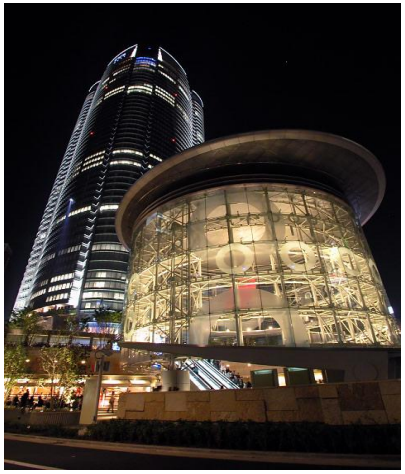
SWF研究会#2 発表#1

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>

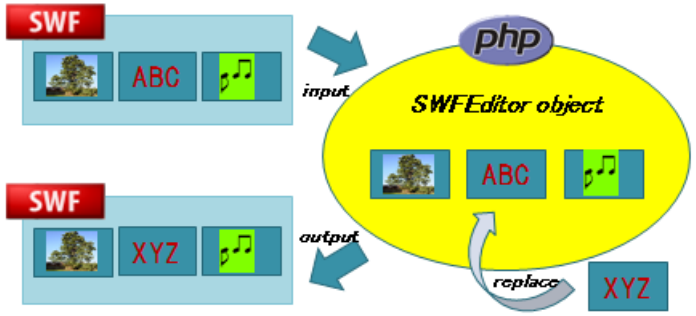
自己紹介

- 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

(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 ⇒ 画像も入れ替えちゃえ

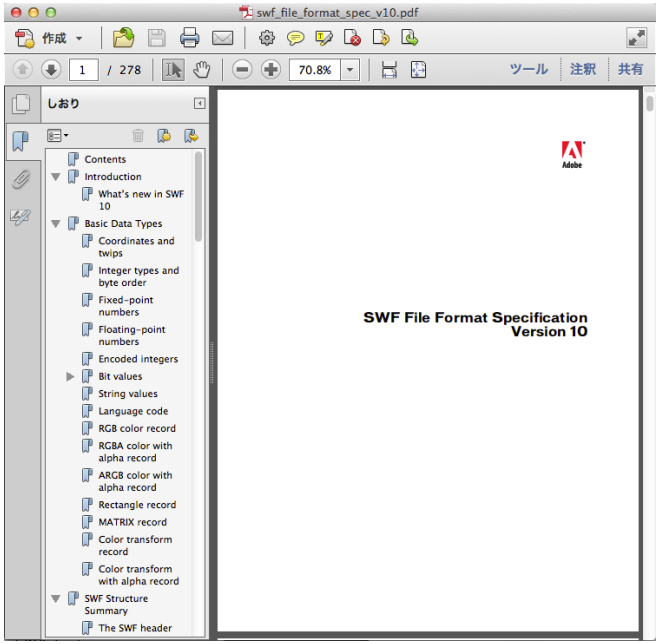
＼まさかの実行ファイル(SWF)編集／

- 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／

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

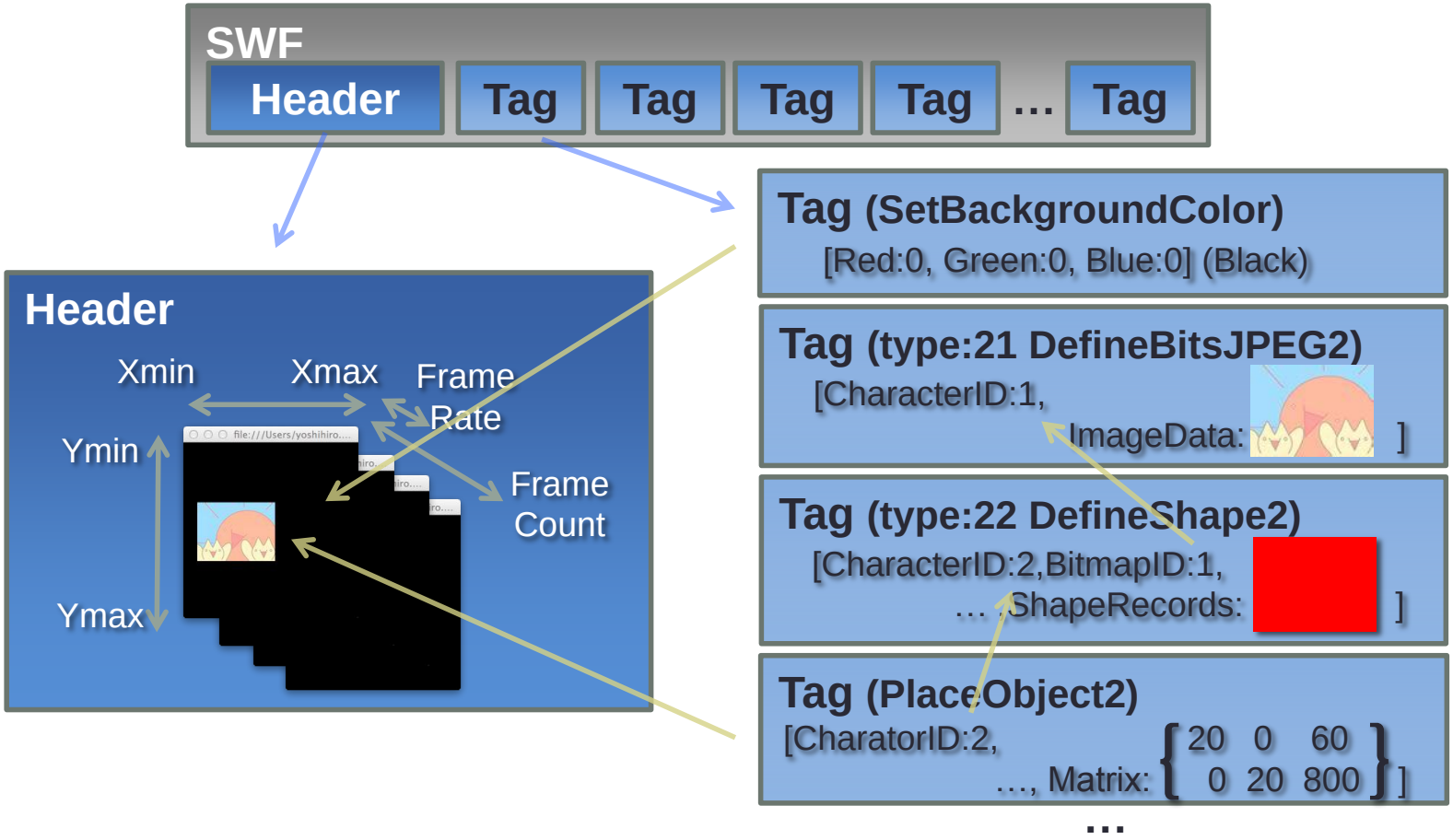


- 設計書レベルでは無い

- 自力で調べる必要あり
  - Flash Player のブラックボックス解析で仕様を推測する
  - 古本を漁る (お勧め → macromedia Flash ActionScript バイブル)

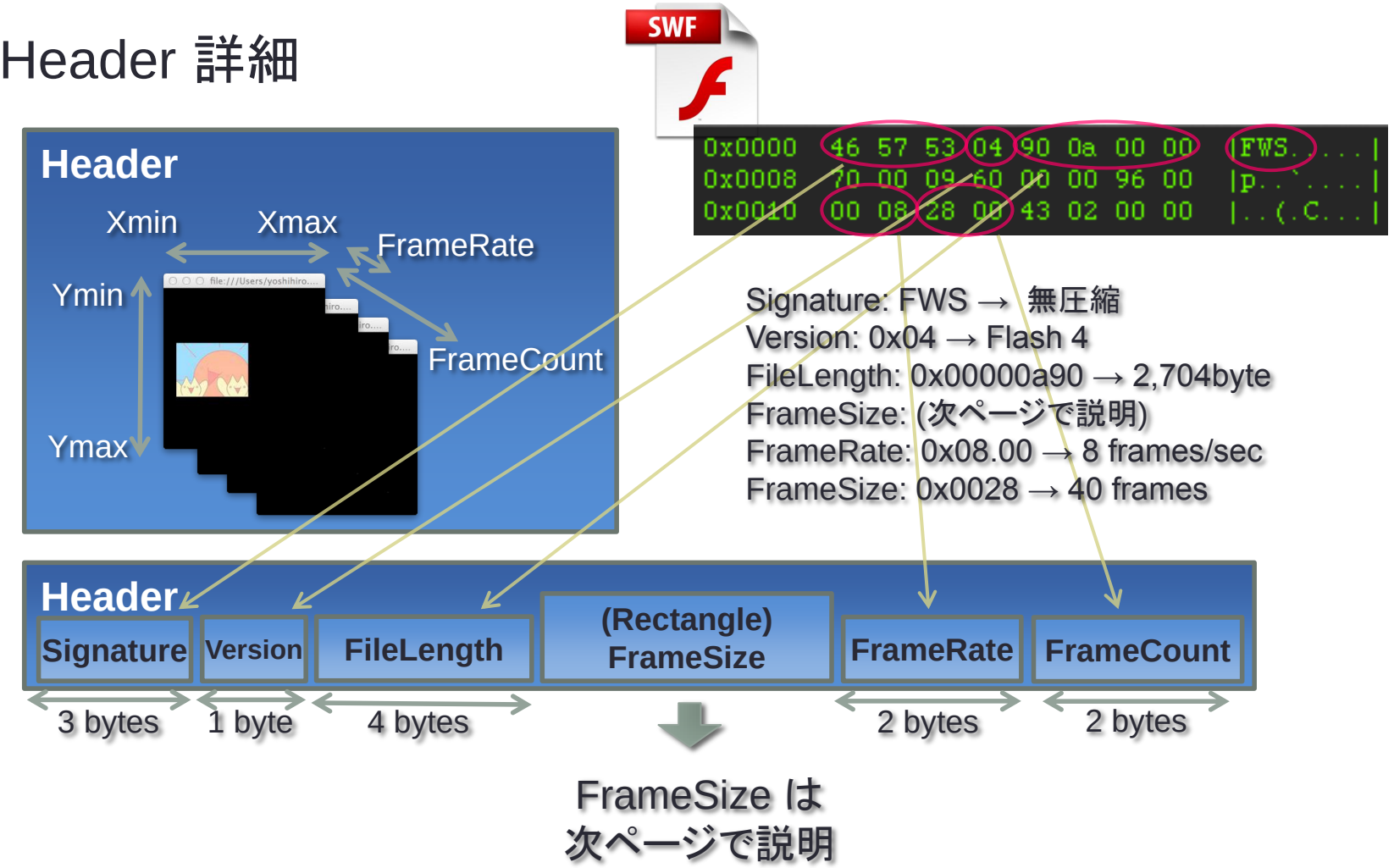
SWF 全体構造

- Header と Tag のイメージ　　＼概念／



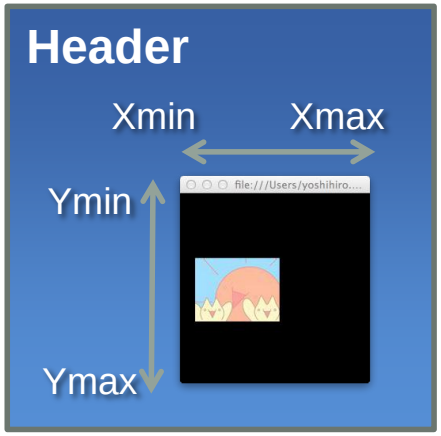
SWF Header

- Header 詳細

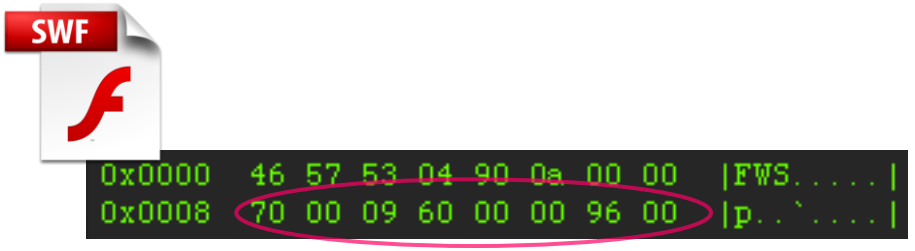


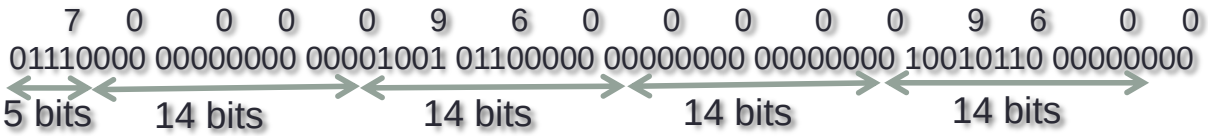
SWF Header FrameSize

- Header 詳細

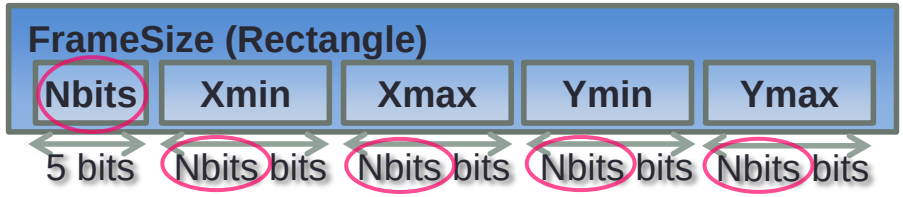


(Rectangle)
FrameSize



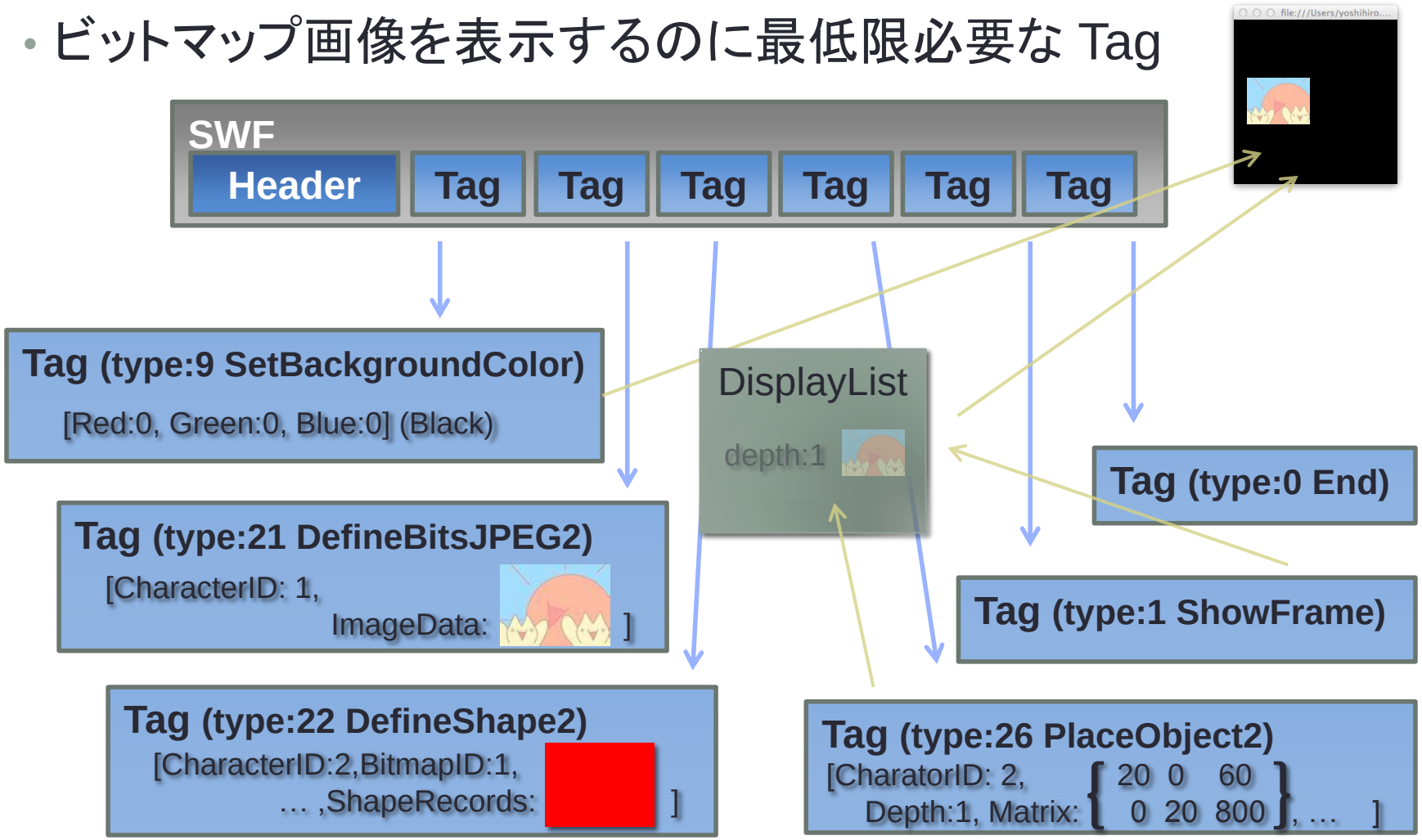


Nbits: 01110 → 14bits
Xmin: 000 00000000 000 → 0 twips → 0 pixel
Xmax: 01001 01100000 0 → 4800 twips → 240 pixel
Ymin: 0000000 0000000 → 0 twips → 0 pixel
Ymax: 0 10010110 00000 → 4800 twips → 240 pixel



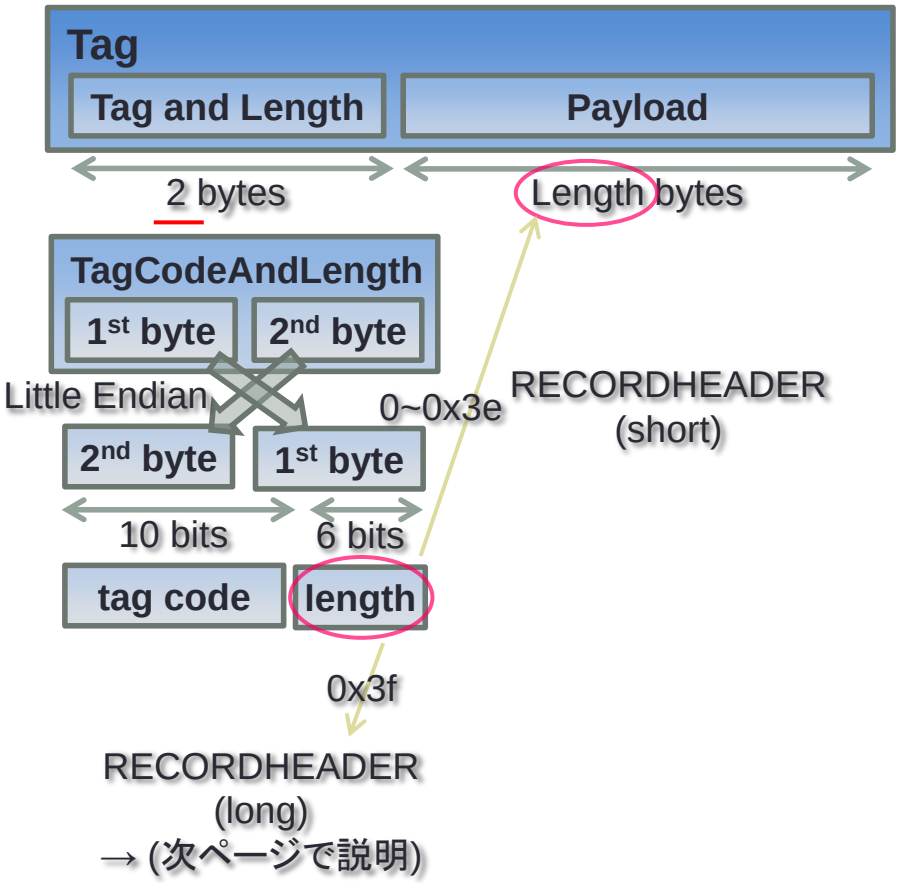
SWF Tag example

- ビットマップ画像を表示するのに最低限必要な Tag



SWF Tag format (short)

- SWF Tag 共通 format (short)



SWF Tag format (long)

- SWF Tag 共通 format (long)