpleContent>
    <xsd:extension base="xsd:base64Binary">
      <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
      <xsd:attribute name="Encoding" type="xsd:anyURI"
        use="optional"/>
    </xsd:extension>
  </xsd:simpleContent>
</xsd:complexType>
```

(4) XAdESTimeStampType データ型

タイムスタンプを格納するデータ XAdESTimeStampType データ型は GenericTimeStampType データ型の派生として定義される。GenericTimeStampType データ型からは、XAdESTimeStampType データ型と OtherTimeStampType データ型が派生して定義されるが、OtherTimeStampType データ型は非推奨である。リスト 13 に GenericTimeStampType データ型の XMLSchema 定義を示す。また、それから派生される XAdESTimeStampType データ型の XMLSchema 定義をリスト 14 に示す。

リスト 13：GenericTimeStampType データ型の XMLSchema 定義

```
<xsd:element name=”Include” type=”IncludeType”>
<xsd:complexType name="IncludeType">
  <xsd:attribute name="URI" type="xsd:anyURI" use="required"/>
  <xsd:attribute name="referencedData" type="xsd:boolean" use="optional"/>
</xsd:complexType>

<xsd:element name="ReferenceInfo" type="ReferenceInfoType"/>
<xsd:complexType name="ReferenceInfoType">
  <xsd:sequence>
    <xsd:element ref="ds:DigestMethod"/>
    <xsd:element ref="ds:DigestValue"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
  <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>

<xsd:complexType name="GenericTimeStampType" abstract="true">
  <xsd:sequence>
    <xsd:choice minOccurs="0">
      <xsd:element ref="Include" maxOccurs="unbounded"/>
      <xsd:element ref="ReferenceInfo" maxOccurs="unbounded"/>
    </xsd:choice>
    <xsd:element ref="ds:CanonicalizationMethod" minOccurs="0"/>
    <xsd:choice maxOccurs="unbounded">
      <xsd:element name="EncapsulatedTimeStamp"
                   type="EncapsulatedPKIDataType"/>
      <xsd:element name="XMLTimeStamp" type="AnyType"/>
    </xsd:choice>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

リスト 14：XAdESTimeStampType データ型の XMLSchema 定義

```
<xsd:element name="XAdESTimeStamp" type="XAdESTimeStampType"/>

<xsd:complexType name="XAdESTimeStampType">
  <xsd:complexContent>
    <xsd:restriction base="GenericTimeStampType">
      <xsd:sequence>
        <xsd:element ref="Include"  minOccurs="0" maxOccurs="unbounded"/>
        <xsd:element ref="ds:CanonicalizationMethod" minOccurs="0"/>
        <xsd:choice maxOccurs="unbounded">
          <xsd:element name="EncapsulatedTimeStamp"
                       type="EncapsulatedPKIDataType"/>
          <xsd:element name="XMLTimeStamp" type="AnyType"/>
        </xsd:choice>
      </xsd:sequence>
      <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
    </xsd:restriction>
  </xsd:complexContent>
</xsd:complexType>
```

XAdESTimeStampType データ型の要素にタイムスタンプトークンが含められることになるが、TSA へ送るダイジェスト値の算出方法に関しては 2 通りの方法を定義する。

- Implicit Mode
  XAdESTimeStampType の要素の中に Include 要素がない場合、TSA へ送付するダイジェスト値の計算対象となる XAdES 要素の指定は暗黙的に実行される。処理手順は以下のようになる。

  Signed Properties の場合

  1. 各 XAdESTimeStampType 型の要素の仕様として指示されている要素や署名された要素内容を取り出す。
  2. 取り出した要素や署名された要素内容に対して、もし対象としている XAdESTimeStampType 型の要素内に ds:Canonicalization 要素が存在すれば、それに従った正規化を行う。ds:Canonicalization 要素が存在しなければ、XMLDSIG で標準的な正規化手法で正規化する。
  3. 処理された各データを連結する。

  Unsigned Properties の場合

  1. タイムスタンプトークンを含むプロパティより前に現れる、

UnsignedSignatureProperties の子要素を全て取り出す。

2. 取り出した要素のそれぞれについて、もし対象としている XAdESTimeStampType 型の要素内に ds:Canonicalization 要素が存在すれば、それに従った正規化を行う。ds:Canonicalization 要素が存在しなければ、XMLDSIG で標準的な正規化手法で正規化する。

3. 処理された各データを連結する。

どちらの場合も連結されたデータをもとにダイジェスト値を計算し、TSA に送付する。また、以下の要素はこのモードで計算される。

- SignatureTimeStamp 要素
- RefsOnlyTimeStamp 要素
- SigAndRefsTimeStamp 要素

- Include Mode
  XAdESTimeStampType の要素の中に Include 要素がある場合、TSA へ送付するダイジェスト値の計算対象となる XAdES 要素の指定は明示的に処理される。Include 要素の URI 属性は、TSA へ送付するダイジェスト計算の計算対象を参照する。ds:Reference 要素自体を参照する場合は、XAdESTimeStampType の要素に referencedData 属性が存在する場合がある。その値が ture の場合は、XMLDSIG の処理モデル従って ds:Reference 要素を処理した結果を元にタイムスタンプを計算することになる。もし、referencedData 属性が存在しないか、値が false である場合は、ds:Refernece 要素自体を計算対象とする。各 Include 要素は以下のような手順に従って処理される。

  1. URI 属性で参照されているデータを取り出す。

  2. 取り出したデータが ds:Reference 要素で referneceData 属性が true の場合、取り出された ds:Reference 要素を XMLDSIG の処理モデルに従って処理しその結果を得る。referencedData 属性が存在しない場合、または値が false である場合は ds:Reference 要素自体を計算対象として取り出す。

  3. 取り出した結果データが XML 形式の場合は、ds:Canonicalization 要素に従って正規化を行う。ds:Canonicalization 要素がない場合は、

XMLDSIG で使われる標準的な正規化手法が使われる。

4. 計算結果を処理済の Include 要素の計算結果につなぎ合わせる。

連結されたデータをもとにダイジェスト値を計算し、TSA に送付する。また、以下の要素はこのモードで計算される。

- AllDataObjectsTimeStamp 要素
- IndividualDataObjectsTimeStamp 要素

なお、ArchiveTimeStamp 要素については両方のモードが利用される。

2.2.3. Basic electronic signature (XAdES-BES)

XAdES-BES では、以下のどちらか一方が必須となる。

- <SignedSignatureProperties>要素の中に<SigningCertificate>要素を含み、署名値計算の対象として署名計算に含める。
- <ds:Signature>要素に<ds:KeyInfo>を含み、署名値計算の対象として署名計算に含める。

以降、それぞれについて説明する。

(1) SigningCertificate 要素

この要素には、署名者証明書のダイジェスト値と証明書への参照を含めなければならない。また、信頼点までの証明書チェーンを構成する証明書のダイジェスト値とシリアル番号を含むことも出来る。ただし、署名ポリシで規定されている場合には、信頼点までの証明書チェーンを構成する証明書のダイジェスト値と発行者のシリアル番号を含まなければならない。リスト 15 に SigningCertificate 要素の XMLSchema 定義を示す。なお、ここで言う証明書の参照とは、証明書を発行した認証局の DN と証明書のシリアル番号を含む ds:X509IssuerSerialType 型の要素<IssuerSerial>で表現される。

この要素は、SigndProperties の含まれる他の要素とともに署名値の計算対象として署名計算に含められる。

これらの要素は、Simple sustitution 攻撃を防ぐために用いる。

リスト 15：SigningCertificate 要素の XMLSchema 定義

```
<xsd:element name="SigningCertificate" type="CertIDListType"/>

<xsd:complexType name="CertIDListType">
  <xsd:sequence>
    <xsd:element name="Cert" type="CertIDType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CertIDType">
  <xsd:sequence>
    <xsd:element name="CertDigest" type="DigestAlgAndValueType"/>
    <xsd:element name="IssuerSerial" type="ds:X509IssuerSerialType"/>
  </xsd:sequence>
  <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>

<xsd:complexType name="DigestAlgAndValueType">
  <xsd:sequence>
    <xsd:element ref="ds:DigestMethod"/>
    <xsd:element ref="ds:DigestValue"/>
  </xsd:sequence>
</xsd:complexType>
```

(2) ds:KeyInfo 要素

SigningCertificage 要素が存在しない、もしくは署名計算の対象となっていない場合は、ds:KeyInfo 要素が必須であり、以下の条件を満たさなければならない。

- ds:KeyInfo は、署名者証明書を含む ds:X509Data 要素を含まなければならない
- ds:KeyInfo は、信頼点までの証明書チェーンを構成する証明書も含む場合がある。
- ds:SignedInfo 要素の ds:Reference 要素で ds:KeyInfo を参照することにより、署名の計算対象として署名値の計算に含まれなければならない。

2.2.4. Explicit policy electronic signatures (XAdES-EPES)

XAdES-EPES は、XAdES で基本となる形式の 1 つで、XAdES-BES に署名ポリシに関する要素である SignaturePolicyIdentifier 要素を追加したものである。SignaturePolicyIdentifier 要素は、SignedSignatureProperties 要素に追加され XAdES-EPES では必須要素である（リスト 6）。この属性は、作成者の署名で保護される。

(1) SignaturePolicyIdentifier 要素

リスト 16 に SignaturePolicyIdentifier 要素の XMLSchema 定義を示す。

リスト 16：SignaturePolicyIdentifier 要素の XMLSchema 定義

```
<xsd:element name="SignaturePolicyIdentifier"
               type="SignaturePolicyIdentifierType"/>

<xsd:complexType name="SignaturePolicyIdentifierType">
  <xsd:choice>
    <xsd:element name="SignaturePolicyId"
                 type="SignaturePolicyIdType"/>
    <xsd:element name="SignaturePolicyImplied"/>
  </xsd:choice>
</xsd:complexType>

<xsd:complexType name="SignaturePolicyIdType">
  <xsd:sequence>
    <xsd:element name="SigPolicyId"
                 type="ObjectIdentifierType"/>
    <xsd:element ref="ds:Transforms" minOccurs="0"/>
    <xsd:element name="SigPolicyHash"
                 type="DigestAlgAndValueType"/>
    <xsd:element name="SigPolicyQualifiers"
                 type="SigPolicyQualifiersListType"
                 minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="SigPolicyQualifiersListType">
  <xsd:sequence>
    <xsd:element name="SigPolicyQualifier"
                 type="AnyType"
                 maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

2.2.5. XAdES-BES でオプショナルな要素

XAdES-BES では、SingedSiganture Properties 要素に以下の要素を含めることが出来る。

- SigningTime
- SignatureProductionPlace
- SignerRole

SignedDataObjectProperties 要素に以下の要素を含めることが出来る。

- DataObjectFormat
- CommitmentTypeIndication
- AllDataObjectsTimeStamp
- IndividualDataObjectsTimeStamp

UnsignedSignatureProperties 要素に以下の要素を含めることができる。

- CounterSignature

以降、それぞれを簡単に説明する。

(1) SigningTime 要素

この要素は、署名者が署名を実行した時刻を表す要素である。内部のデータ型は、W3CRecommendation “XML Schema Part2:Datatypes”で定義される xsd:dateTîme 型となる。この要素は、ひとつの署名文書のたかだか 1 つしか含まれない。リスト 17 に SigningTime の XMLSchema 定義を示す。

リスト 17：SigningTime 要素の XMLSchema 定義

```
<xsd:element  name="SigningTime"  type="xsd:dateTime"/>
```

(2) SignatureProductionPlace 要素

この要素は、署名が生成された場所を示す。リスト 18 に SignatureProductionPlace 要素の XMLSchema 定義を示す。

リスト 18：SignatureProductionPlace 要素の XMLSchema 定義

```
<xsd:element name="SignatureProductionPlace"
             type="SignatureProductionPlaceType"/>

<xsd:complexType name="SignatureProductionPlaceType">
  <xsd:sequence>
    <xsd:element name="City" type="xsd:string" minOccurs="0"/>
    <xsd:element name="StateOrProvince" type="xsd:string" minOccurs="0"/>
    <xsd:element name="PostalCode" type="xsd:string" minOccurs="0"/>
    <xsd:element name="CountryName" type="xsd:string" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
```

(3) SignerRole 要素

契約によっては、ある特定のポジションの人によって署名されたかどうかのみが重要である場合がある。この要素は、そのような場合に対応するために署名者の役割を表す要素である。リスト 19 に SignerRole 要素のの XMLSchema 定義を示す。また、署名者の役割を記述するために以下の２つの方法を定義する。

- 署名者自らが主張する役割名

ClaimedRoles 要素に役割名を含める

- 認められた役割を含む属性証明書
  CertifiedRolses 要素に属性証明書を格納する

リスト 19：SignerRole 要素の XMLSchema 定義

```
<xsd:element name="SignerRole" type="SignerRoleType"/>
<xsd:complexType name="SignerRoleType">
  <xsd:sequence>
    <xsd:element name="ClaimedRoles"
                 type="ClaimedRolesListType" minOccurs="0"/>
    <xsd:element name="CertifiedRoles"
                 type="CertifiedRolesListType" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ClaimedRolesListType">
  <xsd:sequence>
    <xsd:element name="ClaimedRole"
                 type="AnyType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CertifiedRolesListType">
  <xsd:sequence>
    <xsd:element name="CertifiedRole"
                 type="EncapsulatedPKIDataType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

(4) DataObjectFormat 要素

この要素は、署名されたデータオブジェクトのデータフォーマットを記述する要素である。この要素は、もし署名されたデータ内に暗黙のうちにデータフォーマットが含まれておらず、署名されたデータを検証のため人間のユーザに提供する場合は必須である。この要素は、署名されたデータオブジェクト毎に追加することができる。リスト 20 に DataObjectFormat 要素の XMLShema 定義を示す。

リスト 20：DataObjectFormat 要素の XMLSchema 定義

```
<xsd:element name="DataObjectFormat" type="DataObjectFormatType"/>

<xsd:complexType name="DataObjectFormatType">
  <xsd:sequence>
    <xsd:element name="Description"
                 type="xsd:string" minOccurs="0"/>
    <xsd:element name="ObjectIdentifier"
                 type="ObjectIdentifierType" minOccurs="0"/>
    <xsd:element name="MimeType"
                 type="xsd:string" minOccurs="0"/>
    <xsd:element name="Encoding"
                 type="xsd:anyURI" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="ObjectReference" type="xsd:anyURI" use="required"/>
</xsd:complexType>
```

ObjectReference 属性は必須属性であり、特定したいデータオブジェクトの対応する ds:Signature 要素内の ds:Reference 要素を参照する。その他に以下のような情報を伝達することが出来る。

- Description 要素で、署名されたデータオブジェクトに関するテキスト情報を記述できる。
- ObjectIdentifier 要素で、署名されたデータオブジェクトのタイプを指定できる。
- MimeType 要素で、署名されたデータオブジェクトの MIME type を指定できる。
- Encoding 要素で、署名されたデータオブジェクトの enoding フォーマットを指定できる。

Description 要素、ObjectIdentifier 要素および MimeType 要素のうち少なくとも 1 つが DataObjectFomat 要素中に存在しなくてはいけない。

(5) CommitmentTypeIndication 要素

リスト 21 に CommitmentTypeIndication 要素の XMLSchema 定義を示す。表 2 にコミットメントとその内容の一覧を示す。

リスト 21：CommitmentTypeIndication 要素の XMLSchema 定義

```
<xsd:element name="CommitmentTypeIndication"
             type="CommitmentTypeIndicationType"/>

<xsd:complexType name="CommitmentTypeIndicationType">
  <xsd:sequence>
    <xsd:element name="CommitmentTypeId"
                 type="ObjectIdentifierType"/>
    <xsd:choice>
      <xsd:element name="ObjectReference"
                   type="xsd:anyURI" maxOccurs="unbounded"/>
      <xsd:element name="AllSignedDataObjects"/>
    </xsd:choice>
    <xsd:element name="CommitmentTypeQualifiers"
                 type="CommitmentTypeQualifiersListType" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CommitmentTypeQualifiersListType">
  <xsd:sequence>
    <xsd:element name="CommitmentTypeQualifier"
                 type="AnyType" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

表 2：コミットメントの種別とその内容の一覧

コミットメント	内容
Proof of origin	署名者がその文書を生成したこと、承認したこと、送信したことを示す
Proof of receipt	署名者がその文書を受け取ったことを示す
Proof of delivery	TSP(信頼できるサービスプロバイダがその文書をアクセスできる状態でローカルなストアに置いたことを提示したことを示す
Proof of sender	その提示をしたエンティティがその文書を送信したことを示す（生成したものでなくてもよい）
Proof of approval	署名者がその文書を承認したことを示す
Proof of creation	署名者がその文書を生成したことを示す（承認したり送信したりする必要はない）

(6) AllDataObjectsTimeStamp 要素

この要素は、署名計算の実行前に署名対象データに付与されたタイムスタンプ

を格納する。リスト 22 に AllDataObjectsTimeStamp 要素の XMLSchema 定義を示す。

リスト 22：AllDataObjectsTimeStamp 要素の XMLSchema 定義

```
<xsd:element name="AllDataObjectsTimeStamp" type="XAdESTimeStampType"/>
```

ds:SignedInfo に含まれていて SignedProperties 要素以外に署名者が署名したい全ての ds:Referenece を元にタイムスタンプが計算される。この要素を生成するアプリケーションは、SignedPropeties 要素で参照しているものを除く全ての ds:Refernece 要素について Include 要素を生成しなければならない。また、各 Include 要素の referencedData 属性は ture でなくてはならない。

(7) IndividualDataObjectsTimeStamp 要素

この要素は、署名計算の実行前に個別のデータに付与されたタイムスタンプを格納する。リスト 23 に IndividualDataObjectsTimeStamp 要素の XMLSchema 定義を示す。

リスト 23：IndividualDataObjectsTimeStamp 要素の XMLSchema 定義

```
<xsd:element name="IndividualDataObjectsTimeStamp" type="XAdESTimeStampType"/>
```

ds:SignedInfo に含まれている任意の ds:Reference 要素を元にタイムスタンプが計算される。ただし、SignedProperties を参照している ds:Reference 要素を対象として含むことは出来ない。アプリケーションは、SignedPropeties 要素で参照しているものを除く ds:Refernece 要素で対象とするものついては Include 要素を生成しなければならない。また、各 Include 要素の referencedData 属性は ture でなくてはならない。ひとつの XAdES の文書の中にこの要素を複数含めることが出来る。

(8) CounterSignature 要素

CounterSignature 要素は、UnsignedSingatureProperties 要素内に格納される。リスト 24 に CounterSignature 要素の XMLSchema 定義を示す。

リスト 24：CounterSignater 要素の XMLSchema 定義

```
<xsd:element name="CounterSignature" type="CounterSignatureType" />

<xsd:complexType name="CounterSignatureType">
  <xsd:sequence>
    <xsd:element ref="ds:Signature"/>
  </xsd:sequence>
</xsd:complexType>
```

2.2.6. Electronic signature with time (XAdES-T)

XAdES-T は、デジタル署名の存在時刻を確定するために電子署名文書中の署名値（ds:Signature 要素内の ds:SignedInfo 要素内の SignatureValue 要素）に対して TSA から取得したタイムスタンプトークンを追加したものである。署名値から生成したタイムスタンプトークンは、署名の存在時刻とともに、電子データの存在時刻も証明することとなる。XAdES-T の形式はは、XAdES-BES または XAdES-EPES の UnSignedSignatureProperties 要素に SignatureTimeStamp 要素を追加した形式である（UnsignedSignatureProperties 要素の XMLShema 定義はリスト 7 を参照のこと）。

(1) SignatureTimeStamp 要素

この要素は、ds:SignatureValue 要素に対して付与したタイムスタンプを格納する。1 つの署名に対して複数の異なった TSA から取得したタイムスタンプ格納するために、1 つの XAdES 文書に複数の SignatureTiemStamp 要素を格納することが出来る。リスト 25 に SignatureTimeStamp 要素の XMLSchema 定義を示す。

リスト 25：SignatureTimeStamp 要素の XMLSchema 定義

```
<xsd:element name="SignatureTimeStamp" type="XAdESTimeStampType"/>
```

この要素に含まれるタイムスタンプトークンの計算は、Implicit Mode で実行される。具体的には、ds:SignatureValue 要素が、TSA に送付されるダイジェスト値の計算の入力となる。

タイムスタンプトークン自体の検証情報（認証パス及び失効情報）は、次のいずれかに格納する。

1) タイムスタンプトークン内に含める

2) 署名者証明書の検証情報と同じ場所（Complete Certificate Refs, Complete RevocationRefs, CertificateValues, RevocationValues）

2.2.7. Electronic signature with complete validation data references (XAdES-C)

XAdES-C は、XAdES-T に CompleteCertificateRefs 要素と CompleteRevocationRefs 要素を加えたものとなる。CompleteCertificateRefs 要素は、署名者証明書の検証に使われる証明書チェーン上の全ての証明書（署名者証明書を除く）への参照をもつ。CompleteRevocationRefs 要素は、署名者証明書および CA 証明書の検証に必要な全ての失効情報への参照が格納される。

なお、後述する XAdES-A を構成するときは、CompleteCertificateRefs, CompleteRevocationRefs はオプション要素となる。

(1) CompleteCertificateRefs 要素

この要素は、XAdES 文書中に高々ひとつだけ含めることが出来る。リスト 26 に CompleteCertificateRefs 要素の XMLSchema 定義を示す。

リスト 26：CompleteCertificateRefs 要素の XMLSchema 定義

```
<xsd:element name="CompleteCertificateRefs"
             type="CompleteCertificateRefsType"/>

<xsd:complexType name="CompleteCertificateRefsType">
  <xsd:sequence>
    <xsd:element name="CertRefs" type="CertIDListType" />
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

(2) CompleteRevocationRefs 要素

リスト 27 に CompleteRevocationRefs 要素の XMLSchema 定義を示す。

リスト 27：CompleteRevocationRefs 要素の XMLSchema 定義

```
<xsd:element name="CompleteRevocationRefs" type="CompleteRevocationRefsType"/>

<xsd:complexType name="CompleteRevocationRefsType">
  <xsd:sequence>
    <xsd:element name="CRLRefs" type="CRLRefsType" minOccurs="0"/>
    <xsd:element name="OCSPRefs" type="OCSPRefsType" minOccurs="0"/>
    <xsd:element name="OtherRefs" type="OtherCertStatusRefsType"
                 minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>

<xsd:complexType name="CRLRefsType">
  <xsd:sequence>
    <xsd:element name="CRLRef" type="CRLRefType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CRLRefType">
  <xsd:sequence>
    <xsd:element name="DigestAlgAndValue" type="DigestAlgAndValueType"/>
    <xsd:element name="CRLIdentifier" type="CRLIdentifierType" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="CRLIdentifierType">
  <xsd:sequence>
    <xsd:element name="Issuer" type="xsd:string"/>
    <xsd:element name="IssueTime" type="xsd:dateTime" />
    <xsd:element name="Number" type="xsd:integer"  minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>

<xsd:complexType name="OCSPRefsType">
  <xsd:sequence>
    <xsd:element name="OCSPRef" type="OCSPRefType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="OCSPRefType">
  <xsd:sequence>
    <xsd:element name="OCSPIdentifier" type="OCSPIdentifierType"/>
    <xsd:element name="DigestAlgAndValue"
      type="DigestAlgAndValueType"
      minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
```

```
<xsd:complexType name="OCSPIdentifierType">
  <xsd:sequence>
    <xsd:element name="ResponderID" type="xsd:string"/>
    <xsd:element name="ProducedAt" type="xsd:dateTime"/>
  </xsd:sequence>
  <xsd:attribute name="URI" type="xsd:anyURI" use="optional"/>
</xsd:complexType>

<xsd:complexType name="OtherCertStatusRefsType">
  <xsd:sequence>
    <xsd:element name="OtherRef" type="AnyType"
      maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

ETSI TS 101 903 V1.3.1(2005-05)では、署名の中に属性証明書が含まれる場合は、AttributeCertifcateRefs 要素と AttributeRevocationRefs 要素も加えることが出来るように定義されている。しかし、本書の効果的かつ効率的（必要最低限の）プロファイルを提示するという方針に従い、AttributeCertificate には言及しないこととする。

2.2.8. Extended signatures with time forms (XAdES-X)

XAdES-X は、将来の CA の危殆化に備えたり、検証データの完全性を確保したり検証データが入手困難になることに備えるため、XAdES-C を拡張したものである。拡張の仕方により 2 種類プロファイルを定義する。

なお、後述する XAdES-A 形式を構成する場合、XAdES-X として追加される SigAndRefsTimeStamp 要素および RefsOnlyTimeStamp 要素はオプション要素である。

- XAdES-X type1
  XAdES-C 全体に対するタイムスタンプを取得して追加するもので、具体的には UnsingedSignatureProperties 要素に SigAndRefsTimeStamp 要素を追加したものである（UnsignedSignatureProperties 要素の XMLSchema 定義はリスト 7 を参照のこと）。複数の TSP からタイムスタンプを取得する考慮して、複数の SigAndRefsTimeStamp 要素を追加することができるよう定義する。タイムスタンプを取得するために TSP に送信するハッシュ値は、SignatureValue 要素、SignatureTimeStamp 要素、CompleteCertificateRefs 要素および CompleteRevocationRefs 要素を元に計算する。

- XAdES-X type2
  検証情報のリファレンスのみに対するタイムスタンプを取得して追加するもので、具

体的にはUnsignedSignaturePropertiesに RefsOnlyTimeStamp 要素を追加したものである（UnsignedSignatureProperties 要素の XMLSchema 定義はリスト 7 を参照のこと）。複数の TSP からタイムスタンプを取得する考慮して、複数の RefsOnlyTimeStamp 要素を追加することができるよう定義する。タイムスタンプを取得するために TSP に送信するハッシュ値は、CompleteCertificateRefs 要素および CompleteRevocationRefs 要素を元に計算する。

(1) SigAndRefsTimeStamp 要素

この要素に含まれるタイムスタンプトークンの計算は、Implicit Mode で実行される。具体的には、ds:SignatureValue 要素およびすべての SignatureTimeStamp 要素を正規化して連結する。次に、CompleteCertificateRefs 要素、CompleteRevocationRefs 要素をそれぞれ正規化し、XAdES 文書内の出現順序に従って連結する。連結した結果が TSA に送付されるダイジェスト値の計算の入力となる。リスト 28 に SigAndRefsTimeStamp 要素の XMLSchema 定義を示す。

リスト 28：SigAndRefsTimeStamp 要素の XMLSchema 定義

```
<xsd:element name="SigAndRefsTimeStamp" type="XAdESTimeStampType"/>
```

(2) RefsOnlyTimeStamp 要素

この要素には、CompleteCertificateRefs 要素、CompleteRevocationRefs 要素を連結したデータを下に計算したタイムスタンプが格納される。この要素に含まれるタイムスタンプトークンの計算は、Implicit Mode で実行される。具体的には、CompleteCertificateRefs 要素、CompleteRevocationRefs 要素をそれぞれ正規化し、XAdES 文書内の出現順序に従って連結する。連結した結果が TSA に送付されるダイジェスト値の計算の入力となる。リスト 29 に RefsOnlyTimeStamp 要素の XMLSchema 定義を示す。

リスト 29：RefsOnlyTimeStamp 要素の XMLSchema 定義

```
<xsd:element name="RefsOnlyTimeStamp" type="XAdESTimeStampType"/>
```

2.2.9. Extended long electronic signatures with time (XAdES-X-L)

XAdES-X-L は、XAdES-X type1 か type2 のいずれかに対して、UnsingeSignatureProperties 要素に CertificateValues 要素と RevocationValues 要素を加えたものである（UnsignedSignatureProperties 要素の XMLSchema 定義はリスト 7 を参照のこと）。

なお、後述する XAdES-A 形式を構成する場合、XAdES-X type1 や type2 に対して XAdES-X-L を構成する必要はなく、CeritificateValues 要素と RevocationValues 要素があれば良い。

(1) CertificateValues 要素

この要素は、署名者証明書および CompleteCertificateRefs 要素で参照される証明書チェーンを含まなければならない。ただし、ds:Signature 要素内の ds:KeyInfo 要素に既に含まれている証明書は CertificateValues 要素内に含む必要はない。リスト 30 に CertifiCateValues 要素の XMLSchema 定義を示す。

リスト 30：CertificateValues 要素の XMLSchema 定義

```
<xsd:element name="CertificateValues" type="CertificateValuesType"/>

<xsd:complexType name="CertificateValuesType">
    <xsd:choice minOccurs="0" maxOccurs="unbounded">
        <xsd:element name="EncapsulatedX509Certificate"
                     type="EncapsulatedPKIDataType"/>
        <xsd:element name="OtherCertificate" type="AnyType"/>
    </xsd:choice>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
```

(2) RevocationValues 要素

この要素には、署名検証に必要な証明書の証拠情報が格納される。この要素は一つの XAdES 署名文書について高々一つしか存在しない。リスト 31 に RevocationValues 要素の XMLSchema 定義を示す。

リスト 31：RevocationValues 要素の XMLSchema 定義

```
<xsd:element name="RevocationValues" type="RevocationValuesType"/>

<xsd:complexType name="RevocationValuesType">
  <xsd:sequence>
    <xsd:element name="CRLValues" type="CRLValuesType" minOccurs="0"/>
    <xsd:element name="OCSPValues" type="OCSPValuesType" minOccurs="0"/>
    <xsd:element name="OtherValues" type="OtherCertStatusValuesType"
                 minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="Id" type="xsd:ID"  use="optional"/>
</xsd:complexType>

<xsd:complexType name="CRLValuesType">
  <xsd:sequence>
     <xsd:element name="EncapsulatedCRLValue"
                  type="EncapsulatedPKIDataType"
                  maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>


<xsd:complexType name="OCSPValuesType">
  <xsd:sequence>
      <xsd:element name="EncapsulatedOCSPValue"
                   type="EncapsulatedPKIDataType" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>
```

2.2.10. Archival electronic signatures (XAdES-A)

電子署名の長期保存のためには、署名対象文書、デジタル署名、タイムスタンプおよび検証情報全体をタイムスタンプや耐タンパな仕組みで保護する必要がある。長期署名フォーマットでは、アーカイブタイムスタンプによりこれを実現する。このとき、XAdES-C や XAdES-X で利用した検証情報へのリファレンスや検証情報のリファレンスへのタイムスタンプは必要なくなり、検証情報そのものを CertificateValues や RevocationValues で確保し、アーカイブタイムスタンプを付与すればよい。

また、電子署名の検証可能期間を極めて長くしようとしたとき、タイムスタンプの署名の危殆化や TSA 証明書の有効期限切れが発生しうるため、タイムスタンプの署名を複数回重ねることが要求されることがある。このとき、ArchiveTimeStamp 要素が用いられる。このタイムスタンプは期間を置いて繰り返される。

(1) ArchiveTimeStamp 要素

この要素は、アーカイブタイムスタンプが格納される。この要素に含まれるタ

イムスタンプの含まれるハッシュ値の計算方法は以下のようになる。

1. ArchiveTimeStamp 要素内に、ds:SignedInfo 要素内の ds:Reference 毎に Include 要素を生成する。Inculde 要素の URI 属性では、それぞれ対応する ds:Reference 要素を参照する。また、referneceData 属性は ture でなければならない。
2. 以下の要素を取り出す
   - ds:SignedInfo
   - ds:SignatureValue
   - ds:KeyInfo
3. XAdES 文書中の出現順序に従い以下の要素を取り出す
   - XAdES 文書中にある SignatureTimeStamp 要素
   - 存在した場合は、CounterSignatureProperties 要素
   - 存在した場合は、CompleteCertificateRefs 要素
   - 存在した場合は、CompleteRevocationRefs 要素
   - CertificateValues 要素。存在しない場合は、追加しなくてはならない
   - RevocationValues 要素。存在しない場合は、追加しなくてはならない
   - SigAndRefsTimeStamp 要素
   - RefsOnlyTimeStamp 要素
   - 既に存在する ArchiveTimeStamp 要素
   - QualifyingProperties を含まず、ds:Reference で参照されていないような ds:Object 要素
4. 取り出したすべての要素について正規化を行い、その結果を連結してハッシュ計算の入力とする。

リスト 32 に ArchiveTimeStamp 要素の XMLScheme 定義を示す。同時に複数の TSA へタイムスタンプのリクエストを送信した場合、得られる複数のタイムスタンプトークンは、一つの ArchiveTimeStamp 要素内に格納しなければならない。また、アーカイブタイムスタンプ自身の検証情報（認証パス及び失効情報）はアーカイブタイムスタンプに含めるか、もしくは別途安全に保管しておく必要がある。

リスト 32：ArchiveTimeStamp 要素の XMLSchema 定義

```
<xsd:element name="ArchiveTimeStamp" type="XAdESTimeStampType"/>
```

2.3. XAdES 長期署名フォーマットにおける必須要素

本稿では、何種類かの形式の XAdES 署名を定義したが、表 3 では XAdES の各形式における必須要素、オプション要素の分類を示す。

表 3：XAdES の形式と要素の対応

	XAdES-BES	XAdES-EPES	XAdES-T	XAdES-A	
QualifyingProperties	○	○	○	○	
SignedProperties	○	○	○	○	
SignedSignatureProperties	○	○	○	○	
SigningTime	△	△	△	△	XAdES(V1.1.1)では必須
SigningCertificate	△1	△1	△1	△1	XAdES(V1.1.1)では必須
SignaturePolicyIdentifier	×	○	△2	△2	XAdES(V1.1.1)では必須
SignatureProductionPlace	△	△	△	△	
SignerRole	△	△	△	△	
SignedDataObjectProperties	△	△	△	△	
DataObjectFormat	△	△	△	△	
CommitmentTypeIndication	△	△	△	△	
AllDataObjectsTimeStamp	△	△	△	△	
IndividualDataObjectsTimeStamp	△	△	△	△	
UnSignedProperties	△	△	○	○	
UnSignedSignatureProperties	△	△	○	○	
CounterSignature	△	△	△	△※	
SignatureTimeStamp	×	×	○	○	
CompleteCertificateRefs	×	×	×	△※	
CompleteRevocationRefs	×	×	×	△※	
AttributeCertificateRefs	×	×	×	△3※	XAdES(V1.1.1)では未定義
AttributeRevocationRefs	×	×	×	△3※	XAdES(V1.1.1)では未定義

				SigAndRefsTimeStamp	×	×	×	△3※
				RefsOnlyTimeStamp	×	×	×	△3※
				CertificateValues	×	×	×	○
				RevocationValues	×	×	×	○
				ArchiveTimeStamp	×	×	×	○

○：必須要素

△：オプション要素(本属性が存在することを理由として、構築時や検証時にエラーとしてはならない。)

△１：ds:KeyInfo に署名者証明書が格納されていて、以下の条件を満たす場合はこの要素はなくても良い。

- ds:KeyInfo は、署名者証明書を含む ds:X509Data 要素を含まなければならない
- ds:KeyInfo は、信頼点までの証明書チェーンを構成する証明書も含む場合がある。
- ds:SignedInfo 要素の ds:Reference 要素で ds:KeyInfo を参照することにより、署名の計算対象として署名値の計算に含まれなければならない。

△２：XAdES-EPES を元に XAdES-T や XAdES-A を構成した場合、SignaturePolicyIdentifier 要素は必須となる。

△３：存在は任意だが推奨しない。

※：存在する場合は、ArchiveTimeStamp の計算の対象に加える必要がある

×：不要（あってはならない要素）

また、準拠する ETSI 101 903 “XML Advanced Electronic Signatures(XAdES)”のバージョンは、表 4 に示すいずれかを選択する。

表 4：準拠する ETSI 101 903 “XML Advanced Electronic Signatures(XAdES)”のバージョン

	ETSI TS 101 903 V1.1.1 (2002-02)	ETSI TS 101 903 V1.2.2(2004-4)	ETSI TS 101 903 V1.3.1(2005-05)
準拠するバージョン	△	△	△