

XAdES と CAdES (2種類の長期署名フォーマット)

XAdES – JIS X5093 – ETSI TS 101 903

XML署名 利用例: ODF, OOXML, XPS 等	ベース電子署名規格	CMS (PKCS#7) 形式 利用例: PDF, S/MIME 等
XML (テキスト)	ベースフォーマット	ASN.1/BER (バイナリ)

日本のPKI業界ではXMLは少数
 欧州ではCAdESよりも優勢
 テキスト形式で可読性が高い
署名対象はURIで指定
 XMLの正規化等による冗長性あり
一般的XMLパーサで解析可能
 証明書等はASN.1/BER形式の為
結局CMS等の知識も必要になる

CAdES – JIS X5092 – ETSI TS 101 733

PKI業界で昔から使われている
 日本ではXAdESよりも優勢
 ファイルサイズが小さい
 署名対象は内包か外包のみ
 署名対象はバイナリとして扱う
 ASN.1/BER対応のパーサが必要
 証明書等も全てASN.1/BER形式
 CMS等の知識だけ良い

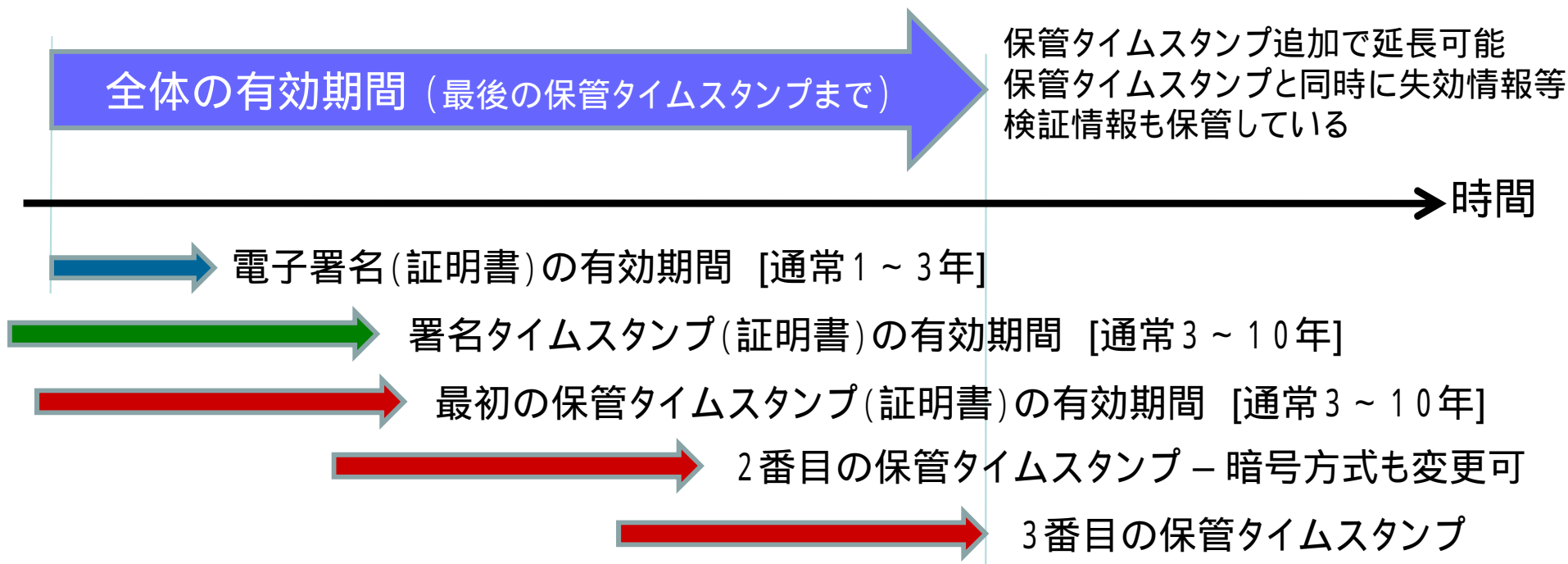
長期署名としての要素となる情報や電子署名 + タイムスタンプとしての仕様は両社共ほぼ同等。
 署名対象となる文書フォーマットやデータフォーマットで使い分けられているケースが多い。

電子署名と長期署名の仕組み

電子署名 「誰が」「何に」を保証

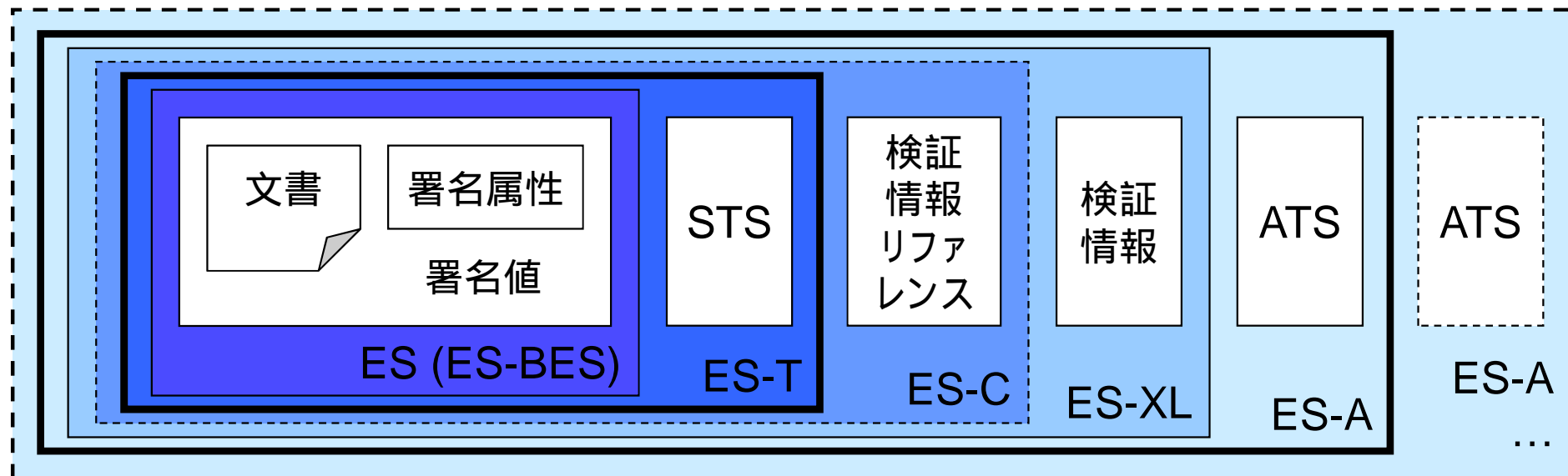
タイムスタンプ(署名タイムスタンプ) 「何時(いつ)」を保証

長期署名(保管タイムスタンプ) 「長期保管」を保証



XAdESの構造 (長期署名の階層構造)

- ES / ES-BES (XAdES) = 電子署名文書。
- **ES-T (XAdES-T)** = ESに署名タイムスタンプ(STS)を追加。 - **JIS定義**
- ES-C (XAdES-C) = ES-Tに検証情報リファレンスを追加。
- ES-X Long / ES-XL (XAdES-XL) = ES-T/ES-Cに検証情報を追加。
- **ES-A (XAdES-A)** = ES-XL に保管タイムスタンプ(ATS)を追加。 - **JIS定義**



保管タイムスタンプを追加して行く事で電子文書を長期間保証可能な構造。

XAdESの構造 2 (長期署名のXML構造)

```

<Signature>                                     // XML署名開始タグ
  <SignedInfo>                                   // 署名対象要素                               ES-BES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
      :
      <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)                               ES-BES要素
    <KeyInfo/>                                    // 署名者の秘密鍵情報 (オプション)             ES-BES要素
    <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 (必須: 署名対象の1つ)
          <SignedSignatureProperties/>             // XAdES署名要素 (例: <SigningTime>等)         ES-BES要素
        </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               ES-T要素
            <CertificateValues/>                 // XAdES-X-Long証明書一覧要素                   ES-XL要素
            <RevocationValues/>                  // XAdES-X-Long検証情報一覧要素                 ES-XL要素
            <ArchiveTimeStamp/>                  // XAdES-A保管タイムスタンプ要素 (複数回可能)   ES-A要素
          :
          <ArchiveTimeStamp/>                     // XAdES-A保管タイムスタンプ要素 (最終)         ES-A要素
        </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

```