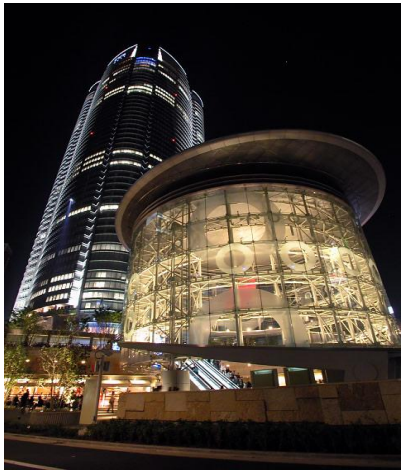
SWF研究会#2 発表#1

SWF の情報要素とバイナリの読み方

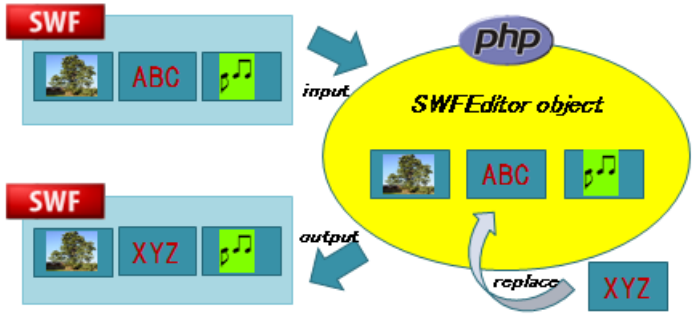
2012年9月25日(火) “よや“ <yoya@awm.jp>

自己紹介



- 六本木の方から来ました
  - 会社は着ているTシャツでお察し下さい
  - アウェイで発表頑張ります！
- SWF バイナリ編集が趣味 (主に Flash Lite)
  - PHP の SWFバイナリ編集ライブラリを作ってます

(動的生成が下火でそろそろ過去形 ;ω;)



- http://sourceforge.jp/projects/swfed/
- http://openpear.org/package/IO_SWF

伝えたい事

- SWF フォーマットの読み方
  - SWF に含まれる情報要素とその意味
  - それらを SWF バイナリからどう切り出すか

- SWF バイナリの切り出しのコツ
  - 幾つかのパターンが分かれば簡単

Little Endian (Byte) , MSB (Bit) , “tag_and_length”
Byte Alignment , 8 bit Flags
Length Dependency Optional Field , ¥0 Terminate
Offset to foobaa , Offset Table.

SWF を触る目的

- ガラケー時代 ＞ Flash Lite の制限に力づくで対応
  - 最大100KB ⇒ 最小限のデータを SWF に載せる
  - 実行引数渡せない ⇒ SWF にパラメータ値を埋め込もう
  - 画像を動的に入れ替えし辛い ⇒ SWF の画像も入れ替えちゃえ

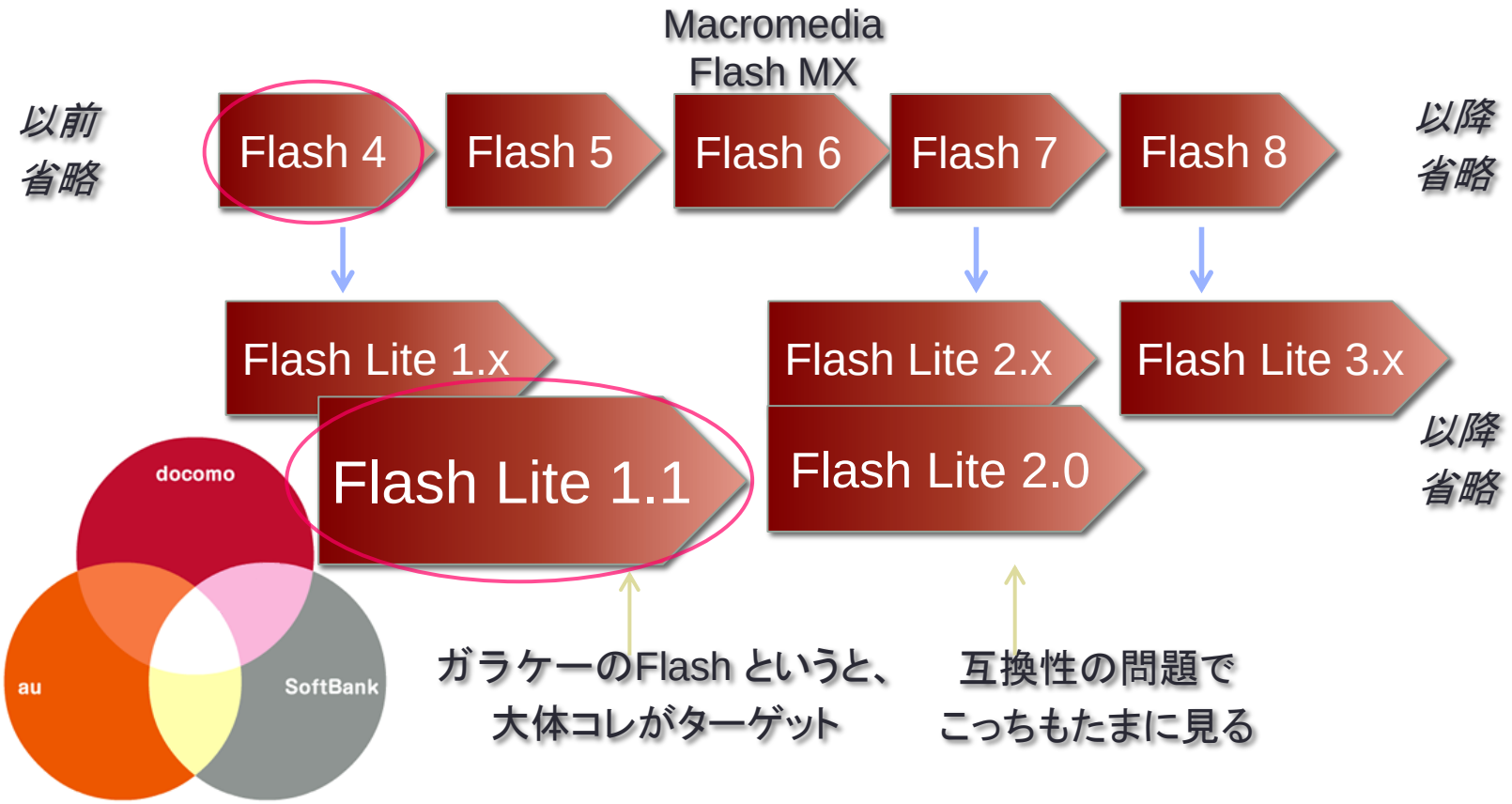
＼まさかの実行ファイル(SWF)動的生成／

- スマートフォン時代 ＞ Flash Player 代わりの処理
  - iOS に Flash Player が無い ⇒ JavaScript で SWF を解釈して何か表示
  - Android も 4.1 から Flash Player が無い ⇒ じゃぁ、こっちも！

＼まさかの Flash Player 実装／

Flash Lite と SWF version

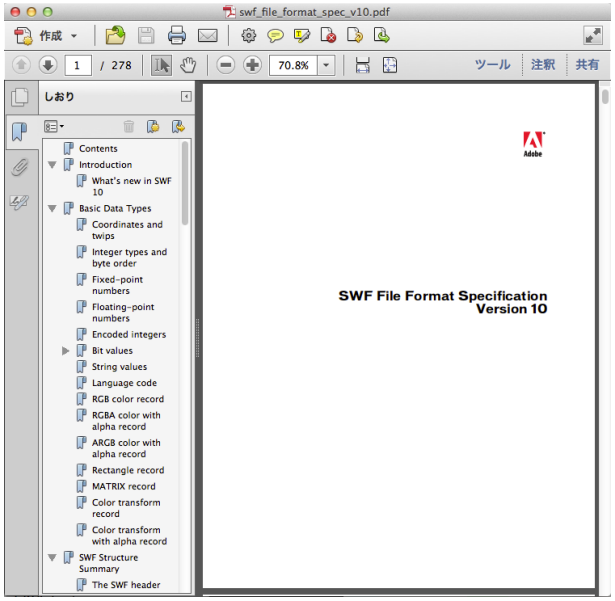
- Flash と Flash Lite の SWF version



引用元) http://www.adobe.com/jp/devnet/devices/articles/develop_in_japan.html

SWFの仕様

- 公式仕様書
  - http://www.adobe.com/devnet/swf.html

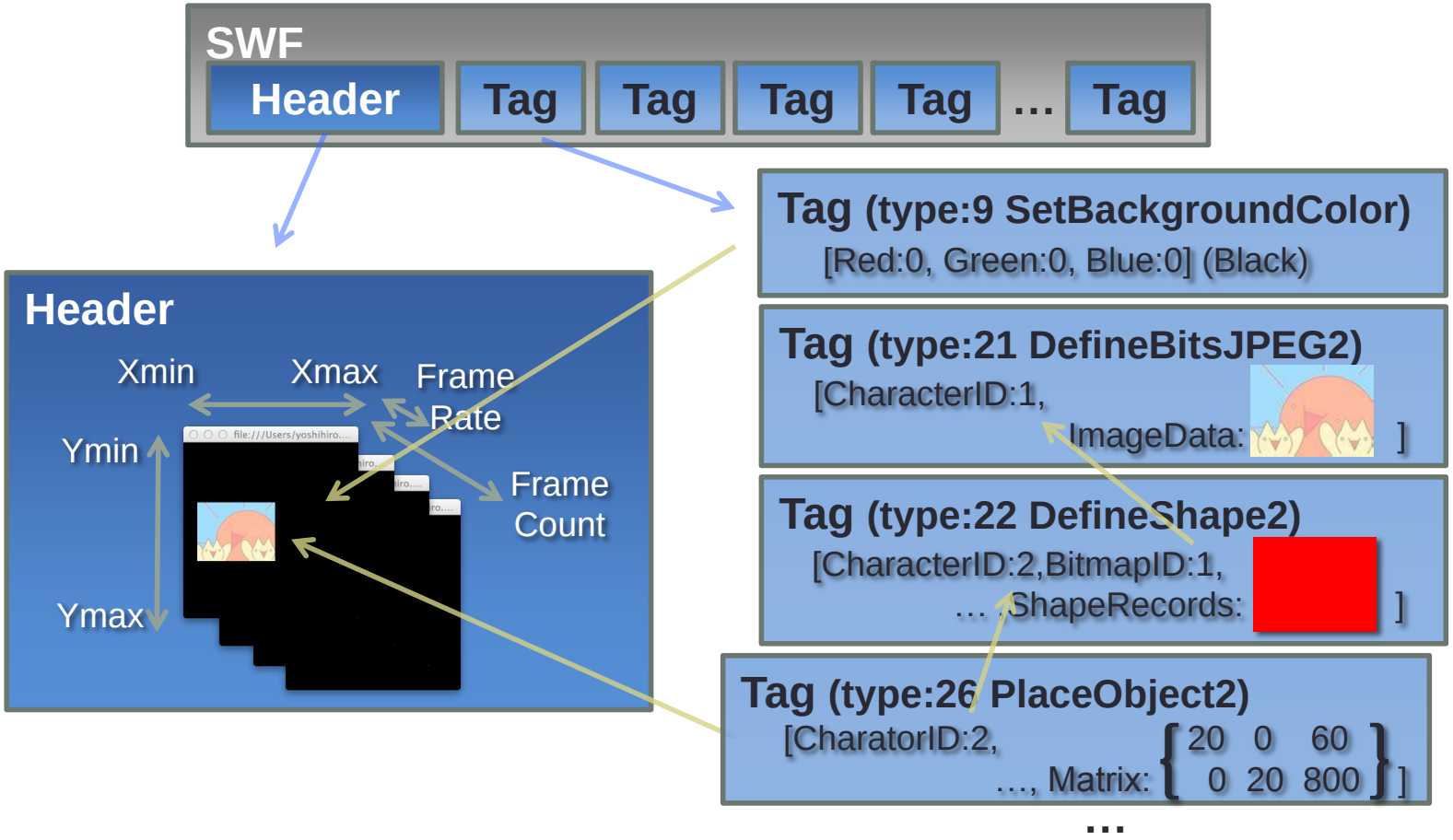


- データ形式は(正確さはさておき)
  詳細に書かれているが、
  意味の記述が全然足りない

- 自力で調べる必要あり
  - Flash Player のブラックボックス解析
  - 2000年初頭の書籍を漁る (だって Flash 4 だし…)
    お勧め → オーム社の Macromedia Flash ActionScript バイブル

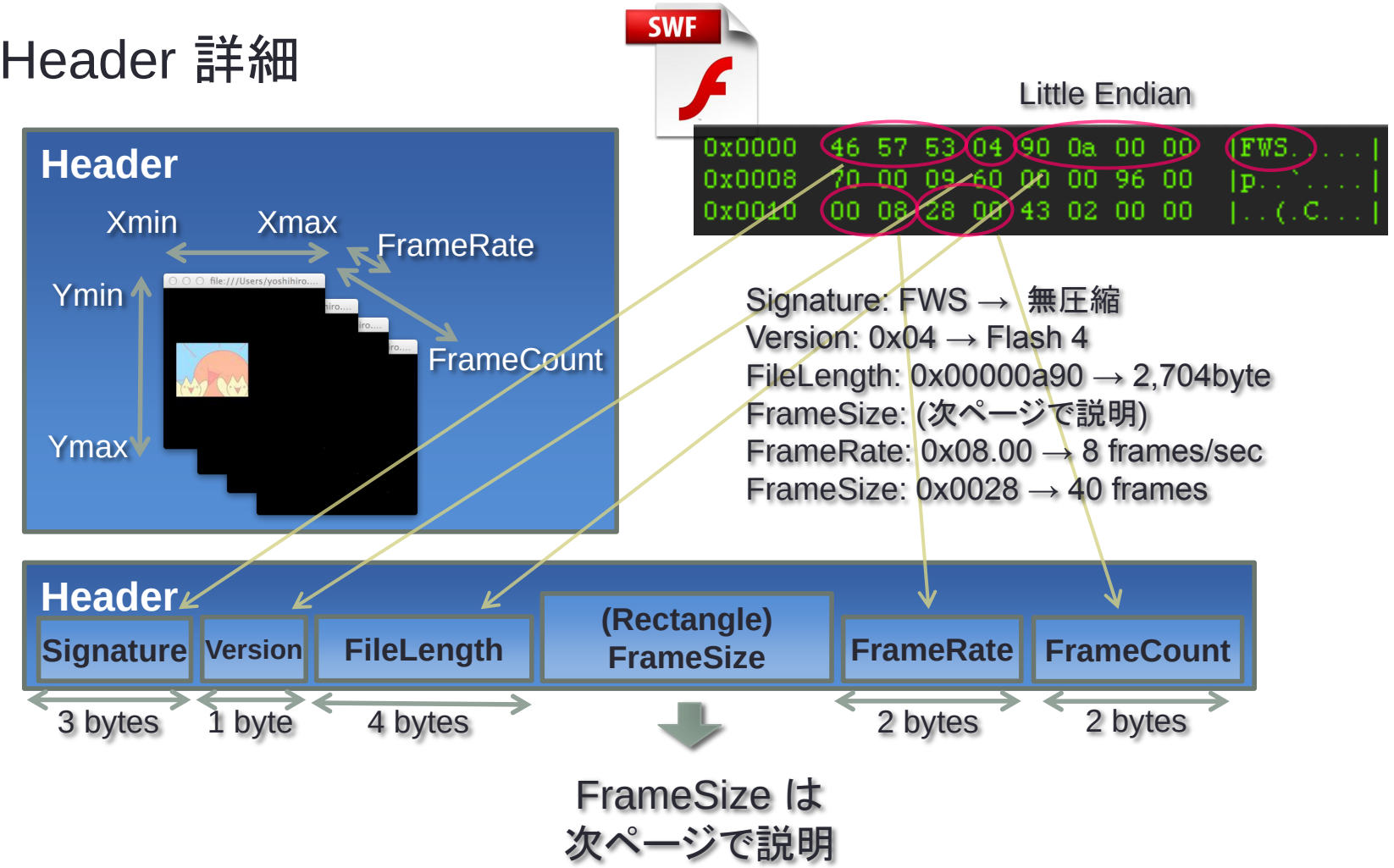
SWF 全体構造

- Header と Tag のイメージ　　＼概念／



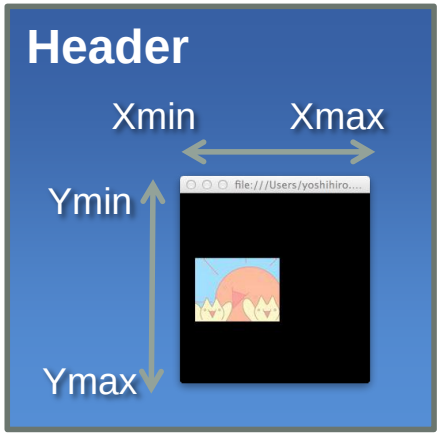
SWF Header

- Header 詳細

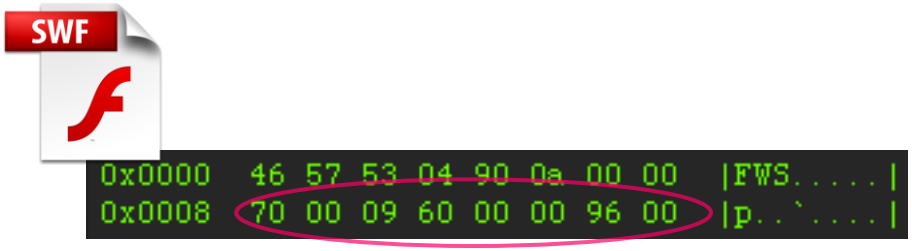


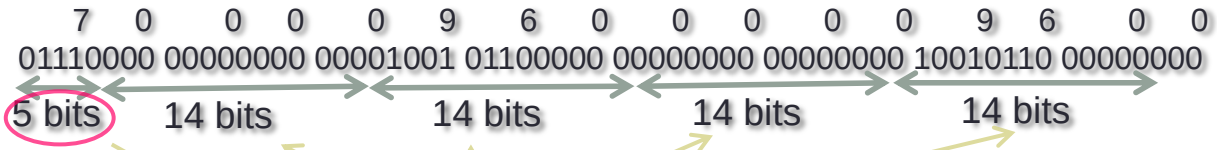
SWF Header FrameSize

- Header 詳細

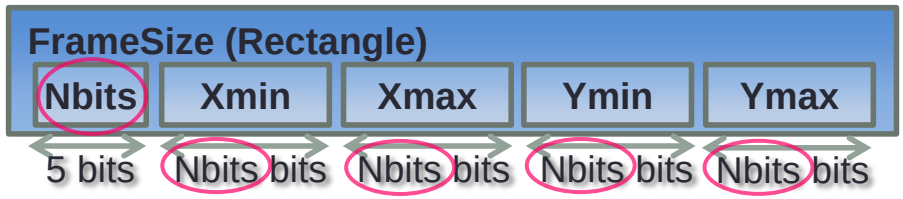


(Rectangle)
FrameSize



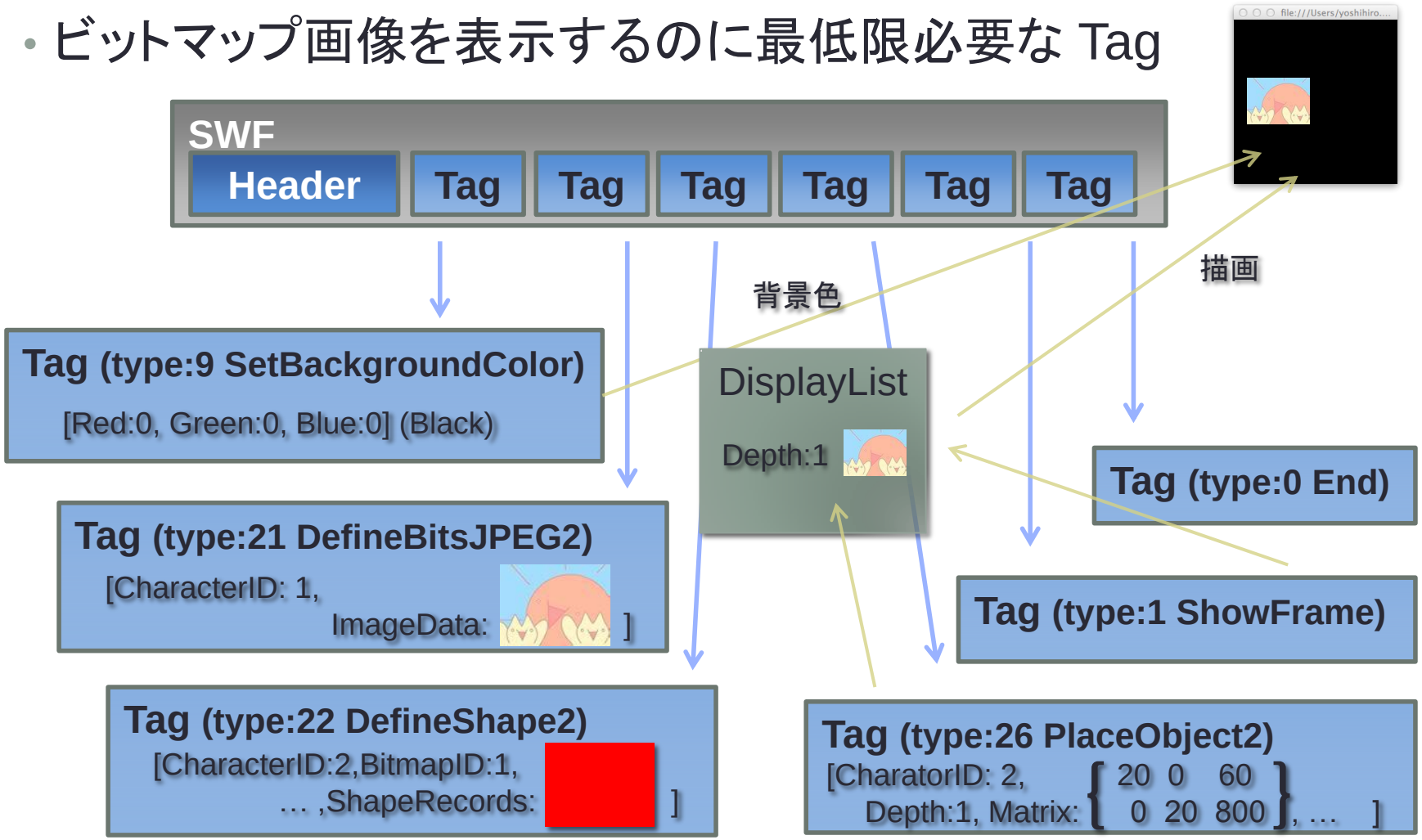


Nbits: 01110 → 14bits
Xmin: 000 00000000 000 → 0 twips → 0 pixel
Xmax: 01001 01100000 0 → 4800 twips → 240 pixel
Ymin: 0000000 0000000 → 0 twips → 0 pixel
Ymax: 0 10010110 00000 → 4800 twips → 240 pixel



SWF Tag example

- ビットマップ画像を表示するのに最低限必要な Tag



SWF Tag type

- SWF Tag type (仕様書の appendix B)

APPENDIX B

Reverse index of tag values

B

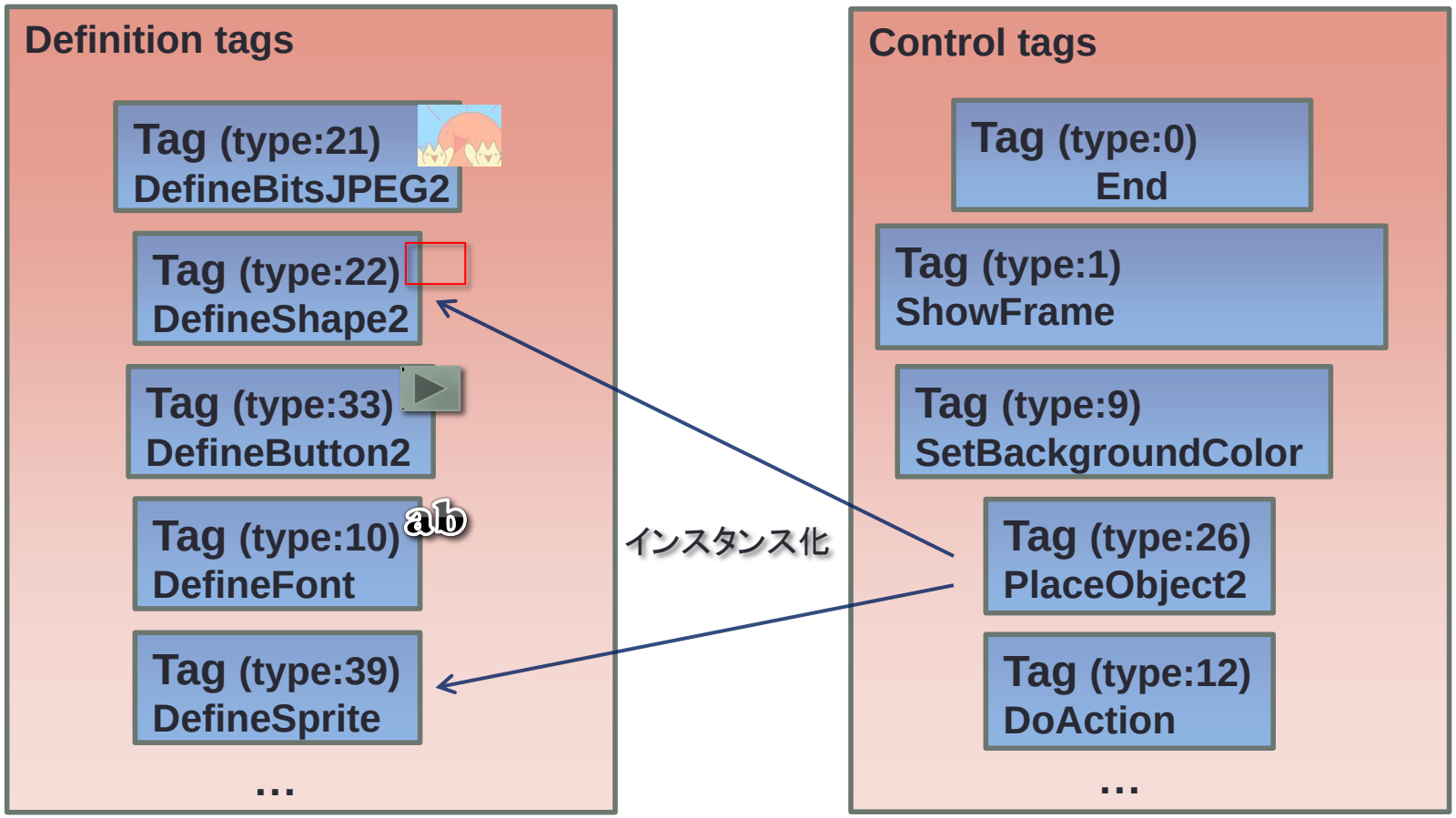
This table provides a quick lookup, allowing any tag in the SWF specification to be found by its tag value.

Tag type

Tag value	Tag name
0	End
1	ShowFrame
2	DefineShape
4	PlaceObject
5	RemoveObject
6	DefineBits
7	DefineButton
8	JPEGTables
9	SetBackgroundColor
10	DefineFont
11	DefineText
12	DoAction

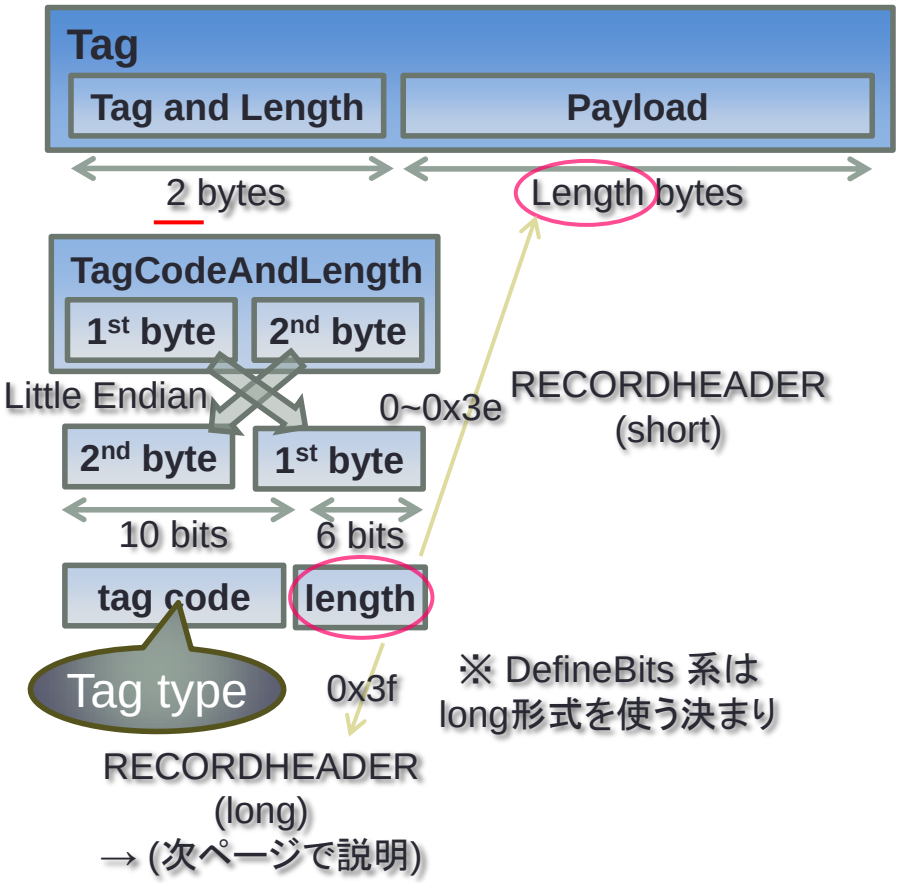
SWF Tag Categories

- SWF Tag type Categories



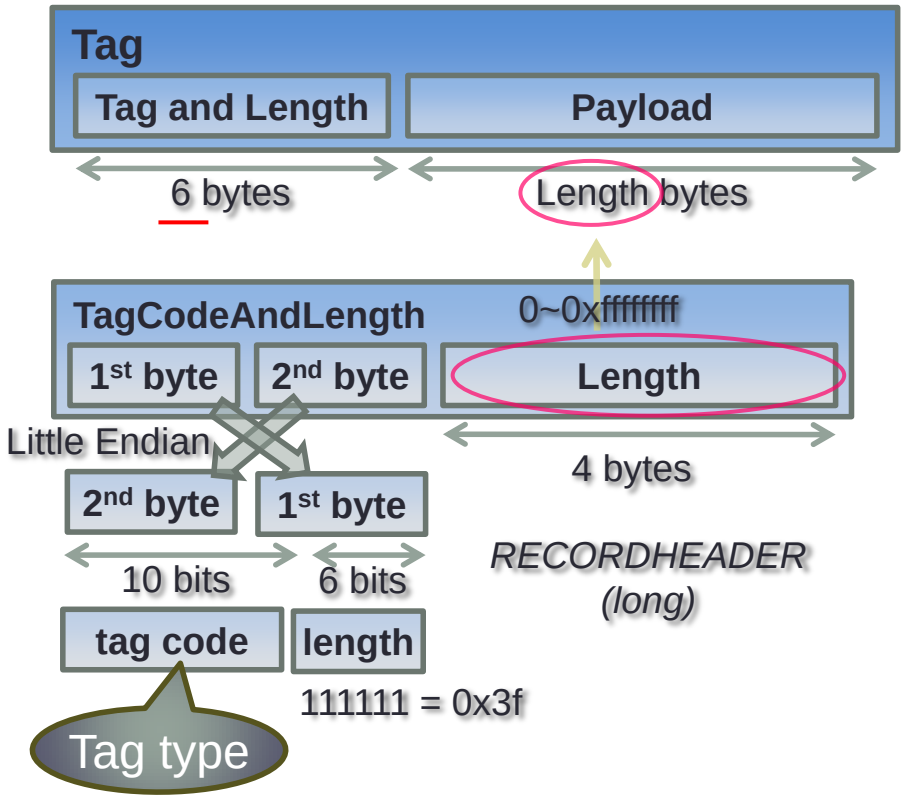
SWF Tag format (short) “ ≦ 0x3e ”

- SWF Tag 共通 format (short)



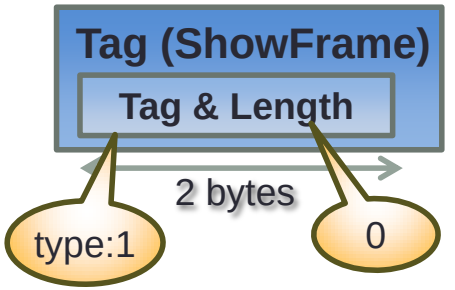
SWF Tag format (long) “ ≧ 0x3f ”

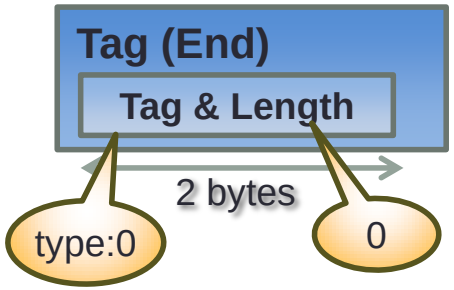
- SWF Tag 共通 format (long)



ShowFrame, End

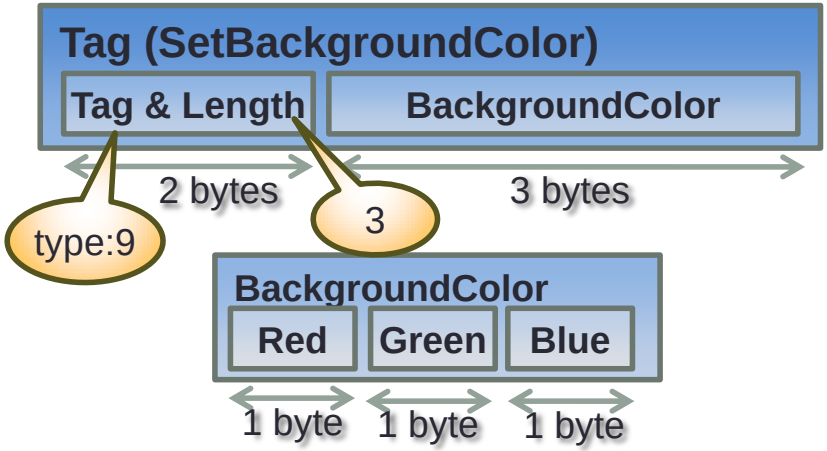
- ShowFrame, End (payload 無し)





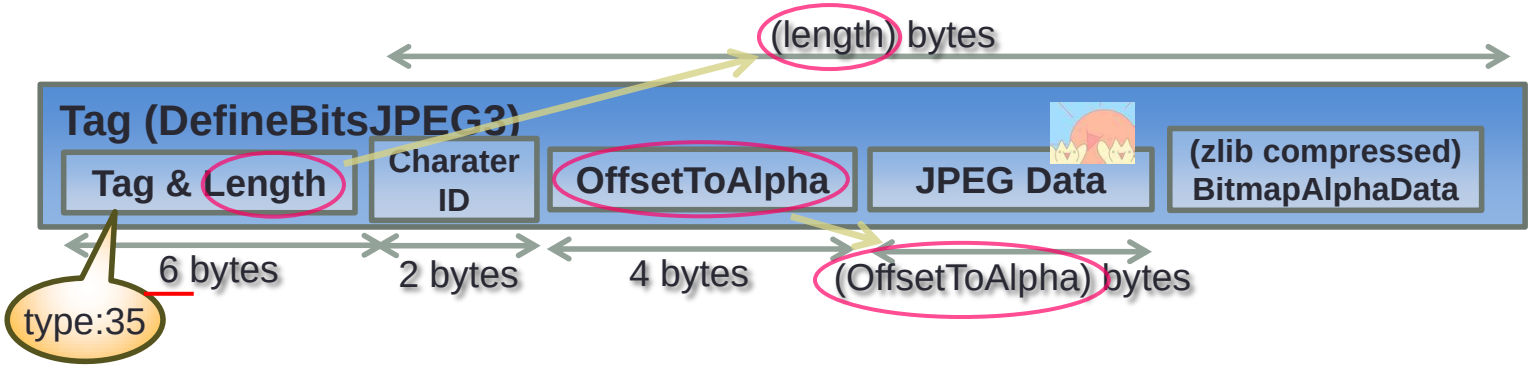
SetBackgroundColor (背景色設定)

- SetBackgroundColor (簡単な例)



DefineBitsJPEG (JPEG画像)

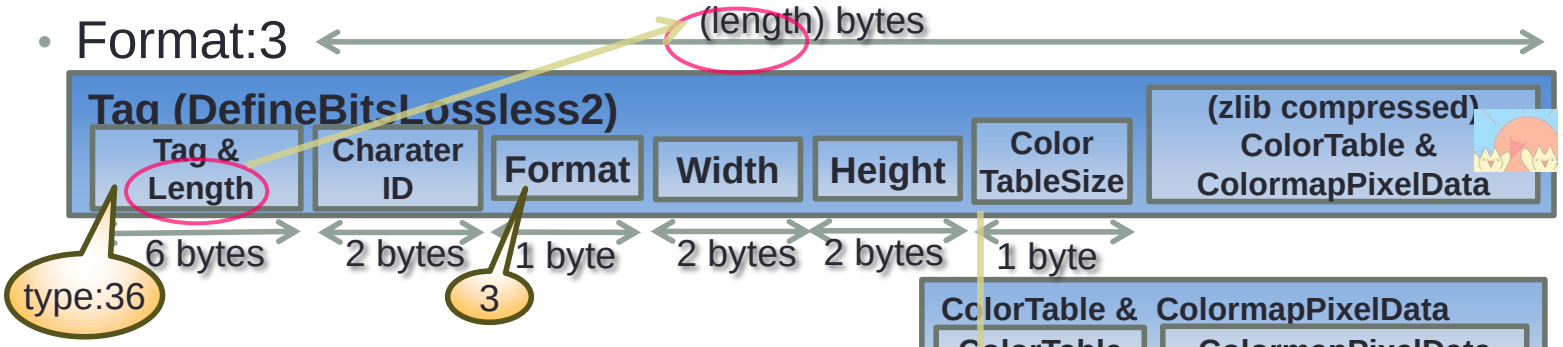
- DefineBitsJPEG3 (JPEG に透明度を追加したもの)



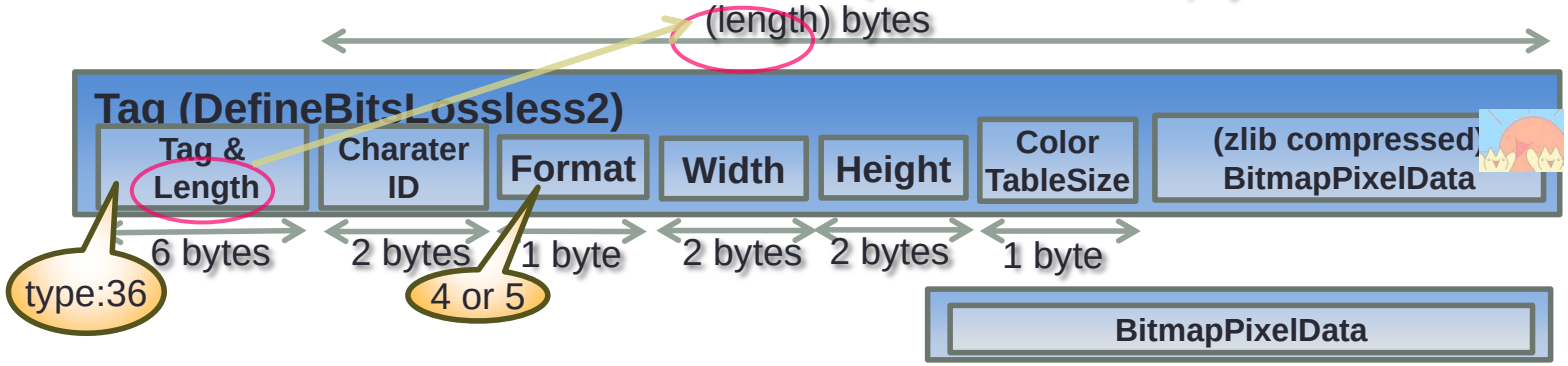
参考) http://labs.gree.jp/blog/2010/09/782/ SWFバイナリ編集のススメ第三回 (JPEG)

DefineBitsLossless (可逆圧縮画像)

- DefineBitsLossless2 (透明度付き PNG/GIF 画像)
  - Format:3



  - Format: 4, 5



参考) http://labs.gree.jp/blog/2010/12/1902/ SWFバイナリ編集のススメ第五回 (PNG)

DefineShape (ベクター画像)

- DefineShape2

参考) http://labs.gree.jp/blog/2011/04/2328/ SWFバイナリ編集のススメ第七回 (Shape基本構造)

PlaceObject (画像の貼り付け)

DoAction (ActionScript実行コード)

参考) http://labs.gree.jp/blog/2011/07/3259/ SWFバイナリ編集のススメ第八回 (Action – AS2 Bytecode編)

DefineButton (ボタンの振る舞い)

DefineSprite (シンボル)

まとめ

- 16bits, 32bits値は LittleEndian で埋まっている
- Bit は先頭から切り出せば OK
  - tag_and_lenght だけ 16Bits まとまってるので LittleEndian 処理
- Byte Alignment が重要
  - Matrix 等、情報要素によって Alignment を取るか決まる
  - 8Bit 単位でフラグが並んでいる場合は仕様書になくても alignment を取る
- あ
  - tag_and_lenght だけ 16Bits まとまってるので LittleEndian 処理