JNSA 電子署名WG　スキルアップTF

なんとなく分かった気になるPDF電子署名仕様入門2

LangEdge,Inc.
有限会社 ラング・エッジ

宮地直人（miyachi@langedge.jp）

2013年10月30日

PDF電子署名仕様入門

○ PDF基本

PDFの内部構造と基本要素

増分更新

○ PDF電子署名基本

PDFの署名要素

○ PAdES（PDF長期署名）基本

PAdESの構造

LTV構造の構成

PDF基本1：PDFをテキストエディタで見てみよう

```
%PDF-1.3
%%%%%
6 0 obj
76
endobj
4 0 obj
<</Length 6 0 R>>
stream
0 0 0 rg
BT
/F0 11.00 Tf
85.0 730.0 Td
[ (ABC) ] TJ
ET
q Q
endstream
endobj
3 0 obj
<</BleedBox[0 0 595.320010 841.919980]
/Contents[4 0 R]
/CropBox[0 0 595.320010 841.919980]
/MediaBox[0 0 595.320010 841.919980]
/Parent 2 0 R
/Resources<</Font<</F0 5 0 R>>
/ProcSet[/Text/ImageC]>>
/Type/Page>>
endobj
2 0 obj
<</Count 1
/Kids[3 0 R]
/Parent 1 0 R
/Type/Pages>>
endobj
1 0 obj
<</BleedBox[0 0 595.320010
841.919980]
/Count 1
/CropBox[0 0 595.320010 841.919980]
/Kids[2 0 R]
/MediaBox[0 0 595.320010 841.919980]
/Type/Pages>>
endobj
7 0 obj
<</Ascent 985
/AvgWidth 464
/CapHeight 985
/Descent -215
/Flags 42
/FontBBox[-165 -307 1246 1201]
/FontName/Century
/ItalicAngle 0
/MaxWidth 1410
/StemV 0
/Type/FontDescriptor>>
endobj
5 0 obj
<</BaseFont/Century
/Encoding/WinAnsiEncoding
/FirstChar 32
/FontDescriptor 7 0 R
/LastChar 67
/Name/F0
/Subtype/TrueType
/Type/Font
/Widths[278 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 722 722
722]>>
endobj
9 0 obj
[3 0 R/XYZ 0 841.919980 null]
endobj
8 0 obj
<</OpenAction 9 0 R
/Pages 1 0 R
/Type/Catalog>>
endobj
10 0 obj
<</CreationDate(D:20110610150233+09'00')
/ModDate(D:20110610150233+09'00')
/Producer(Test ¥(1.0¥))
/Trapped/False>>
endobj
xref
0 11
0000000000 65535 f
0000000444 00000 n
0000000380 00000 n
0000000160 00000 n
0000000034 00000 n
0000000785 00000 n
0000000016 00000 n
0000000602 00000 n
0000001061 00000 n
0000001016 00000 n
0000001123 00000 n
trailer
<</ID[
<BF61BD682C7E7D44F2DF1EAB84335E2B>
<BF61BD682C7E7D44F2DF1EAB84335E2B>]
/Info 10 0 R
/Root 8 0 R
/Size 11>>
startxref
1283
%%EOF
```

PDF基本2：主なオブジェクト例

1．数値オブジェクト

```
6 0 obj   ← オブジェクト開始（オブジェクト番号が6 、生成番号が0）
76        ← 整数型で値が76
endobj    ← オブジェクト終了
```

2．辞書オブジェクト（キーと値で情報を記述するオブジェクト）

```
2 0 obj
<<                    ← 辞書型開始
/Type /Pages          ← キーが”/Type”の名前型で、値が”/Pages”
/Kids [ 3 0 R]        ← キーが”/Kids”の配列型で、配列中の値が間接指定型で”3 0 R”
/Count 1              ← キーが”/Count”の整数型で、値が1
/Parent 1 0 R         ← キーが”Parent”の間接指定型で、値が”1 0 R”
>>                    ← 辞書型終了
endobj
```

ポイント：オブジェクト番号と生成番号

オブジェクト番号は重複しないオブジェクト識別用IDです。

生成番号は本来オブジェクトを再利用した時に更新される番号ですが現在では事実上利用されておらず常にゼロ0と考えて貰って構いません。

PDF基本3：主なオブジェクト例2

3. ストリームオブジェクト（任意データを埋め込むオブジェクト）

```
4 0 obj
<</Length 6 0 R>>          ← 長さはオブジェクト番号6で定義
stream                     ← ストリーム開始
0 0 0 rg
BT                         ← テキスト開始
/F0 11.00 Tf               ← フォント名/F0とサイズ11.00の指定
85.0 730.0 Td              ← 座標 85.0, 730.0 に移動
[ (ABC) ] TJ               ← テキスト"ABC"の描画
ET                         ← テキスト終了
q Q
endstream                  ← ストリーム終了
endobj
```

描画用オペレータ

※ フィルター指定ストリームオブジェクト

```
4 0 obj
<</Length 6 0 R            ← 長さはオブジェクト番号6で定義
/Filter /FlateDecode>>     ← FlateDecodeによりZIP圧縮を実行
Stream
※ バイナリ値（ZIP圧縮されたデータ）
endstream
endobj
```

PDF基本4:オブジェクトの種類

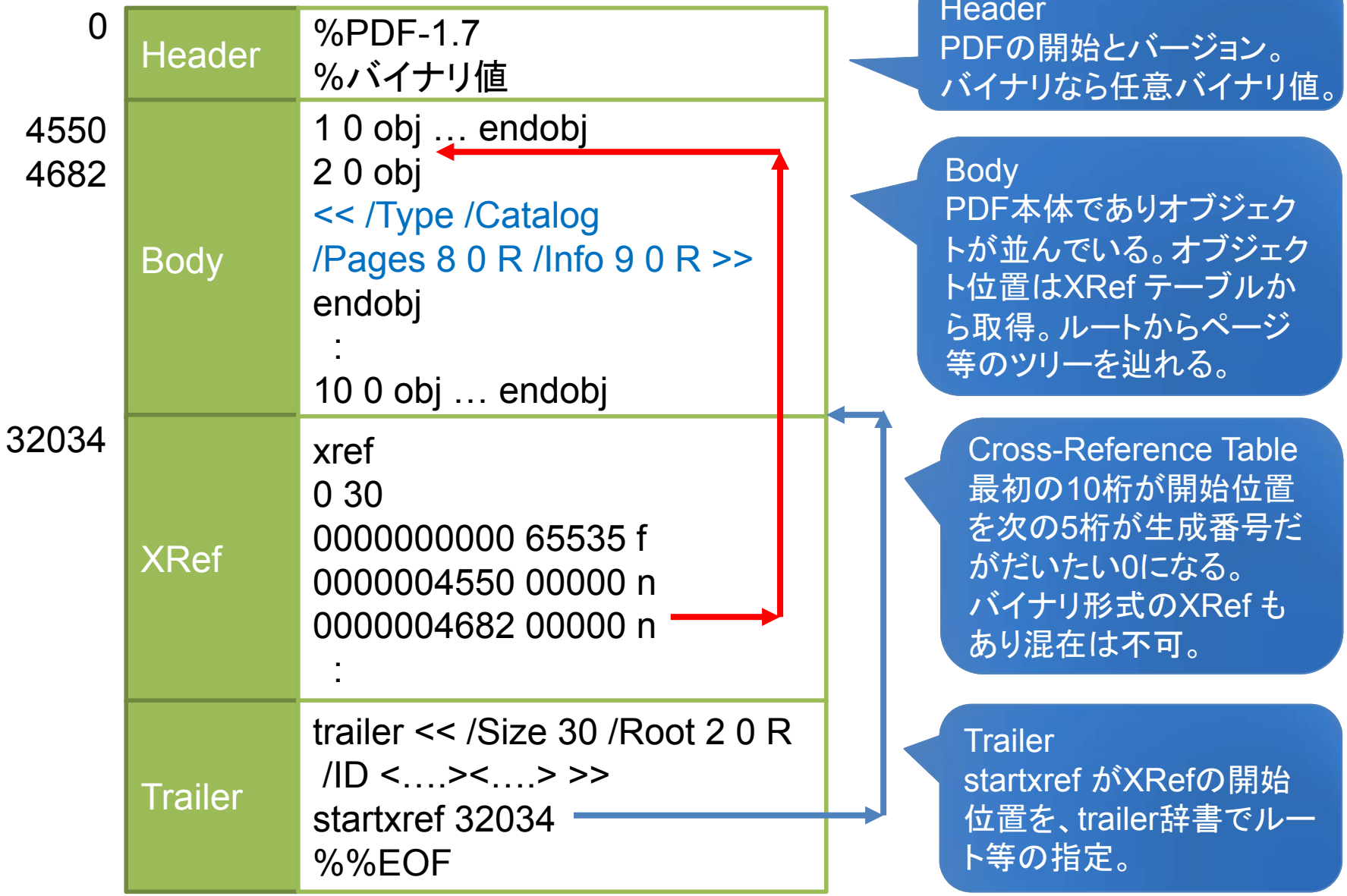
➢ オブジェクト形式

- オブジェクト番号と生成番号とobj/endobj: 1 0 obj value endobj

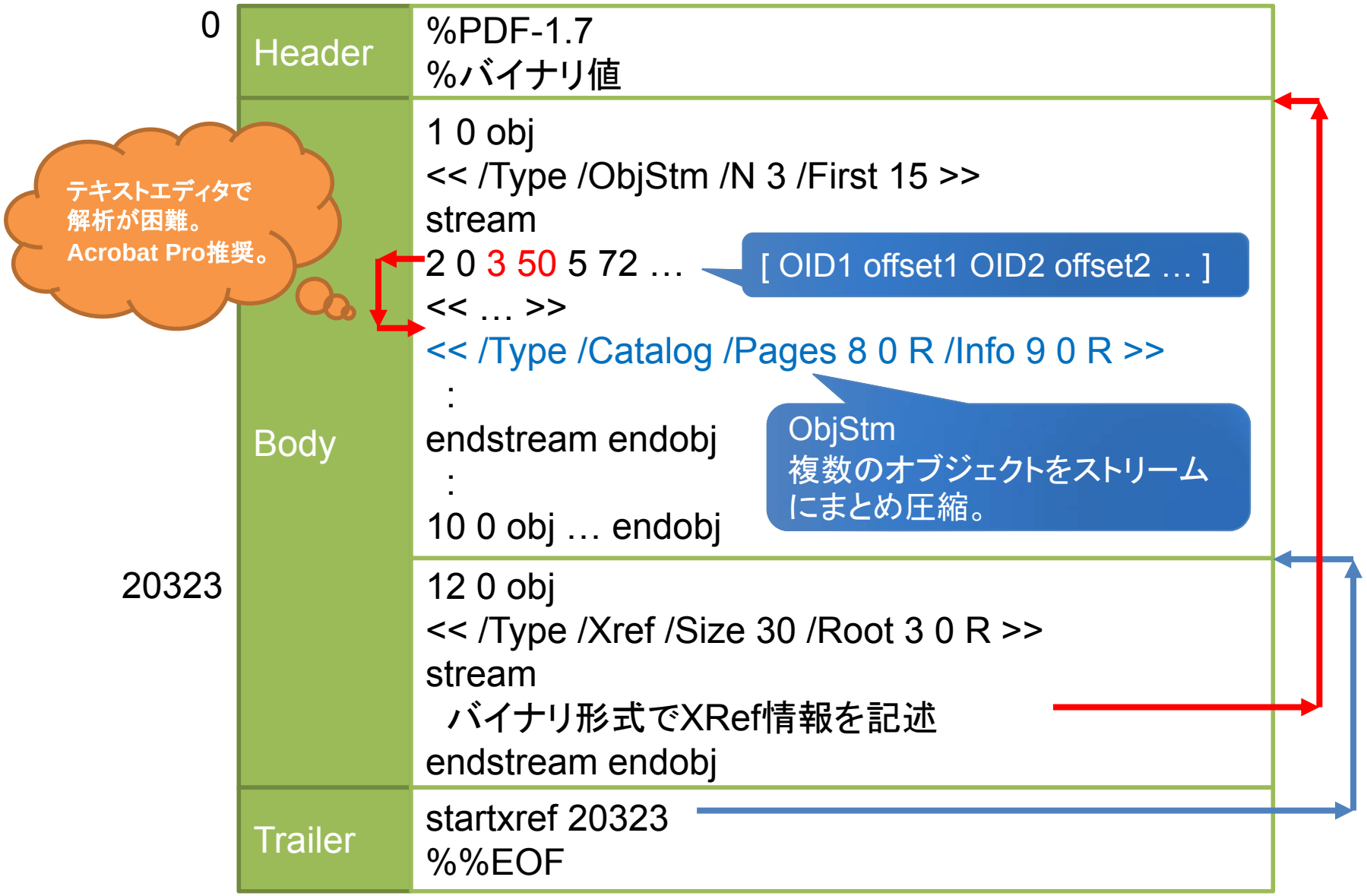
➢ オブジェクト(Objects / Value)

- ブーリアン(Boolean values): true, false
- 数値(Integer and Real numbers): 10, -3, 3.4, -0.32, +10.0
- 文字列(Strings) ※暗号化対象
  - 定数文字列(Literal Strings): (Ver ¥(1.0¥)) ※エスケープ文字"¥"あり
  - 16進文字列(Hexadecimal Strings): <4E6A> ※バイナリにも使われる
- 名前(Names): /Name, /Color#20Green, /A#42
- 配列(Arrays): [value1 value2 value3]
- 辞書(Dictionaries): << /Key1 value1 /Key2 value2 /Key3 value3 >>
- ストリーム(Streams): <<Dictionary>>stream … endstream ※暗号化対象
  - /Filter: /FlateDecode (ZIP), /DCTDecode (JPEG), /ASCIIHexDecode, …
- null
- 間接指定(Indirect): 23 0 R (23 0 obj を示す)

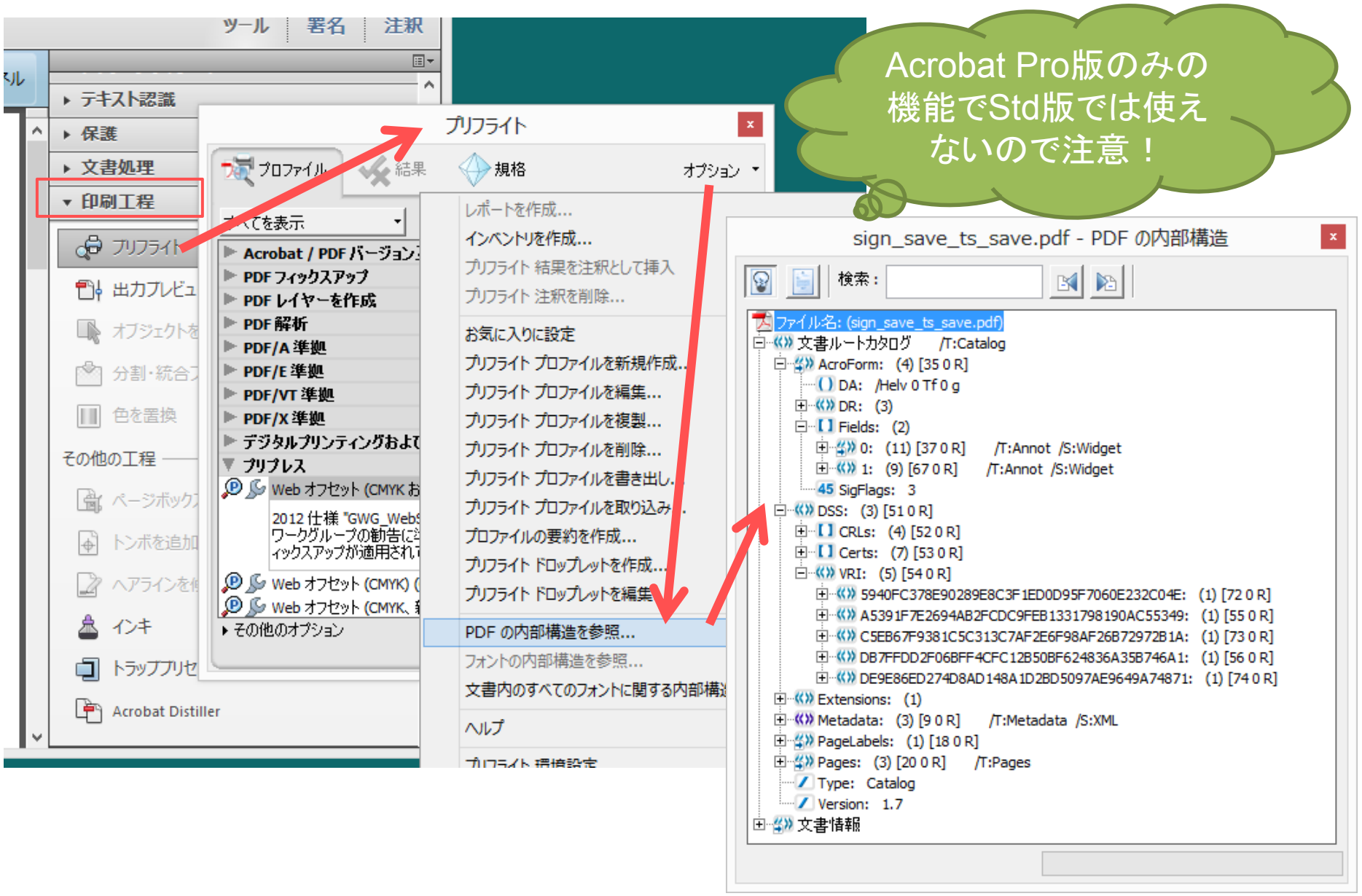
PDF基本5：PDFファイル構造1（レガシー）形式



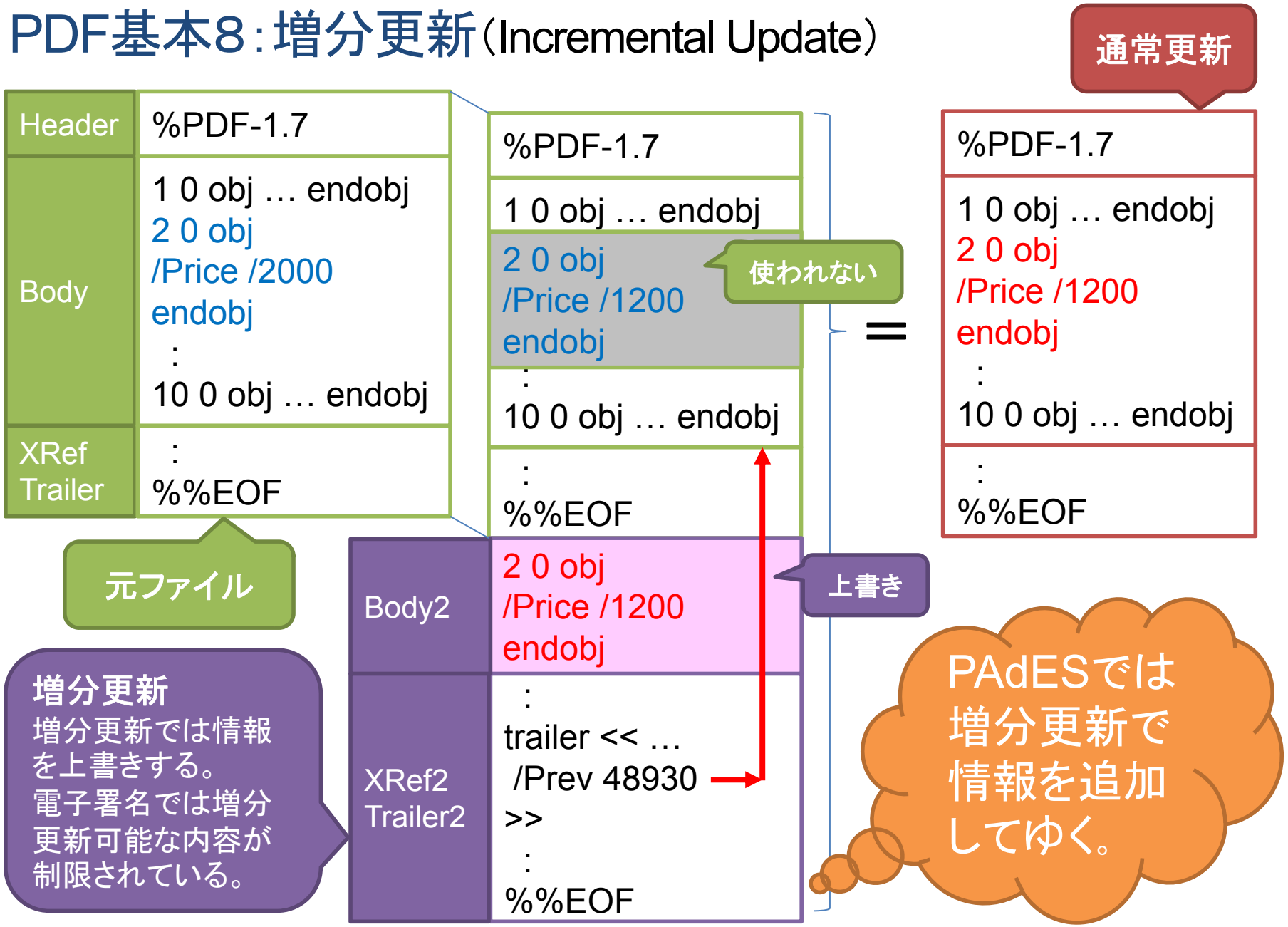
PDF基本6：PDFファイル構造2（Cross-Reference Streams & object stream）



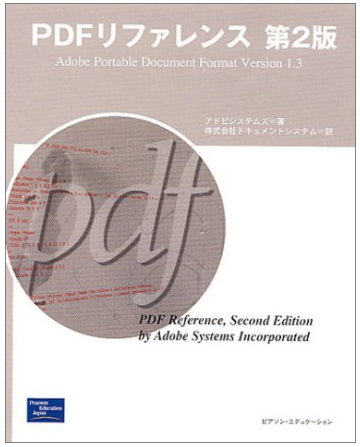
PDF基本7：Acrobat ProでPDF内部構造を見る

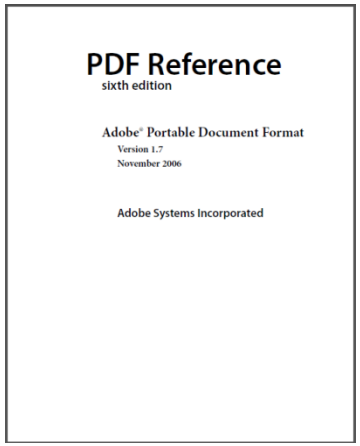


PDF基本8：増分更新（Incremental Update）



PDF基本9：PDFに関する資料





・PDF Reference 2nd edition（PDF1.3）を和訳化した書籍
古い版だが基本的な構造を日本語で読める。
PDFファイル構造はレガシー形式のみ
とりあえずPDFを勉強するなら持っていて損は無い。
定価は税別6800円だが中古市場では7,000～14,000円くらい。
定価で売っているお店があれば確保推奨。
ISBN-10: 4894713381 / ISBN-13: 978-4894713383

・PDF Reference の原本はアドビが無償配布
最終はPDF1.7だがISOとの比較資料等もあります。
他にもアドビから署名外観等の有用情報が多数あり。
ISO版は有償なのでPAdES以外ならアドビ版で十分。
http://www.adobe.com/jp/devnet/pdf/pdf_reference.html

・最後にISO32000
ISO32000-1はISOから購入が可能、ISO32000-2が待たれる。
238スイスフラン（約26,000円）
http://www.iso.org/iso/catalogue_detail.htm?csnumber=51502

PDF署名基本1:オブジェクト要素

➢ 署名フィールド/署名注釈(SigField/SigAnnotation)

- 本来署名フィールドと署名注釈は別の辞書構造だが1つの辞書として指定可能。最近では別々にするような実装は少ないが注意。
- ページ番号と矩形を指定。矩形がサイズゼロなら不可視署名になる。
- Root→AcroForm→Fields or Root→Pages→Page→Annots で辿れる。
- 署名辞書を /V キーで指定。未指定なら未署名の署名フィールドとなる。
- 署名外観を /AP キーで指定。不可視署名ならブランクを指定。

➢ 署名辞書(SigDict) ※電子署名として最も重要な要素

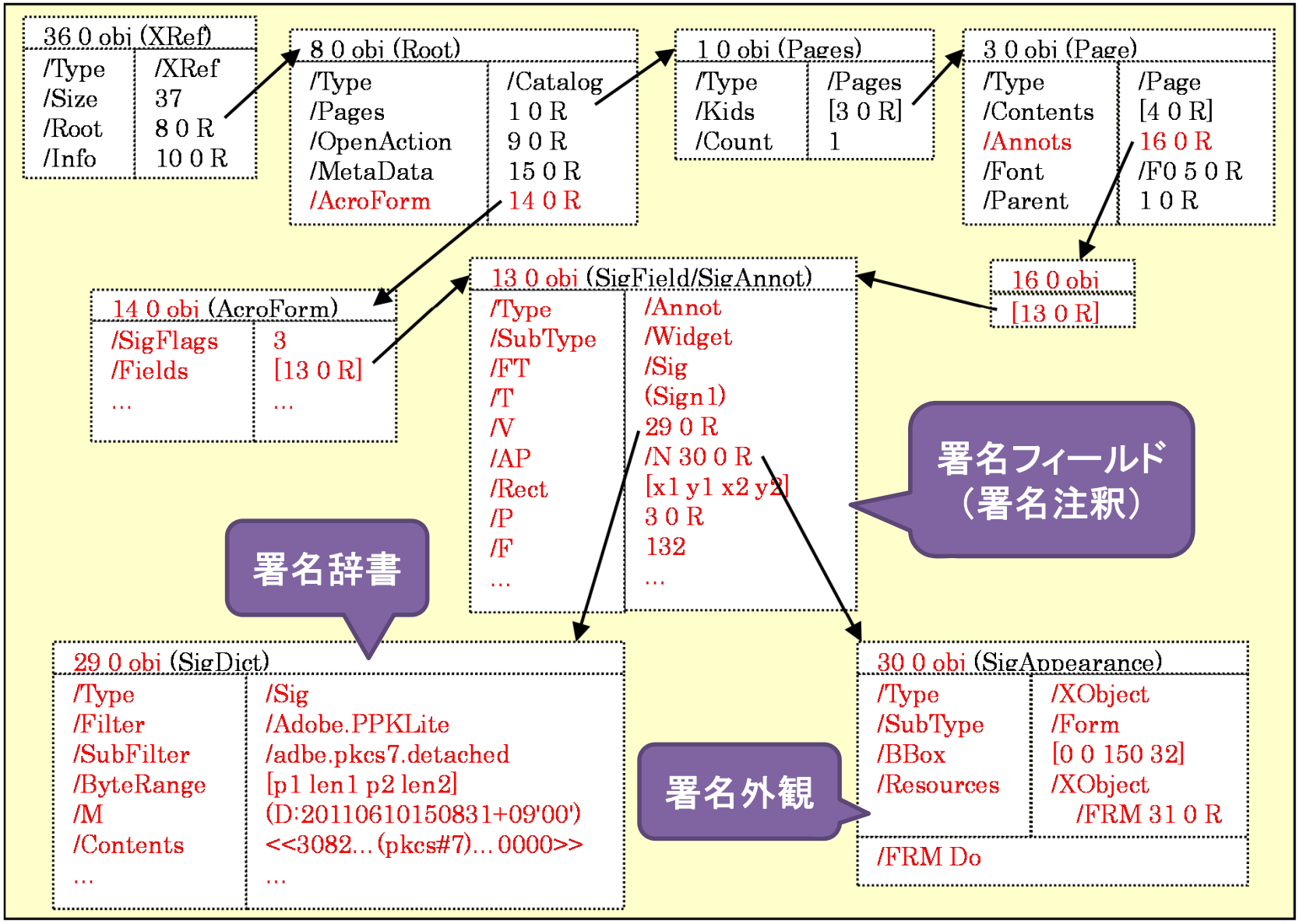
- /Type は /Sig か /DocTimeStamp を指定。
- 署名データを /Contents キーで16進文字列として保持。
- /ByteRange や /Filter /SubFilter 等の情報を保持。

暗号化対象のはず(仕様に記述無し)だが実際には、暗号化しては駄目

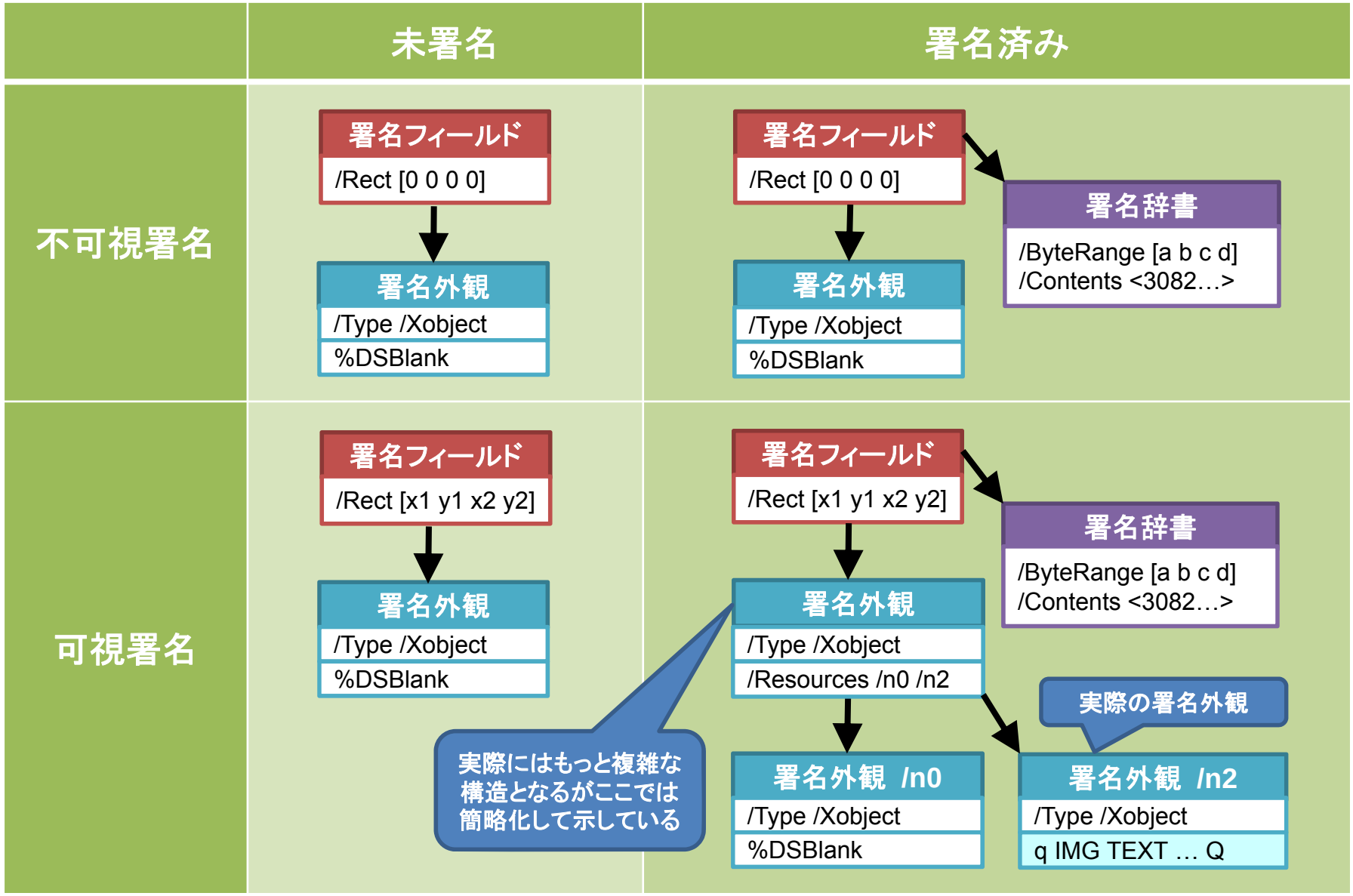
➢ 署名外観(SigAppearance)

- XObject のリソースとして外観情報を指定。実は ISO 等の標準ではない。
- デファクトは「Adobe Acrobat 9 Digital Signature Appearances」である。
  http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/acrobat_digital_signature_appearances_v9.pdf

PDF署名基本2：内部構造例



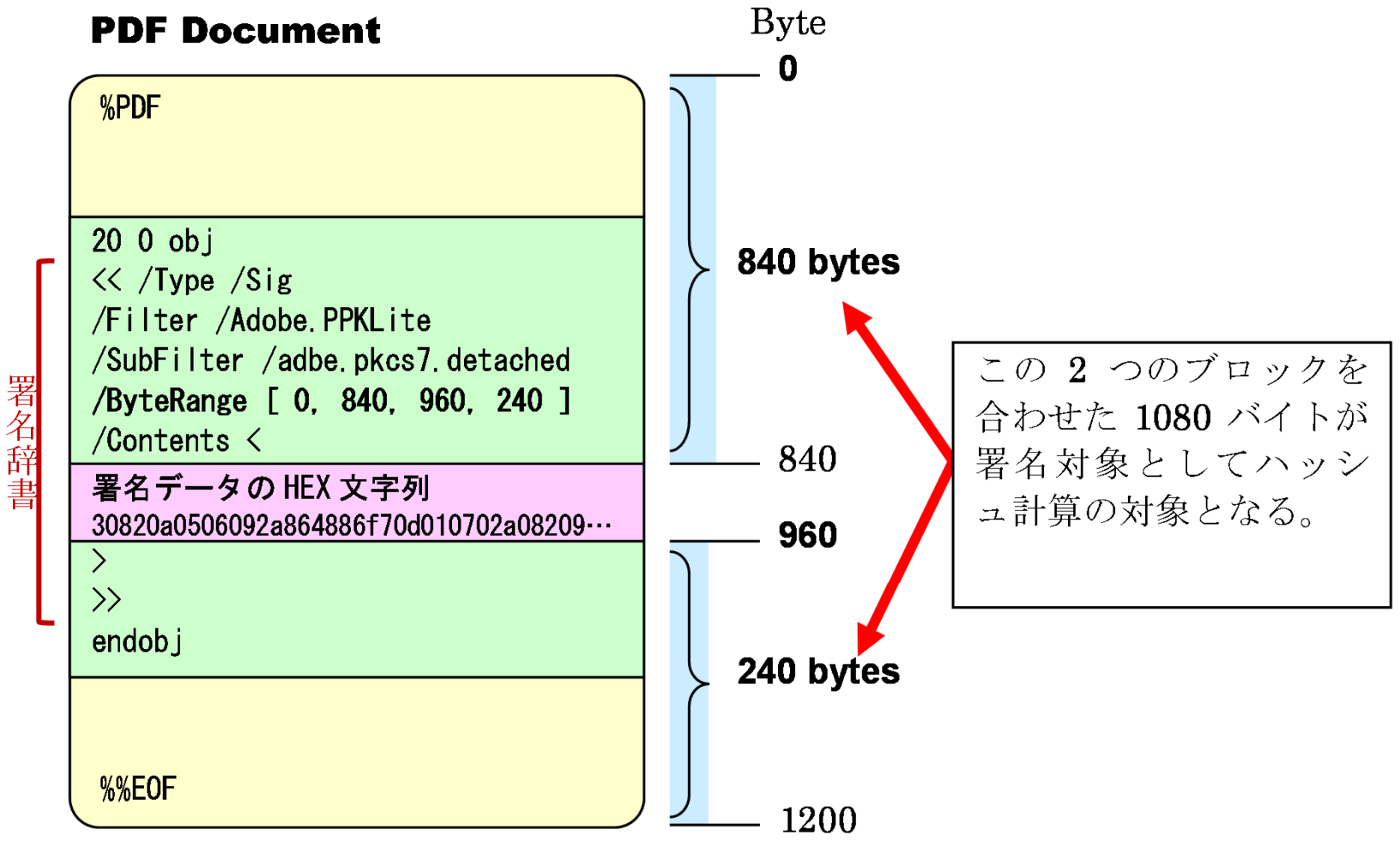
PDF署名基本3:オブジェクトの組み合わせ



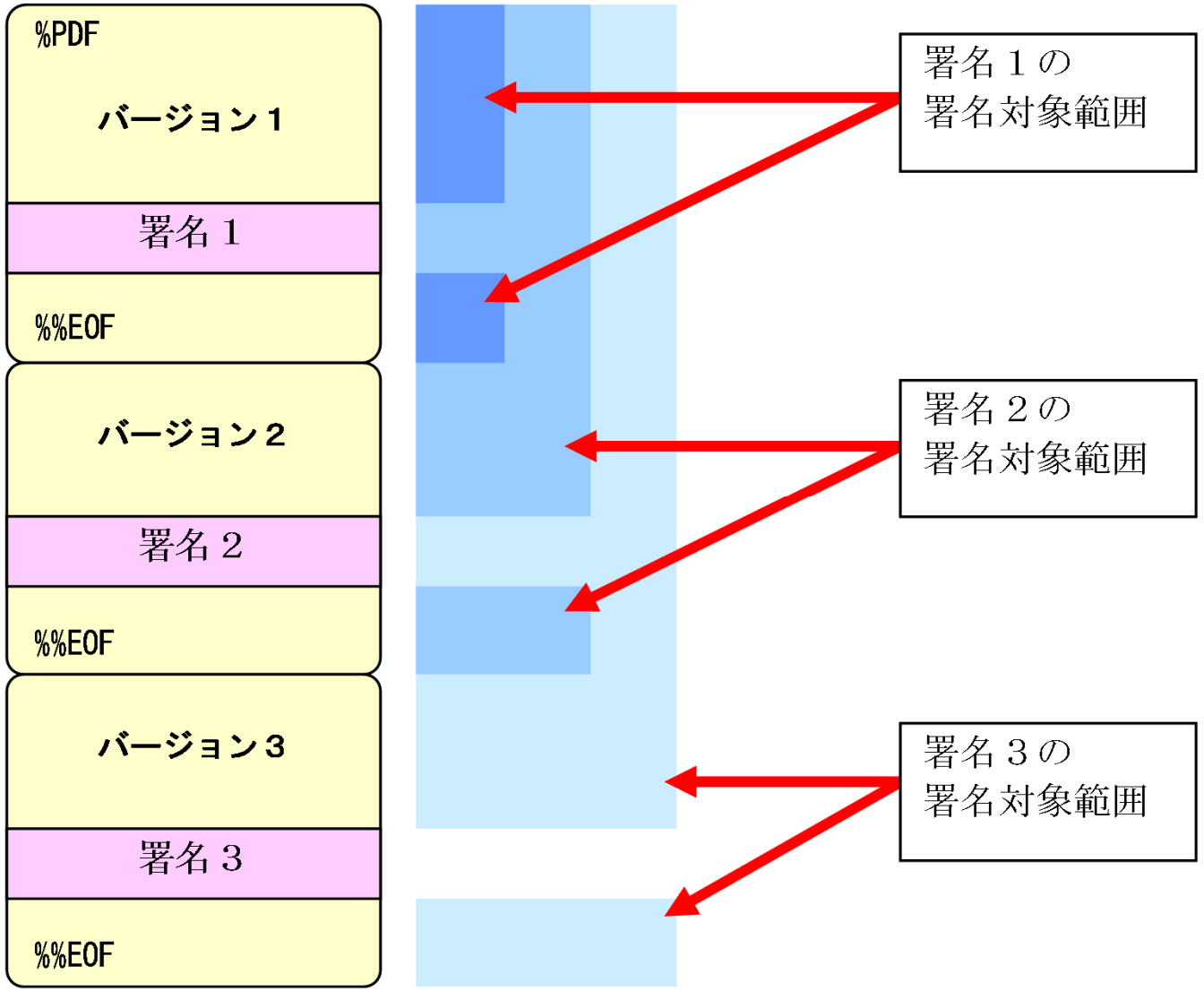
PDF署名基本4：ByteRangeと署名対象

署名辞書 ： /ByteRange [開始位置1 長さ1 開始位置2 長さ2]

配列



PDF署名基本5:シリアル署名(複数署名)



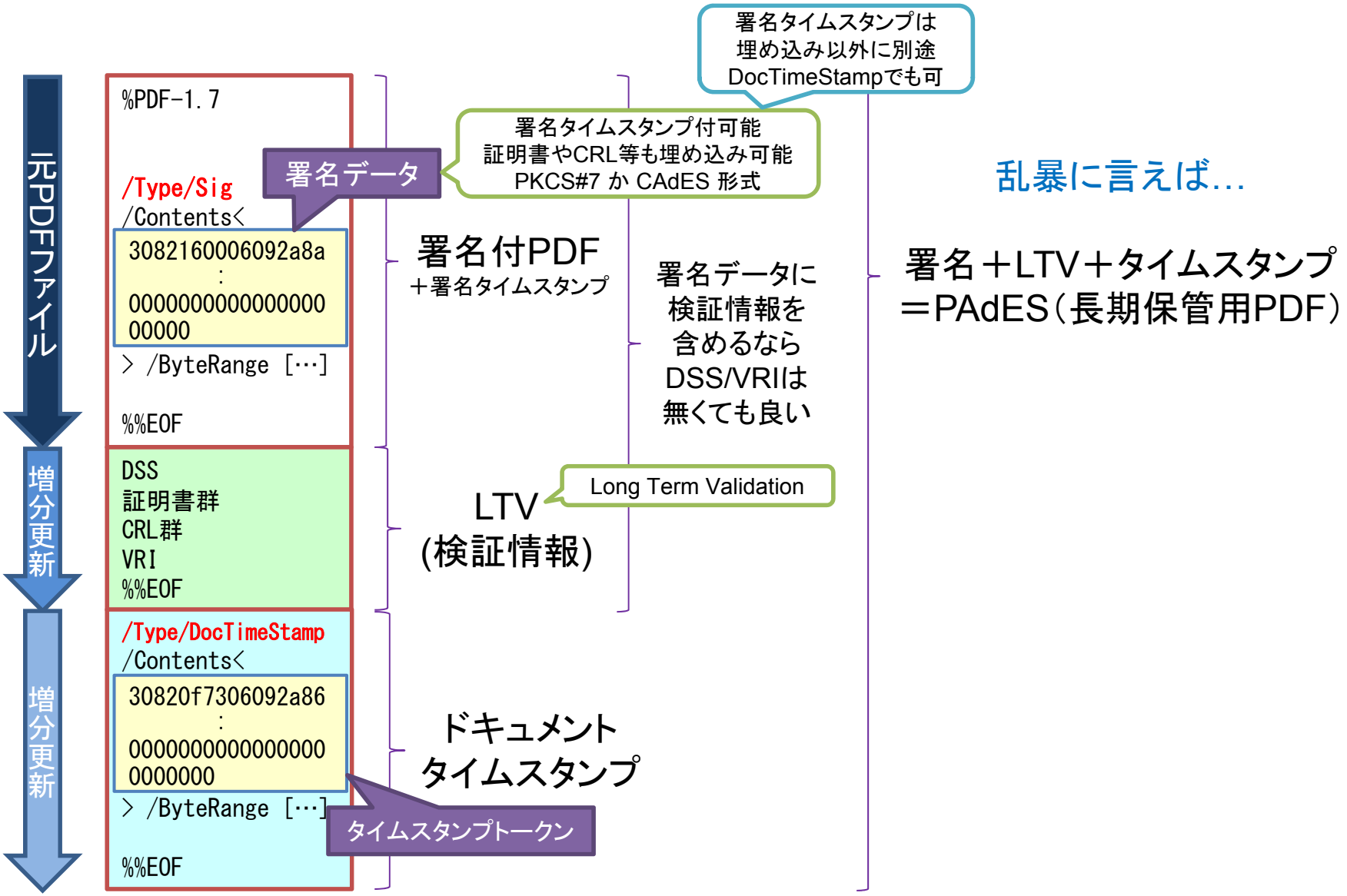
PAdES基本1：PAdESの構成

Part	Title	About
Part1:	PAdES Overview	PAdES全体の概要を解説している。最初に読むべき解説。
Part2:	PAdES Basic	既存のPDF仕様（ISO 32000-1/PDF1.7）に基づく署名プロファイル。署名プロファイルとしてPKCS#7(CMS)を利用。
Part3:	PAdES Enhanced	署名プロファイルとしてCAdES-BES/CAdES-EPES/CAdES-Tを使った署名プロファイル。
Part4:	PAdES Long Term (LTV)	PAdES-LTV（Long Term Validation）Profile 長期署名の為に新たに加えられたDSS/VRI辞書を使って検証情報とドキュメントタイムスタンプをPDFに埋め込む。
Part5:	PAdES for XML Content	PDFに添付されたXMLドキュメントや、XFA（XML Forms Architecture）として埋め込まれたXMLフォームに対して、XAdESを使った長期署名プロファイル
Part6:	Visual Representations of Electronic Signatures	署名外観や検証に関する仕様 ただし簡易説明であり詳細は別仕様を参照

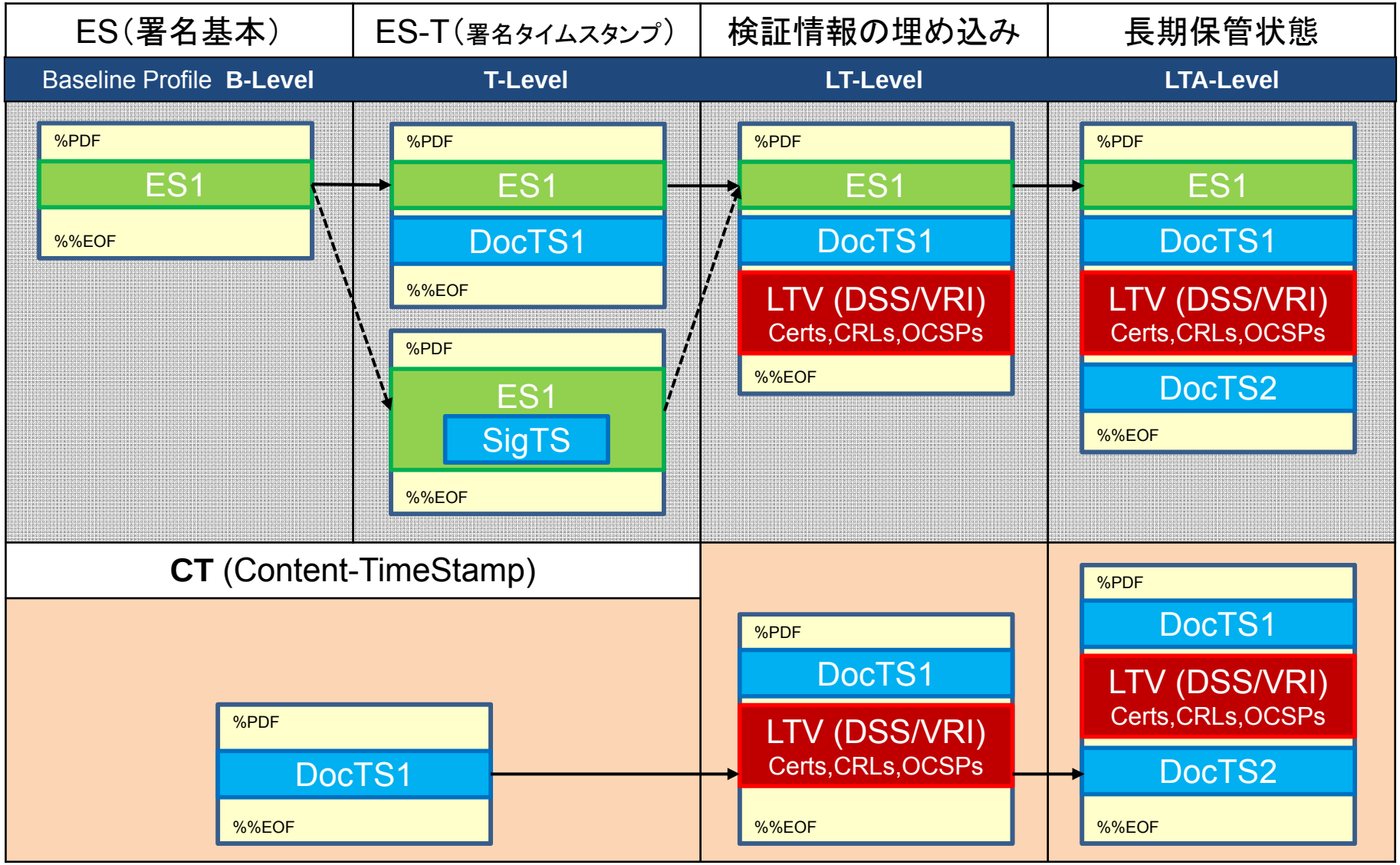
※ 署名辞書の違い

形式	/Type	/SubFiler	署名部 /Contents	その他
PAdES-Basic	/Sig	/adbe.pkcs7.detached /adbe.pkcs7.sha1	PKCS7 (+TST)	ISO32000-1の署名ほぼそのまま
PAdES-Enhanced	/Sig	/ETSI.CAdES.detached	CAdES	CAdES-T/BES/EPES
DocTimeStamp (PAdES-LTV)	/DocTimeStamp	/ETSI.RFC3161	TST	Name, M, Location, Reason等は非推奨

PAdES基本2：PAdESの構成



PAdES基本3：PAdESのレベル遷移

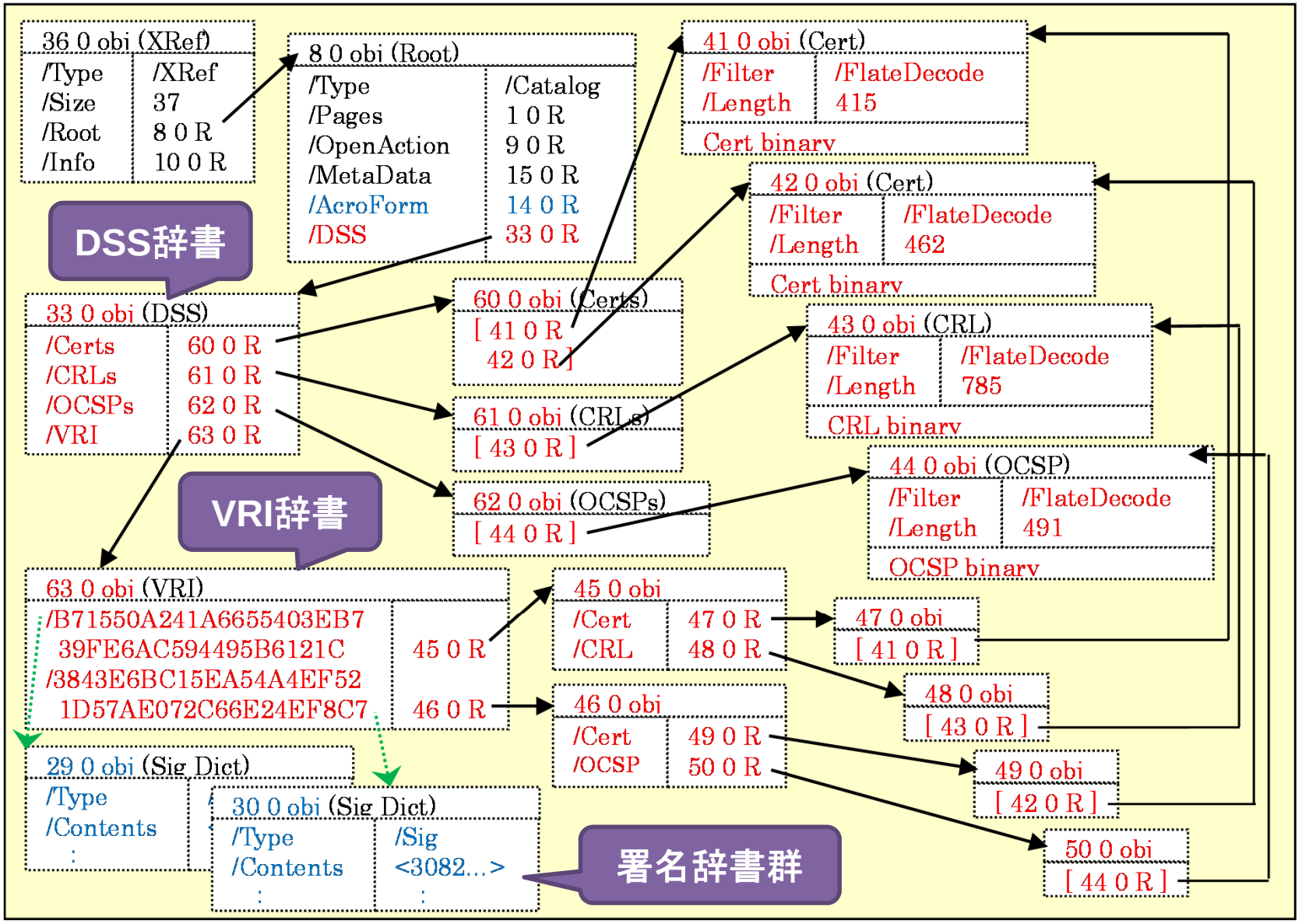


PAdES基本4：検証情報

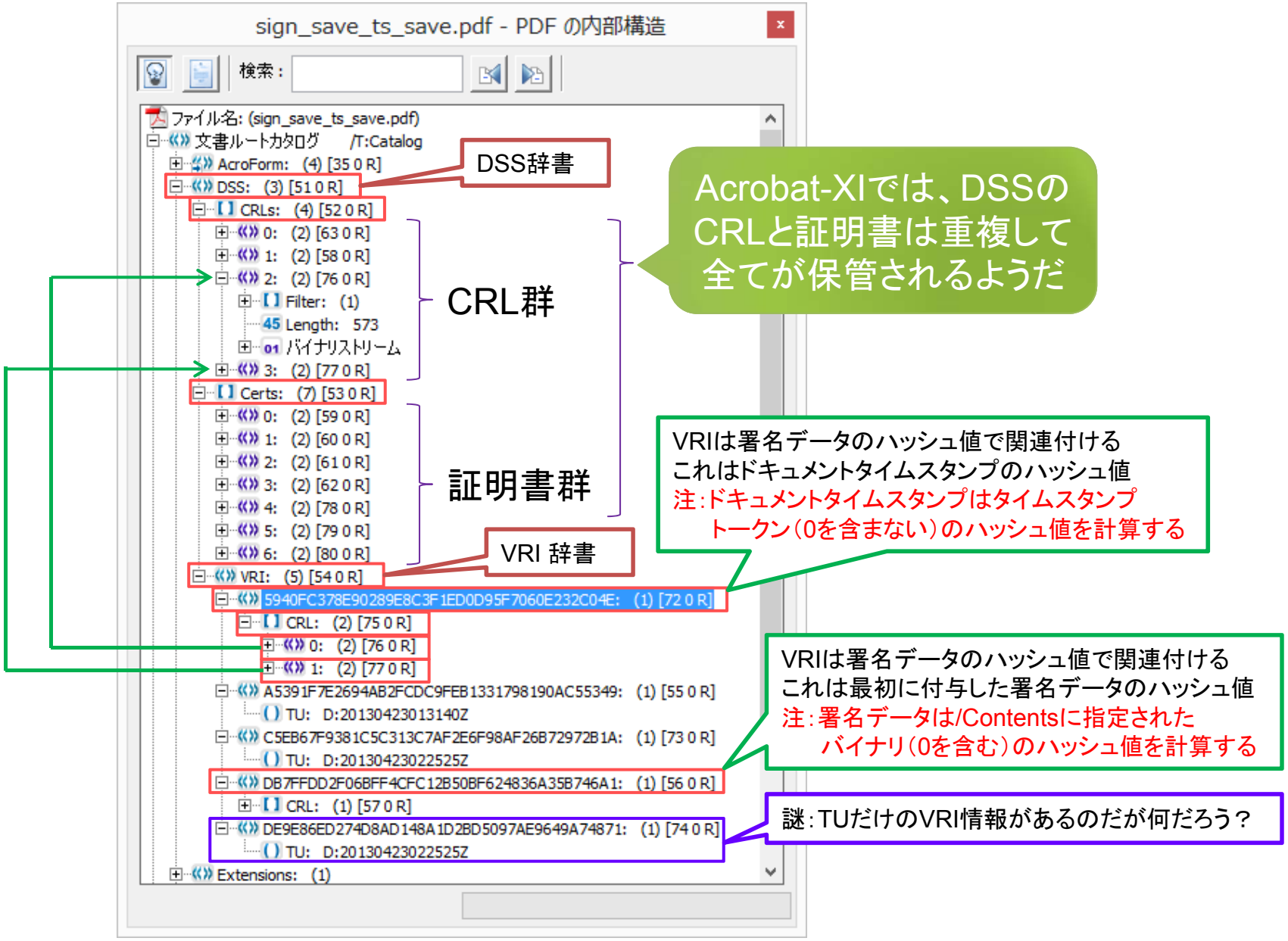
検証情報の種類	説明
署名書群	署名証明書（タイムスタンプ証明書を含む）から信頼されたルート証明書（トラストアンカー）までの証明書チェーン（認証パス）を構築する為に必要な全証明書が必要。
失効情報群	失効情報には、CRL（証明書失効リスト）とOCSP（オンライン失効情報問合せ）の2種類がある。CRLは失効している証明書の情報であり、OCSPは指定された証明書の失効を含む各種状態を返す。失効情報としてCRLとOCSPのどちらを使っても良い。

優先順位	検証情報の格納場所
1	DSS の中の署名VRI 要素から参照されている検証情報
2	DSS から参照されている検証情報
3	署名データ自身に埋め込まれている検証情報
4	ローカルなリポジトリに保管されている検証情報（外部から提供）
5	オンラインソースから取得された検証情報（ネットワークから取得）

PAdES基本5：PAdES-LTVの内部構造例



PAdES基本6：PAdES-LTVの内部構造例2



PAdES基本7：PAdES（PDF長期署名）に関する資料

1. ETSI仕様書

   以下ダウンロードサイトから”TS 102 778”で検索してダウンロード

   http://pda.etsi.org/pda/queryform.asp

2. ECOM 電子署名普及に関する活動報告2009

   3.1 PAdESの概要、経緯、動向

   http://www.jipdec.or.jp/archives/ecom/results/h21seika/H21results-09.pdf

3. PDFインフラストラクチャー解説（現在更新中）

   22.7 PDF長期署名（PAdES） 他にもPDF署名等の説明もあり

   http://www.cas-ub.com/project/index.html#Free

4. Acrobat-XIでPAdESファイルを作成する

   http://www.langedge.jp/download/20130424-PAdES-doc.pdf