



**JPEG テスト支援ツール**  
**iFuzzMaker**  
**操作手順書**  
**第 1. 0 版**

## 改訂履歴

版数	内容	改訂日
1.0	新規作成	2013/07/30

## 目次

---

1	はじめに .....	3
1.1	本書の読み方 .....	3
1.2	利用規約 .....	3
1.3	謝辞 .....	4
1.4	免責事項 .....	4
1.5	用語集 .....	4
2	概要 .....	5
2.1	iFuzzMaker とは .....	5
2.2	必要なもの .....	6
2.3	動作イメージ .....	7
2.4	iFuzzMaker の使い方 .....	8
3	操作手順 : iFuzzMaker を使ってみる .....	10
3.1	インストール .....	10
3.2	iFuzzMaker の操作 .....	10
3.3	アンインストール .....	22
4	使い方 : 製品のテストを使うデータを作る .....	23
4.1	JPEG ファイルの準備 .....	23
4.2	テストデータ生成ルールの作成 .....	23
5	一歩進んだ使い方 : Exif 仕様がない Exif タグもテストしたい .....	35
5.1	メーカー独自の Exif タグをテスト対象に追加する .....	35
5.2	SOF0 以外のセグメントもテスト対象に追加する .....	40
6	仕様 .....	46
6.1	動作環境 .....	46
6.2	コンパイル環境 .....	46
6.3	ファイル構成 .....	47
付録 A	Exif タグと JPEG ファイルの基礎知識 .....	50
	参考資料 .....	60

## 1 はじめに

本書は JPEG テスト支援ツール「iFuzzMaker」の使い方をまとめたものです。

### 1.1 本書の読み方

先ず「iFuzzMaker」を使ってみたい

**【2章】と【3章】を順番に読んでください。**

【2章】で「iFuzzMaker」の概要を掴んで、【3章】で「iFuzzMaker」の操作方法を理解してください。  
先ず使ってみたい場合、事前に何か準備する必要はありません。

製品のテストに使いたい

**【3章】と【4章】を中心で読んでください。**

Exif

製品のテストに「iFuzzMaker」を使いたい場合、テストの目的に応じた「JPEGファイル」と「テストデータ生成ルール」を準備していただきます。【4章】に従ってそれらを準備していただき、改めて【3章】の説明に基づき、「iFuzzMaker」を使ってください。

より様々なテストデータを作りたい

**【5章】を読んでください。**

Exif

「iFuzzMaker」の初期設定では、「JPEGファイルを読み込む機能」のうち、JPEGファイルに関する様々な情報を読み込む部分のテストに使えるテストJPEGファイルを作ります。しかし、「iFuzzMaker」の設定を変更することで、それ以外の部分のテストに使えるJPEGファイルも作れるようになります。その設定変更方法を知りたい場合、【5章】を読んでください。

動作仕様を知りたい

**【5章】と【6章】を読んでください。**

Exif

「iFuzzMaker」の仕組みやソースコードを使って、別のツールを開発する目的などで、「iFuzzMaker」の動作仕様(ファイル構成など)を知りたい場合、【6章】を読んでください。加えて、【5章】も動作仕様に近いため、【5章】を読むこともおすすめします。

**Exif** マークがある読み方を実践する場合、Exifの仕様に関する知識が必要となります。もし、Exifの仕様に関する知識をお持ちでない場合、適宜【付録A】を参照しながら読み進めてください。

### 1.2 利用規約

iFuzzMaker を利用するためには、別添の利用規約（JPEG テスト支援ツール 「iFuzzMaker」 利用規約）を確認、同意の上でご利用ください。

### 1.3 謝辞

iFuzzMaker は一般社団法人 カメラ映像機器工業会（CIPA）様から許可を得たうえで、下記の箇所について原文のまま転載利用させていただいております。転載利用を快諾していただいたカメラ映像機器工業会様に感謝いたします。

転載元	カメラ映像機器工業会規格 CIPA DC-008-2010 デジタルスチルカメラ用 画像ファイルフォーマット規格 Exif 2.3 <a href="http://www.cipa.jp/hyoujunka/kikaku/pdf/DC-008-2010_J.pdf">http://www.cipa.jp/hyoujunka/kikaku/pdf/DC-008-2010_J.pdf</a>
転載箇所 および 内容	転載元の以下の節における、IFD ポインタおよびタグについての「説明」、「Tag」、「Type」、「Count」、「Default」の説明文 4.6.3 Exif 固有の IFD 4.6.4 TIFF Rev.6.0 の付属情報 4.6.5 Exif IFD の付属情報 4.6.6 GPS に関する付属情報 4.6.7 互換性に関する付属情報

### 1.4 免責事項

iFuzzMaker を利用するための免責事項については、別添の利用規約（JPEG テスト支援ツール「iFuzzMaker」利用規約）の第 6 条を参照してください。

### 1.5 用語集

用語	説明
テストデータ生成ルール	JPEG ファイルのどこ（変更箇所）に、どのような値（テスト値）を埋め込むかを設定するルール
テスト値	テストデータ生成ルールに基づいて、テストデータとして出力する JPEG ファイルに埋め込む値
変更箇所	JPEG ファイル内でテスト値に置き換える部分
テストデータ	変更箇所をテスト値に置き換えた JPEG ファイル
Exif タグ	JPEG ファイルに含まれる、撮影日時やカメラの製造元などの画像に関する付帯情報（付録 A を参照）
セグメント内の要素	JPEG ファイルのセグメント内のマーカー、レンゲス、データ領域内の各データ（付録 A を参照）

## 2 概要

本章では、iFuzzMaker の概要について説明します。

### 2.1 iFuzzMaker とは

「iFuzzMaker」とは、「JPEG ファイル読み込む機能」を持つ製品に対するセキュリティテスト「ファジング<sup>1</sup>」（図 1）に使えるツールです。

製品の「JPEG ファイルを読み込む機能」に脆弱性が存在すると、問題を起こすデータ（例えば極端に長い文字列）を持つ JPEG ファイルを読み込んだ場合、製品の動作に問題（製品そのものの強制終了、最悪の場合、ウイルスへの感染や外部からの遠隔操作）が生じてしまいます。この脆弱性を作りこまないためには、製品出荷前に、このような JPEG ファイル（テストデータ）を読み込ませて、製品の動作に問題が生じないかを確認するセキュリティテスト「ファジング」が有効です。この「iFuzzMaker」では、ファジングで使うテストデータを作ることができます。

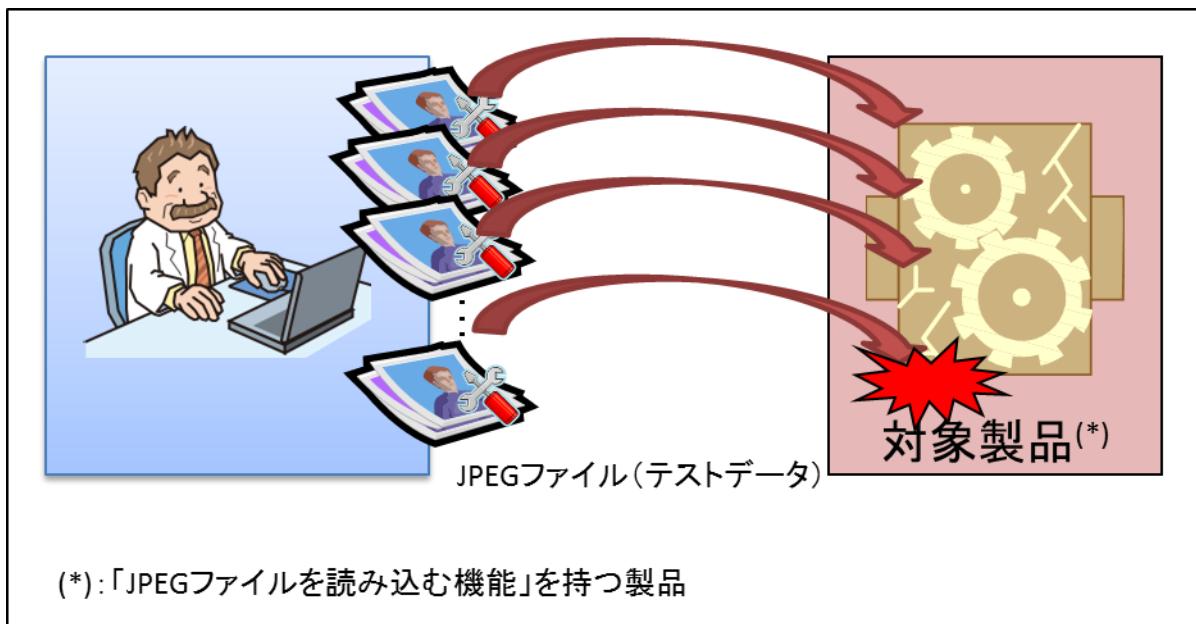


図 1 「JPEG ファイルを読み込む機能」に対するセキュリティテスト「ファジング」

<sup>1</sup> ファジングとは、検査対象の製品に、何万種類もの問題を引き起こしそうな値（例：極端に長い文字列など）を含んだテストデータを送り込み、製品の応答や挙動（例：製品が異常終了するなど）から脆弱性を検出するセキュリティテストです。ファジングについて詳しく知りたい方は、IPA が公開している「ファジング活用の手引き」をご覧ください。<http://www.ipa.go.jp/security/vuln/fuzzing.html>

## 2.2 必要なもの

iFuzzMaker を使うためには、「JPEG ファイル」と「テストデータ生成ルール」が必要となります。

iFuzzMaker を使って、製品をテストする場合にはそのテストに応じた「JPEG ファイル」と「テストデータ生成ルール」を準備する必要があります。iFuzzMaker には、動作確認を目的として「JPEG ファイル」と「テストデータ生成ルール」のサンプルファイルを同梱しています。まず iFuzzMaker を使ってみたい場合には、これらのサンプルファイルを使用してください。

表 1 iFuzzMaker を使うために必要なもの

必要なもの	説明
JPEG ファイル	<p>画像ファイルフォーマット規格 Exif 2.3 に準拠した JPEG ファイル。          この JPEG ファイルには、次の 2 つの情報が含まれていること。          (この理由については、2.3 を参照してください)</p> <ul style="list-style-type: none"> <li>● Exif タグ<sup>2</sup></li> <li>● SOFO<sup>3</sup></li> </ul> <p>■ 同梱サンプルファイル「IPA-SAMPLE.JPG」</p>
テストデータ生成ルール	<p>テストデータの作り方を定めたルールファイル。</p> <p>■ 同梱サンプルファイル          「sample-TestRule-List.txt」          「sample-TestRule1.txt」          「sample-TestRule2.txt」          「sample-TestRule3.txt」</p>

<sup>2</sup> Exif タグとは、デジタルカメラなどで撮影した JPEG ファイルに含まれる画像に関する情報です。この Exif タグには、デジタルカメラの製造元情報やモデル情報、JPEG ファイルを撮影したときの位置（GPS）情報などがあります。

<sup>3</sup> SOFO とは、JPEG ファイルに含まれる画像データそのものに関する情報です。SOFO には、画像の縦のサイズや横のサイズなどがあります。

## 2.3 動作イメージ

iFuzzMaker は、「テストデータ生成ルール」で定めた作り方をもとに、用意した「JPEG ファイル」の一部分を書き換えて、テストデータを作ります。

テストデータ生成ルールには、JPEG ファイルの「どこ」を「どのような値」で「どのように」書き換えるかを記述します。例えば、JPEG ファイルの Exif タグにおける「タイトル」を、「極端に長い文字列『AAAAAAA...』」に「置換」する、といったルールを記述します（図 2）。

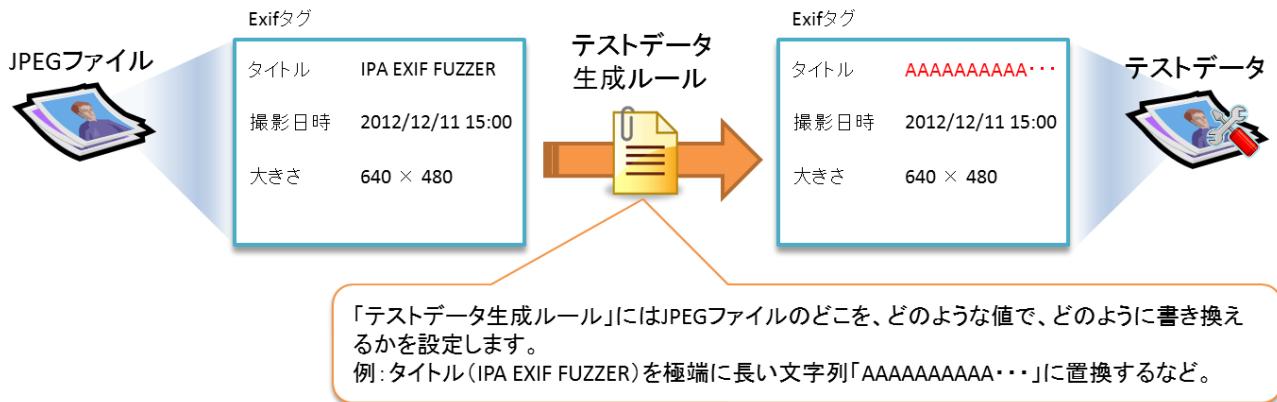


図 2 iFuzzMaker の動作イメージ

テストデータ生成ルールの「どのような値」には制約はありません。しかし、「どこ」と「どのように」については制約があります。

まず、テストデータ生成ルールの「どこ」については、JPEG ファイルに含まれる情報のうち、Exif タグと SOFO のみが対象となります。JPEG ファイルに含まれる Exif タグと SOFO 以外の情報を対象としている場合、iFuzzMaker の設定を変更する必要があります。

次に、テストデータ生成ルールの「どのように」については、「置換」、「上書き」と「挿入」の 3 種類のどれかから選ぶ必要があります。

## 2.4 iFuzzMaker の使い方

---

iFuzzMaker の用途に応じた使い方を説明します。

- 先ず「iFuzzMaker」を使ってみたい

iFuzzMaker の操作手順を確認したり、動作のイメージをつかむには、図 3 の「先は使ってみたい」のフローに沿って本書を読み進めて使ってください。サンプルの JPEG ファイルとサンプルのテストデータ生成ルールを使うことで、iFuzzMaker をすぐにお試しいただけます。

- 製品のテストに使いたい

iFuzzMaker を使ったテストでは、テストデータ次第で製品の脆弱性を検出できるかどうかが決まります。iFuzzMaker を製品のテストに使い、脆弱性を検出する（可能性のある）テストデータを作るには、JPEG ファイルとテストデータ生成ルールを準備して、どのようなテストデータを作成するかを決めることが重要です。このような場合は図 3 の「製品のテストに使いたい」のフローに沿って本書を読み進めて使ってください。

- より様々なテストデータを作りたい

メーカー独自の Exif タグを読み込む製品をテストするには、メーカー独自の Exif タグに応じたテストデータが必要です。iFuzzMaker はメーカー独自の Exif タグを追加するといったカスタマイズが可能です。iFuzzMaker にメーカー独自の Exif タグを追加して、より様々なテストデータを作成するには、図 3 の「より様々なテストデータを作りたい」のフローに沿って本書を読み進めて使ってください。

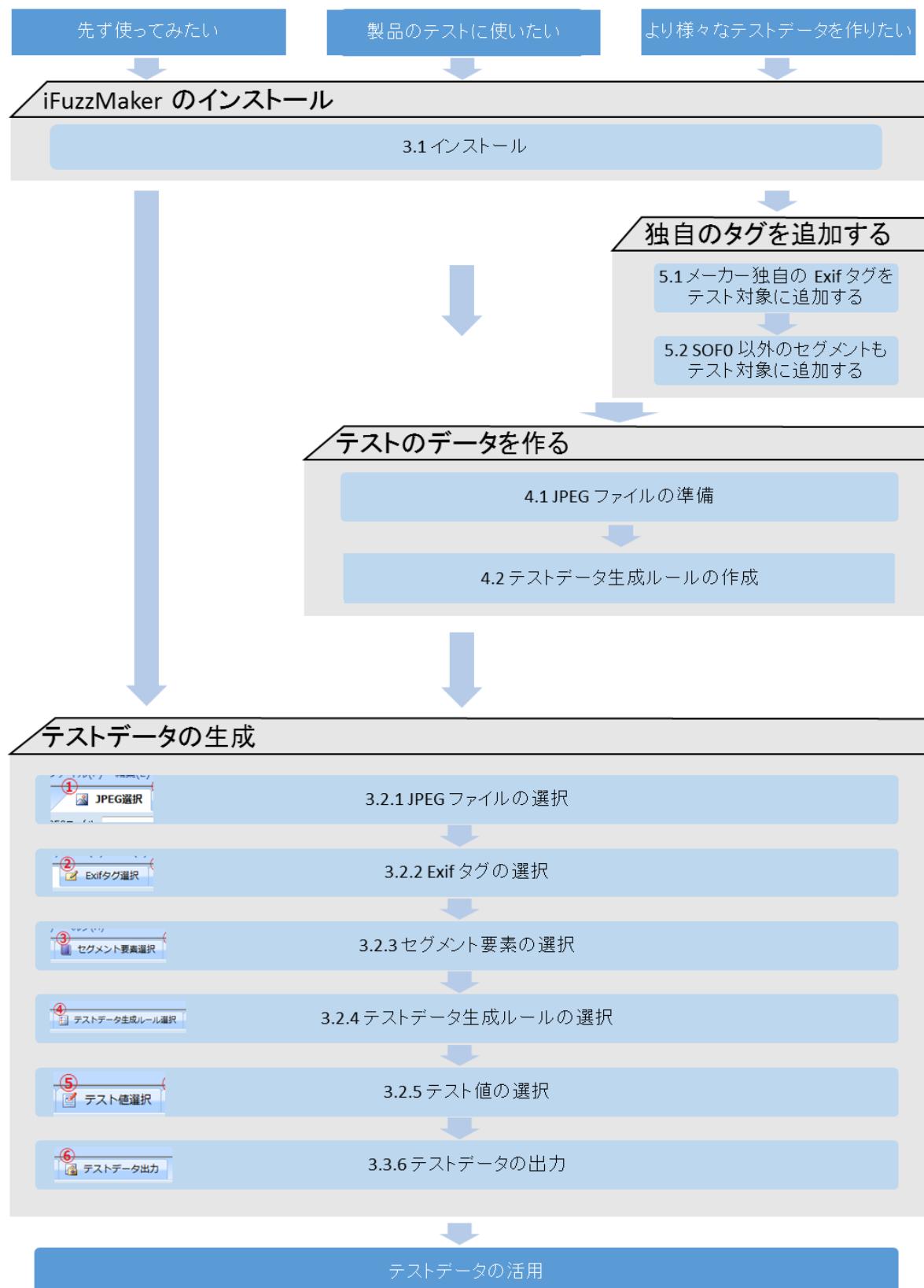


図 3 用途に応じた iFuzzMaker の使い方フロー

### 3 操作手順：iFuzzMaker を使ってみる

本章では、同梱のサンプルファイル「IPA-SAMPLE.JPG」と「sample-TestRule1.txt」「sample-TestRule-List.txt」を使用して、テストデータを生成する操作手順を説明します。同梱のサンプルファイルをお使いいただくと、3.2 からの手順で iFuzzMaker の動作を確認できます。

#### 3.1 インストール

1. ダウンロードした ZIP ファイルを適当なフォルダに展開します。
2. 展開したフォルダ内の iFuzzMaker フォルダを、任意のフォルダへコピーします（例 C:\ipa\iFuzzMaker など）。

#### 3.2 iFuzzMaker の操作

本節では iFuzzMaker を操作してテストデータを生成する手順を説明します。iFuzzMaker によるテストデータの生成は、6 つの Step で実施します。これら 6 つの Step は、iFuzzMaker の画面単位で実施します。図 4 は iFuzzMaker の画面例を示します。操作は画面の左端のタブから順に右へ設定します。



図 4 iFuzzMaker の画面例

- Step1 : JPEG ファイルの選択 (3.2.1)
- Step2 : Exif タグの選択 (3.2.2)
- Step3 : セグメント要素の選択 (3.2.3)
- Step4 : テストデータ生成ルールの選択 (3.2.4)
- Step5 : テスト値の選択 (3.2.5)
- Step6 : テストデータの出力 (3.2.6)

次節から iFuzzMaker の画面を交えながら、テストデータを生成するにはどのように操作するか説明します。

### 3.2.1 Step1 : JPEG ファイルの選択

JPEG ファイルの選択は、「JPEG 選択画面（図 5）」にて操作します。

この画面ではテストデータの元となる JPEG ファイル「IPA-SAMPLE.JPG」を選択します。

本 Step では JPEG ファイル「IPA-SAMPLE.JPG」を選択し、ファイル中にどのような Exif タグとセグメントが含まれているかを確認します。

図 5 を例に JPEG ファイルの選択手順を示します。

- (1) 図中①の「JPEG 選択」タブを選択し、JPEG 選択画面を表示します。iFuzzMaker 起動時に、JPEG 選択が表示されます。
  - (2) 図中②でサンプルの JPEG ファイル「IPA-SAMPLE.JPG」を指定します。入力欄の右端のアイコンをクリックするとファイル選択画面が開きます。
  - (3) 図中③の「解析」ボタンを押下すると、(2)で指定した JPEG ファイルの構造が解析されます。
  - (4) 解析結果として、図中の④の部分領域に JPEG ファイル内のセグメント、IFD、Exif タグなどがツリーとアイコン（表 2）で表示されます。また一覧にはオフセットやサイズなど（表 3）が表示されます。なお、解析できない不明なセグメントや Exif タグには、「×」が表示されます。
- 「×」になっている Exif タグのテスト値は、生成できません。

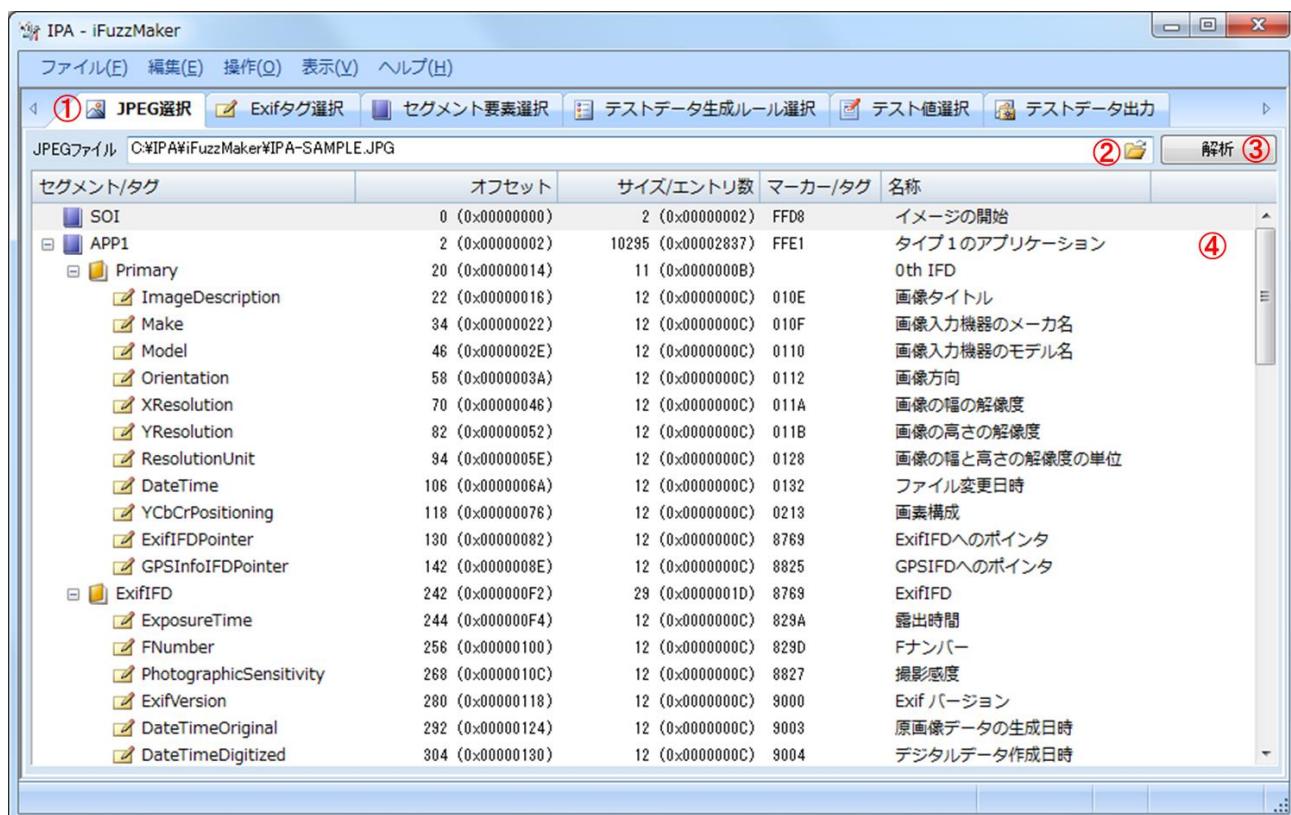


図 5 JPEG 選択画面

表 2 アイコン説明

アイコン	名称
	JPEG のセグメントを示します
	IFD を示します
	Exif タグを示します
	画像データを示します

表 3 JPEG 解析結果一覧の項目

項目	説明
セグメント/タグ	セグメント、IFD、タグ
オフセット	ファイルの先頭からのオフセット
サイズ／エントリ数	セグメントと Exif タグの場合は（12 バイト固定）領域のサイズ、IFD の場合はエントリ数
マーカー／タグ	セグメントマーカーまたは Exif のタグ
名称	セグメント、IFD、タグの名称

### 3.2.2 Step2 : Exif タグの選択

Exif タグの選択は「Exif タグ選択画面（図 6）」にて操作します。この画面では JPEG ファイル内の Exif タグに、どのようなタグやタイプ、値が設定されているかを確認し、変更箇所とする Exif タグを選択します。

図 6 を例に「Exif タグの選択」手順を示します。

- (1) 図中①の「Exif タグ選択」を選択し、Exif タグ選択画面を表示します。
- (2) 図中②に 3.2.1 で解析した JPEG ファイルの Exif タグが一覧表示（表 4）されます。
- (3) 図中③では一覧上で選択されている Exif タグの説明（表 5）が表示されます。
- (4) 一覧の Exif タグをチェックすると、変更箇所として選択されます。一覧は Ctrl キーや Shift キーにより複数選択可能です。マウスの右クリックメニューから全選択、チェック、解除の一括操作が可能です。また、リスト内の IFD 名④をクリックすると、IFD の中にあるタグがすべて選択されます（Windows 7 のみ）。
- (5) 図中⑤には現在一覧で選択されている行数と、チェックされている件数／総行数が表示されます。

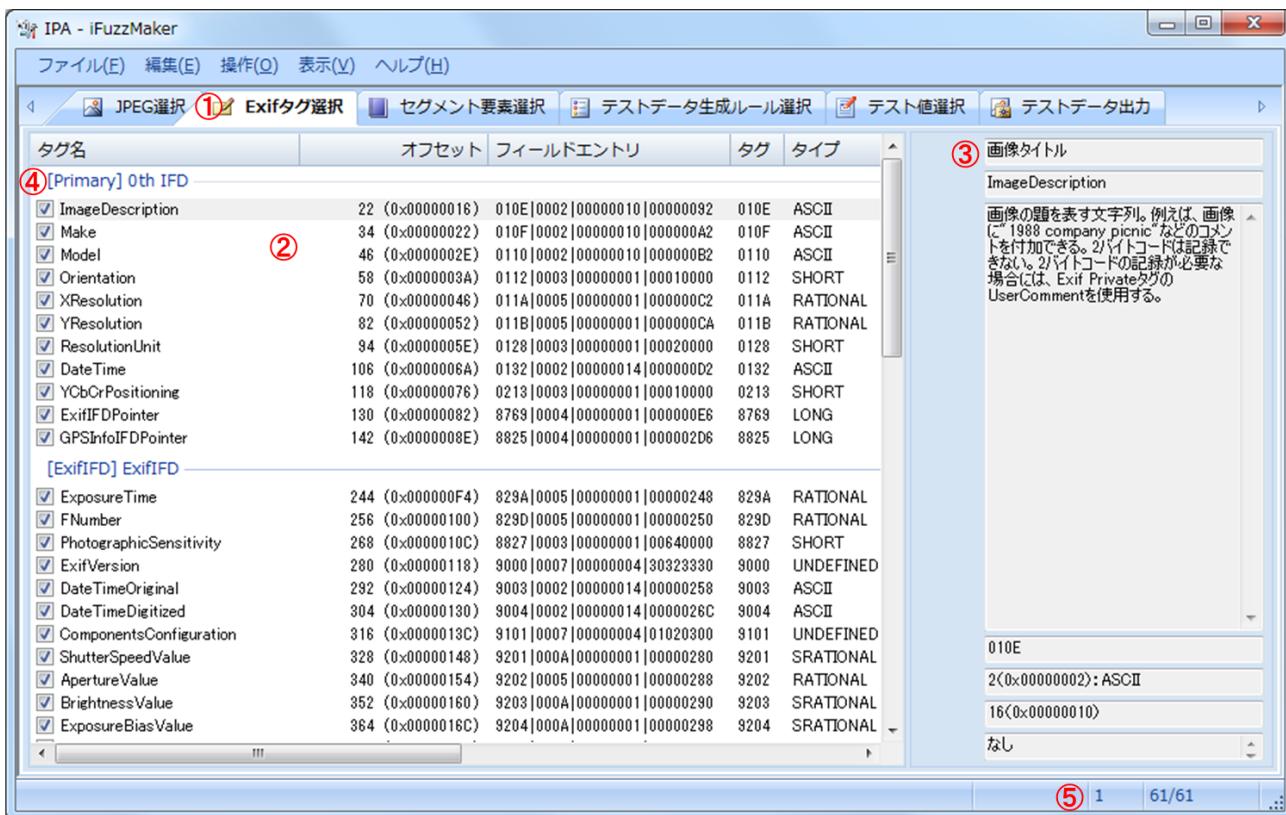


図 6 Exif タグ選択画面

表 4 Exif タグ一覧の項目

項目	説明
タグ名	タグ名
オフセット	ファイルの先頭からのオフセット
フィールドエントリ	フィールドエントリの 16 進ダンプ
タグ	タグ
タイプ	タイプ
カウント	カウント
値／オフセット	値／オフセット
データオフセット	実際の値へのファイルの先頭からのオフセット
データサイズ	実際の値のバイトサイズ
データ値	タイプが BYTE、SHORT、LONG、SLONG の場合は数値、 RATIONAL、SRATIONAL の場合は分数、ASCII、UNDEFINED の場合は文字列として値を表示

表 5 Exif タグの説明項目

項目	説明
タグ	タグの日本語表記
タグ名	タグの英語表記
説明	タグの説明
Tag	フィールドエントリのタグ
Type	タグに設定できるタイプ
Count	タグに設定できるカウント
Default	タグのデフォルト値

### 3.2.3 Step3：セグメント要素の選択

セグメント要素の選択は「セグメント要素選択画面（図 7）」にて操作します。この画面では JPEG ファイル内のセグメントに、マーカー、レングス、データ領域内の各データが設定されているかを確認し、変更箇所とするセグメント要素を選択します。

図 7 を例にセグメント要素の選択手順を示します。

- (1) 図中①の「セグメント要素選択」タブを選択し、セグメント要素選択画面を表示します。
- (2) 図中②には 3.2.1 で解析した JPEG ファイルのセグメントが一覧表示（表 6）されます。
- (3) 一覧のセグメント要素をチェックすると、変更箇所として選択されます。一覧は Ctrl キーや Shift キーにより複数選択可能です。マウスの右クリックメニューから全選択、チェック、解除の一括操作が可能です。また、リスト内のセグメント名③をクリックすると、セグメント内の要素がすべて選択されます（Windows 7 のみ）。
- (4) 図中④には現在一覧で選択されている行数と、チェックされている件数／総行数が表示されます。

セグメント要素	オフセット	サイズ	データ値	データ値(HEX)	説明
③ [SOF0] フレームタイプ 0 開始					
<input checked="" type="checkbox"/> Marker	10431 (0x000028BF)	2 (0x00000002)	49407	FF C0	Marker
<input checked="" type="checkbox"/> Lf	10433 (0x000028C1)	2 (0x00000002)	4352	00 11	Frame header len
<input checked="" type="checkbox"/> P	10435 (0x000028C3)	1 (0x00000001)	8	08	Sample precisor
<input checked="" type="checkbox"/> Y	10436 (0x000028C4)	2 (0x00000002)	57345	01 E0	Number of lines
<input checked="" type="checkbox"/> X	10438 (0x000028C6)	2 (0x00000002)	32770	02 80	Number of samp
<input checked="" type="checkbox"/> Nf	10440 (0x000028C8)	1 (0x00000001)	3	03	Number of image
<input checked="" type="checkbox"/> Ci	10441 (0x000028C9)	1 (0x00000001)	1	01	Component ident
<input checked="" type="checkbox"/> Hi/Vi	10442 (0x000028CA)	1 (0x00000001)	34	22	Horizontal sampl
<input checked="" type="checkbox"/> Tqi	10443 (0x000028CB)	1 (0x00000001)	0	00	Quantization tabl
<input checked="" type="checkbox"/> Ci	10444 (0x000028CC)	1 (0x00000001)	2	02	Component ident
<input checked="" type="checkbox"/> Hi/Vi	10445 (0x000028CD)	1 (0x00000001)	17	11	Horizontal sampl
<input checked="" type="checkbox"/> Tqi	10446 (0x000028CE)	1 (0x00000001)	1	01	Quantization tabl
<input checked="" type="checkbox"/> Ci	10447 (0x000028CF)	1 (0x00000001)	3	03	Component ident
<input checked="" type="checkbox"/> Hi/Vi	10448 (0x000028D0)	1 (0x00000001)	17	11	Horizontal sampl
<input checked="" type="checkbox"/> Tqi	10449 (0x000028D1)	1 (0x00000001)	1	01	Quantization tabl

図 7 セグメント要素選択画面

表 6 Exif タグ一覧の項目

項目	説明
セグメント要素	セグメント要素名
オフセット	ファイルの先頭からのオフセット
サイズ	要素のバイトサイズ
データ値	値
データ値 (HEX)	値の16進ダンプ
説明	セグメント要素の説明

### 3.2.4 Step4：テストデータ生成ルールの選択

テストデータ生成ルールの選択は「テストデータ生成ルール選択画面（図 8）」にて操作します。この画面ではテストデータ生成ルールリスト定義ファイルからテストデータ生成ルールを選択します。

図 8 を例にテストデータ生成ルールの選択手順を示します。

- (1) 図中①の「テストデータ生成ルール選択」タブを選択します。
- (2) 図中②にサンプルのテストデータ生成ルールリスト定義ファイル「sample-TestRule-List.txt」を指定します。入力欄の右端のアイコンをクリックするとファイル選択画面が開きます。
- (3) 図中③の「読み込」ボタンを押すと、サンプルのテストデータ生成ルールファイルを読み込みます。
- (4) 図中④にテストデータ生成ルールファイルに設定された、テストデータ生成ルールの内容（表 7）が一覧表示されます。
- (5) この画面でチェックされたテストデータ生成ルールと変更箇所から、テスト値選択画面（3.2.5）の一覧が作成されます。一覧は Ctrl キー や Shift キーにより複数選択可能です。マウスの右クリックメニューから全選択、チェック、解除の一括操作が可能です。また、リスト内のテストデータ生成ルール名⑤をクリックすると、テストデータ生成ルール内のテスト値がすべて選択されます（Windows 7 のみ）。
- (6) 図中⑥は現在一覧で選択されている行数と、チェックされている件数／総行数が表示されます。

ルール名	データ形式	値	繰返し数	書換モード	変更箇所	変更箇所指定	対象変更箇所	説明
<b>⑤ Stack/Heap Overflows</b>								
A * 1	テキスト	A	1	置換	値	なし		'A'を1回繰り返し
A * 33	テキスト	A	33	置換	値	なし		'A'を33回繰り返し
A * 128	テキスト	A	128	置換	値	なし		'A'を128回繰り返し
A * 240	テキスト	A	240	置換	値	なし		'A'を240回繰り返し
A * 255	テキスト	A	255	置換	値	なし		'A'を255回繰り返し
A * 256	テキスト	A	256	置換	値	なし		'A'を256回繰り返し
A * 257	テキスト	A	257	置換	値	なし		'A'を257回繰り返し
A * 420	テキスト	A	420	置換	値	なし		'A'を420回繰り返し
A * 511	テキスト	A	511	置換	値	なし		'A'を511回繰り返し
A * 512	テキスト	A	512	置換	値	なし		'A'を512回繰り返し
A * 1023	テキスト	A	1023	置換	値	なし		'A'を1023回繰り返し
A * 1024	テキスト	A	1024	置換	値	なし		'A'を1024回繰り返し
A * 2047	テキスト	A	2047	置換	値	なし		'A'を2047回繰り返し
A * 2048	テキスト	A	2048	置換	値	なし		'A'を2048回繰り返し
A * 4096	テキスト	A	4096	置換	値	なし		'A'を4096回繰り返し
A * 4097	テキスト	A	4097	置換	値	なし		'A'を4097回繰り返し
A * 5000	テキスト	A	5000	置換	値	なし		'A'を5000回繰り返し
A * 10000	テキスト	A	10000	置換	値	なし		'A'を10000回繰り返し
A * 20000	テキスト	A	20000	置換	値	なし		'A'を20000回繰り返し
A * 32762	テキスト	A	32762	置換	値	なし		'A'を32762回繰り返し
A * 32763	テキスト	A	32763	置換	値	なし		'A'を32763回繰り返し
A * 32764	テキスト	A	32764	置換	値	なし		'A'を32764回繰り返し

図 8 テストデータ生成ルール選択画面

表 7 テストデータ生成ルール選択一覧の項目

項目	説明
ルール名	表示名
データ形式	値のデータ形式 テキスト、10進数(8、16、32ビット・ビッグエンディアン、リトルエンディアン)、16進ダンプ、ファイルのいずれか
値	値
繰返し数	値の繰り返し回数
書換モード	置換、上書き、挿入のいずれか
変更箇所	タグ、タイプ、カウント、値、オフセット、セグメント要素、ファイル位置指定のいずれか
変更箇所指定	なし、タグ、タイプ、セグメント要素、ファイル位置のいずれか
対象変更箇所	タグ、タイプ、セグメント要素、ファイル位置のいずれか
説明	テストデータ生成ルールの説明

### 3.2.5 Step5：テスト値の選択

テスト値の選択は「テスト値選択画面（図 9）」にて操作します。この画面では選択された Exif タグとセグメント要素、テストデータ生成ルールから、生成できるテスト値の一覧を作成します。この一覧から最終的にファイルとして出力するテストデータを決定します。

図 9 を例にテスト値の選択手順を示します。

- (1) 図中①の「テスト値選択」タブを選択します。
- (2) 図中②の「表示」ボタンを押します。
- (3) 図中③に Exif タグ選択画面とセグメント要素選択画面で選択された変更箇所と、テストデータ生成ルール選択画面で選択されたテストデータ生成ルールから、出力できるテスト値の一覧（表 8）が表示されます。一覧に表示されるテスト値の数は、およそ「変更箇所数×テストデータ生成ルール数=テスト値数」です。
- (4) 一覧のテスト値をチェック（図中④）すると、テストデータ出力画面（3.2.6 参照）でテストデータとして出力されます。一覧は Ctrl キーや Shift キーにより複数選択可能です。マウスの右クリックメニューから全選択、チェック、解除の一括操作が可能です。
- (5) 図中⑤には現在一覧で選択されている行数と、チェックされている件数／総行数が表示されます。

The screenshot shows the IPA - iFuzzMaker application window. The menu bar includes ファイル(E), 編集(E), 操作(O), 表示(V), and ヘルプ(H). The toolbar has icons for JPEG選択, Exifタグ選択, セグメント要素選択, テストデータ生成ルール選択, テスト値選択 (highlighted with a red circle ①), and テストデータ出力. The main area is a table with the following columns: タグ/マーカー, タグ名/セグメント要素, 書換モード, 変更箇所, ルール名, and 説明. The table contains numerous rows for the 'ImageDescription' tag, each with a checked checkbox in the first column (highlighted with a red circle ④). The 'ルール名' column shows various loop counts starting from A \* 1 and increasing by increments of 33 up to A \* 32768. The '説明' column provides a brief description of each rule. The top right of the table has a '表示' button with a red circle ②. The bottom right corner of the table shows the current page number (5), total page count (1), and total row count (11895/11895). A red circle ③ points to the table area.

図 9 テスト値選択画面

表 8 テスト値選択一覧の項目

項目	説明
タグ/マーカー	Exif のタグ、セグメントマーカー、File（変更箇所がファイル位置指定の場合）のいずれか
タグ名/セグメント名	タグ名、セグメント名、挿入位置（変更箇所がファイル位置指定の場合）のいずれか
書換モード	置換、上書き、挿入のいずれか
変更箇所	タグ、タイプ、カウント、値、オフセット、セグメント要素、ファイル位置指定のいずれか
ルール名	ルール名
説明	テストデータ生成ルールの説明

### 3.2.6 Step6：テストデータの出力

テストデータの出力は「テストデータ出力画面（図 10）」にて操作します。この画面では選択されたテストデータをファイル出力します。

図 10 を例にテストデータの出力手順を示します。

- (1) 図中①の「テストデータ出力」タブを選択します。
- (2) 図中②にテストデータの出力先フォルダを指定します。入力欄の右端のアイコンをクリックすると別画面からフォルダを選択できます。
- (3) 図中③にテストデータ出力時の備考を必要に応じて入力します。入力内容は、テストデータとともに出力されるテストデータ一覧の備考欄に反映されます。
- (4) 図中④「テストデータ出力」ボタンを押下すると、指定した出力先に現在の日時を名称したフォルダ（年月日時分秒ミリ秒 例：20130719115328083）が作成され、その配下にテストデータが出力されます。出力を中止するにはキャンセルボタンを押下します。テストデータのファイル名は「00000001.jpg」からの連番で出力されます。またテストデータの出力後、テストデータの一覧がタブ区切りのテキストファイルで出力されます（図 11）。
- (5) テストデータの出力状況は図中⑤に一覧（表 9 の内容）表示されます。
- (6) テストデータの出力途中経過は、図中⑥で確認できます。

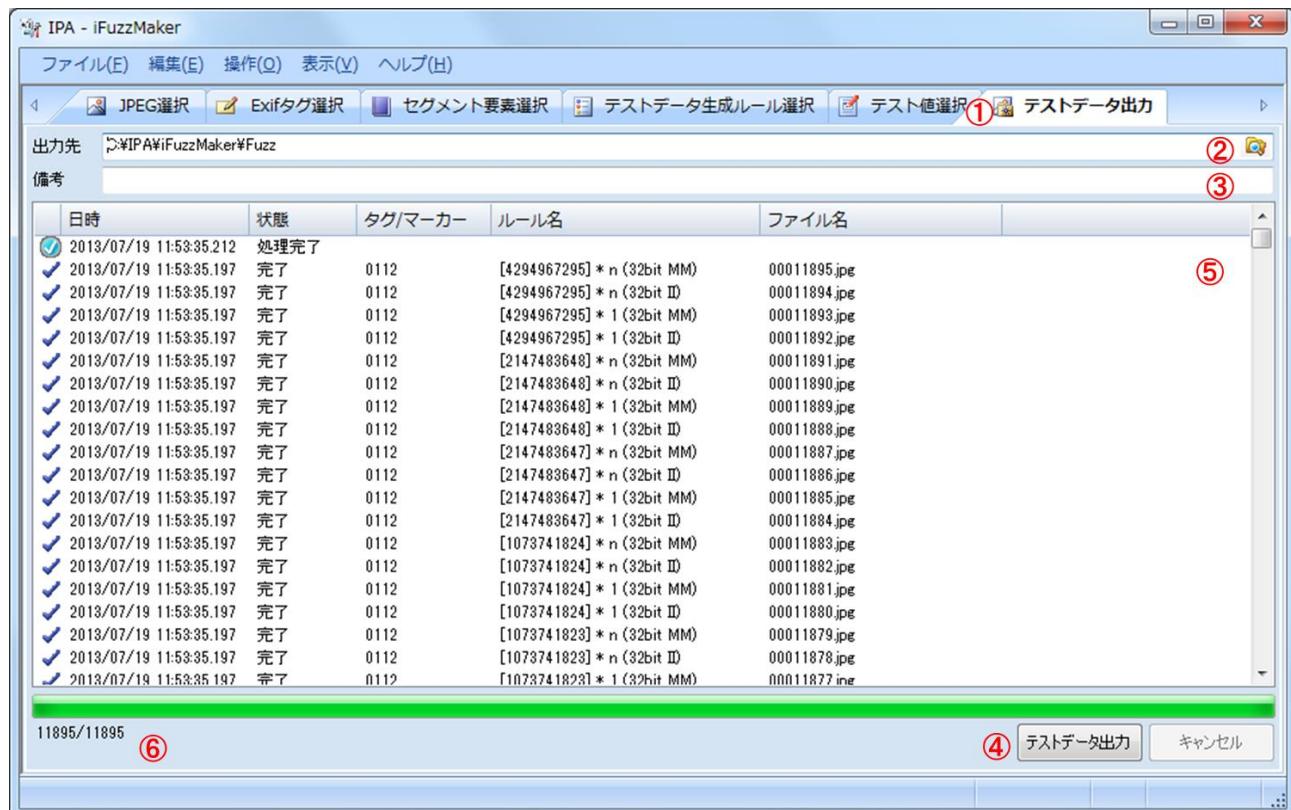


図 10 テストデータ出力画面

表 9 テストデータの出力状況の項目

項目	説明
日時	出力日時
状態	テストデータの出力状況
タグ/マーカー	Exif タグ、セグメントマーカー、File (変更箇所がファイル位置指定の場合) のいずれか
ルール名	ルール名
ファイル名	出力されるファイル名

元ファイル名	C:\YIPIA\YiFuzzMaker\YIPIA-SAMPLE.JPG					
出力日時	2013/07/19 11:53:28.083					
備考						
マーカー/タグ	名称	書換モード	変更箇所	ルール名	説明	ファイル名
010E	ImageDescription	置換	値	A * 1	'A'を1回繰り返し	00000001.jpg
010E	ImageDescription	置換	値	A * 33	'A'を33回繰り返し	00000002.jpg
010E	ImageDescription	置換	値	A * 128	'A'を128回繰り返し	00000003.jpg
010E	ImageDescription	置換	値	A * 240	'A'を240回繰り返し	00000004.jpg
010E	ImageDescription	置換	値	A * 255	'A'を255回繰り返し	00000005.jpg
010E	ImageDescription	置換	値	A * 256	'A'を256回繰り返し	00000006.jpg
010E	ImageDescription	置換	値	A * 257	'A'を257回繰り返し	00000007.jpg
010E	ImageDescription	置換	値	A * 420	'A'を420回繰り返し	00000008.jpg
010E	ImageDescription	置換	値	A * 511	'A'を511回繰り返し	00000009.jpg
010E	ImageDescription	置換	値	A * 512	'A'を512回繰り返し	00000010.jpg
010E	ImageDescription	置換	値	A * 1023	'A'を1023回繰り返し	00000011.jpg
010E	ImageDescription	置換	値	A * 1024	'A'を1024回繰り返し	00000012.jpg
010E	ImageDescription	置換	値	A * 2047	'A'を2047回繰り返し	00000013.jpg
010E	ImageDescription	置換	値	A * 2048	'A'を2048回繰り返し	00000014.jpg
010E	ImageDescription	置換	値	A * 4096	'A'を4096回繰り返し	00000015.jpg
010E	ImageDescription	置換	値	A * 4097	'A'を4097回繰り返し	00000016.jpg
010E	ImageDescription	置換	値	A * 5000	'A'を5000回繰り返し	00000017.jpg
010E	ImageDescription	置換	値	A * 10000	'A'を10000回繰り返し	00000018.jpg
010E	ImageDescription	置換	値	A * 20000	'A'を20000回繰り返し	00000019.jpg
010E	ImageDescription	置換	値	A * 32762	'A'を32762回繰り返し	00000020.jpg
010E	ImageDescription	置換	値	A * 32763	'A'を32763回繰り返し	00000021.jpg
010E	ImageDescription	置換	値	A * 32764	'A'を32764回繰り返し	00000022.jpg
010E	ImageDescription	置換	値	A * 32765	'A'を32765回繰り返し	00000023.jpg
010E	ImageDescription	置換	値	A * 32766	'A'を32766回繰り返し	00000024.jpg
010E	ImageDescription	置換	値	A * 32767	'A'を32767回繰り返し	00000025.jpg

図 11 テストデータ一覧

### 3.3 アンインストール

- 3.1 でインストールしたフォルダ(例 C:\Yipa\YiFuzzMaker など)内の RegDel.bat を起動します。
- インストールしたフォルダごと削除します。

## 4 使い方：製品のテストに使うテストデータを作る

本章では、製品のテストに使うテストデータを作るために用意する JPEG ファイルと、テストデータ生成ルールについて説明します。

本章を読み進めるには、JPEG ファイルと Exif タグに関する知識が必要です。これらの知識については、付録 A 「Exif タグと JPEG ファイルの基礎知識」をご参照ください。

### 4.1 JPEG ファイルの準備

利用者は、対象製品に実施するテストに合わせた JPEG ファイルを準備してください。

Exif2.3 に準拠して、Exif タグと SOFO セグメント構造を持つ JPEG ファイルが必要です。

### 4.2 テストデータ生成ルールの作成

利用者は、対象製品に実施するテストにあわせて、テストデータ生成ルールを準備してください。テストデータ生成ルールは、テストデータ生成ルールを記述した「テストデータ生成ルールファイル」と、テストデータ生成ルールファイルの一覧を記述した、「テストデータ生成ルールリスト定義ファイル」からなります。

まずテストデータ生成ルールファイルから作ります。Exif タグに「どの様なテスト値を」、「どれぐらい」、「どこに」、「どうやって」設定するか検討し、その設定をテストデータ生成ルールファイルに記述します。テストデータ生成ルールファイルは必要に応じて<sup>4</sup>、複数作成することもできます。

テストデータ生成ルールファイルを作成したら、それらのファイルのファイルパスをテストデータ生成ルールリスト定義ファイルに記述します。このように作成したテストデータ生成ルールリスト定義ファイルを iFuzzMaker で使うことで、テストに応じたテスト値を設定した JPEG ファイルを生成できます。

テストデータ生成ルールの作成手順は、下記の (1) から (6) となります。(1) から (5) までが「テストデータ生成ルールファイル」の作成手順で、(6) が「テストデータ生成ルールリスト定義ファイル」の作成手順となります。本節の手順では具体的な例を取り上げていないため、適宜サンプルのテストルール生成ファイル (.¥TestRule¥sample-TestRule1.txt など) を参考にしながら読み進めてください。

- ☞ (1) データ形式と値の設定（どの様なテスト値を）
- ☞ (2) 繰返し数の設定（どれぐらい）
- ☞ (3) 変更箇所の設定（どこに）
- ☞ (4) 書換モードの設定（どうやって）
- ☞ (5) その他の設定
- ☞ (6) ルールリストの設定

<sup>4</sup> テスト値の分類に応じてファイルを分ける場合などを想定

テストデータ生成ルールファイルは、表 10 の要素で構成されています。「テストデータ生成ルールファイル」は ANSI 文字コードのタブ区切り（0x09）のテキストファイルです。このファイルでは、一行（改行コードは 0x0D 0x0A）につき、ひとつのルールを記述します。手順（1）から（5）では、この表 10 の要素を一つずつ埋めていく形となります。手順（1）から（5）で、「表 10 の項番●」という記述があった場合、表 10 の該当する項番に値を設定するものとお考えください。

表 10 テストデータ生成ルールファイルの設定項目と設定値

項目番号	項目	説明	設定値
1	表示・非表示	テストデータ生成ルール選択画面への表示・非表示	0:非表示 1:表示
2	選択・未選択	テストデータ生成ルール選択画面に表示時の初期選択状態	0:未選択 1:選択
3	ルール名	表示用の名称	
4	データ形式	テスト値のデータ形式	0:テキスト 1:10進数[8bit] 2:10進数[16bit]（インテル形式 リトルエンディアン） 3:10進数[16bit]（モトローラ形式 ビッグエンディアン） 4:10進数[32bit]（インテル形式 リトルエンディアン） 5:10進数[32bit]（モトローラ形式 ビッグエンディアン） 6:16進ダンプ 7:ファイル(バイナリ)
5	値	テスト値の元となる値	データ形式に応じた値を設定
6	繰返し数	値を繰り返し設定する回数	0:領域分 数値:固定値
7	書換モード	テスト値の書換モード	0:置換 1:上書き 2:挿入
8	変更箇所	JPEG ファイル内のテスト値の変更箇所	1:タグ 2:タイプ 3:カウント 4:値 5:オフセット 6:セグメント要素 7:ファイル位置指定（ファイル内の任意の位置）
9	変更箇所指定	変更箇所の指定方法を設定	0:なし 1:タグ 2:タイプ 3:セグメント要素 4:ファイル位置
10	対象変更箇所	変更箇所指定が0の場合は空白 変更箇所指定が1:タグ 2:タイプ 3:セグメント要素 4:ファイル位置のみ設定	タグ:16進 タイプ:10進 セグメント要素:テキスト ファイル位置:10進（先頭からのバイト数、-1はファイル末尾）
11	説明	テスト値の説明	

### (1) データ形式と値の設定（どの様なテスト値を）

「データ形式と値の設定」はテストデータ生成ルールファイルの「データ形式（表 10 の項番 4）」と「値（表 10 の項番 5）」に設定します。iFuzzMaker で使用できるテスト値のデータ形式は、表 11 のように大きく 4 種類あります。

表 11 テスト値のデータ形式

形式	説明
テキスト	ANSI 文字コードのテスト値
数値	8、16、32 ビットの型のサイズと、リトルエンディアン、ビッグエンディアンのバイトオーダーを組み合わせでできるテスト値
ダンプ	16 進ダンプ値を設定するテスト値
ファイル	ファイルの内容を設定するテスト値、ファイルにはどのような値を設定してもよい

「A」をそれぞれの形式で設定する場合について説明します。

- テキスト形式の場合  
テキスト形式で設定する場合は文字「A」を値として設定します。
- 数値形式の場合  
数値形式で設定する場合は「A」の文字コード（10 進数）[65] を値として設定します。
- ダンプ形式の場合  
ダンプ形式で設定する場合は「A」の文字コード（16 進ダンプ）[41] を値として設定します。
- ファイル形式の場合  
ファイル形式で設定する場合は、ファイルの内容が文字「A(文字コード 10 進[65]:16 進[41])」となっているファイル（例えば.¥A.bin）を値として設定します。

これらの設定例を表 12 にまとめます。

表 12 データ形式と値の設定例

形式	データ形式（項番 4）	値（項番 5）
テキスト	0: テキスト	A
数値	1: 10 進数[8bit]	65
ダンプ	6: 16 進ダンプ	41
ファイル	7: ファイル(バイナリ)	ファイルパス (.¥A.bin)

いずれの設定の場合も、生成されるテスト値は全て同じです。このことから、同じテスト値を生成する場合でも、設定方法が複数あることがわかります。どの形式でどのような値を設定するかは、iFuzzMaker の利用者が自由に設定できます。

## (2) 繰り返し数の設定（どれぐらい）

「繰り返し数の設定」はテストデータ生成ルールファイルの「繰り返し数（表 10 の項番 6）」に設定します。iFuzzMaker は、「(表 10 の項番 5) 値を指定回数繰り返したものをテスト値にする」ことが可能です。例えば、「A」という値を「100」回繰り返してテスト値とするなどです。この場合、テスト値には「100」個分の「A」が生成されます。このようなテスト値を生成するような設定は複数あります。たとえば以下の設定で生成されるテスト値は全て同じテスト値になります。

- 値「A」を 100 回繰り返す
- 値「AA」を 50 回繰り返す
- 値「AAA…（100 文字分値に設定）…A」を 1 回繰り返す

また、変更箇所（変更箇所については（3）で説明します）に指定した領域と同じサイズ分繰り返すといった設定も可能です。たとえば、変更箇所として設定した領域が 4 バイトある場合、「A」を 4 バイト分繰り返したテスト値が生成されます。

このように、どのような値を何回繰り返してテスト値とするかは、iFuzzMaker の利用者が自由に設定できます。これらの設定例を表 13 にまとめます。

表 13 繰り返し数の設定例

設定	値（項番 5）	繰り返し数（項番 6）
値「A」を 100 回繰り返す	A	100
値「AA」を 50 回繰り返す	AA	50
値「AAA…（100 文字分値に設定）…A」を 1 回繰り返す	AAA…（100 文字分値）…A	1
値「A」を 4 バイトの変更箇所の領域分繰り返す	A	0

## (3) 変更箇所の設定（どこに）

「変更箇所の設定」はテストデータ生成ルールファイルの「変更箇所（表 10 の項番 8）」に設定します。iFuzzMaker は、を変更箇所として JPEG ファイル内の「Exif タグ」、「セグメント要素」、「任意のファイル位置」を指定できます。なお、JPEG ファイルの構造や Exif タグの構造については付録 A を参照してください。

- Exif タグを変更箇所とする場合

Exif タグを変更箇所とする場合はタグ、タイプ、カウント、値、オフセットのいずれかを変更箇所として指定します。タグの変更箇所は図 12 の中の「①タグ」です。同じようにタイプは「②タイプ」、カウントは「③カウント」、値は「④値/オフセット」、オフセットは「④値/オフセット」

が JPEG ファイル内の変更箇所です。ただし、値を指定した場合、元の Exif タグの値のサイズが 4 バイトを超える場合は、自動的に「⑤エントリの値」が変更箇所になります。

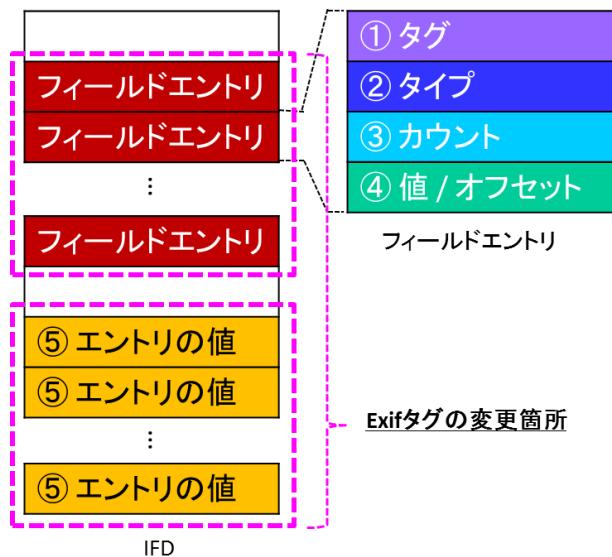


図 12 Exif タグの変更箇所

Exif タグを変更箇所とする場合にテストデータ生成ルールファイルで設定できる変更箇所の設定例を表 14 にまとめます。

表 14 Exif タグの変更箇所の設定例

設定	変更箇所（項目番号）
Exif タグの「タグ」が対象	1:タグ
Exif タグの「タイプ」が対象	2:タイプ
Exif タグの「カウント」が対象	3:カウント
Exif タグの「値」が対象	4:値
Exif タグの「オフセット」が対象	5:オフセット

iFuzzMaker は Exif タグを変更箇所に設定した場合、基となる JPEG ファイルに含まれるすべての Exif タグのテストデータを生成します。例えば、基となる JPEG ファイルに「タイトル」、「撮影日時」、「大きさ」といった 3 つの Exif タグが含まれている場合に、例にあげたルールを適用すると、図 13 のように 3 つのテストデータが生成されます。

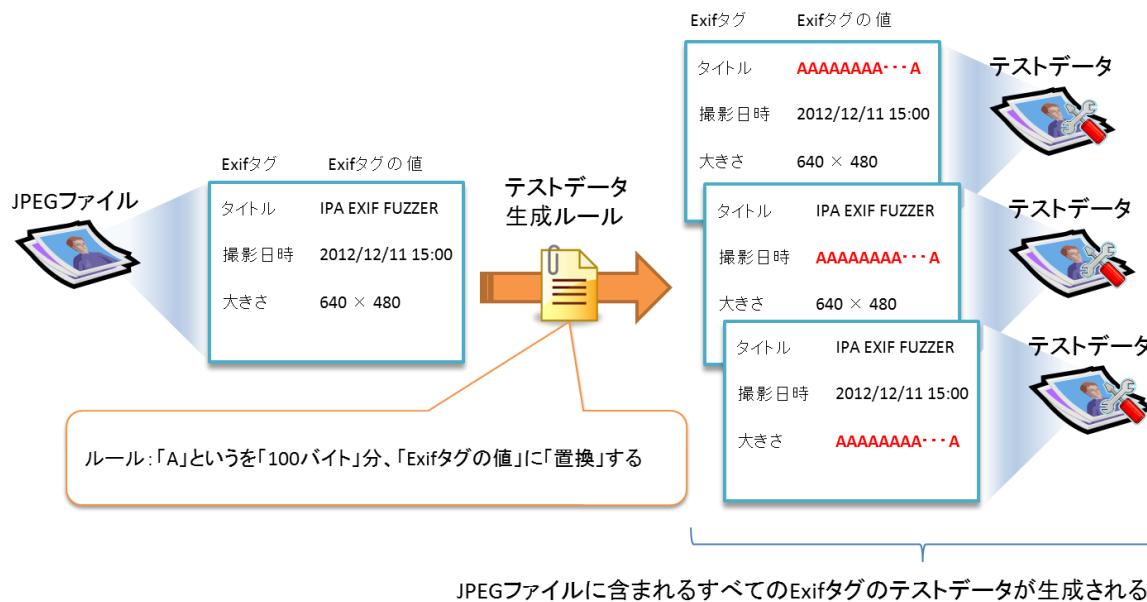


図 13 Exif タグを変更箇所とした場合のテストデータ生成例

iFuzzMaker は Exif タグを変更箇所に設定した、特定の Exif タグやタイプのみを変更箇所として設定することも可能です。この設定は、「変更箇所指定（表 10 の項番 9）」と「対象変更箇所（表 10 の項番 10）」で設定します。

- 指定しない場合  
変更箇所指定を「なし」に設定します。
- タグ指定で Exif タグのタイトルタグに設定する場合  
変更箇所指定をタグに設定し、対象変更箇所にタイトルタグの ID 「010E」 を設定します。
- タイプ指定で RATIONAL に設定する場合  
変更箇所指定をタイプに設定し、対象変更箇所に RATIONAL のタイプ「5」を設定します。

表 15 にこれらの設定をまとめます。

表 15 変更箇所指定の設定例

設定	変更箇所指定（項番 9）	対象変更箇所（項番 10）
指定しない場合	0:なし	(空白)
Exif タグのタイトルタグに設定する 場合	1:タグ	010E (Exif タグのタイトルタ グの ID)
RATIONAL に設定する場合	2:タイプ	5 (RATIONAL のタイプ)

#### ● セグメント要素を変更箇所とする場合

セグメント要素を変更箇所とする場合は、セグメント構造情報ファイル（表 28 を参照）でセグ

メントがあらかじめ設定されている必要があります(iFuzzMaker に付属しているセグメント構造情報ファイルには、SOF0 セグメントのみが設定されています、セグメントの追加方法は 5.2 を参照してください)。JPEG ファイル内の変更箇所は図 14 の「⑥セグメント」です。

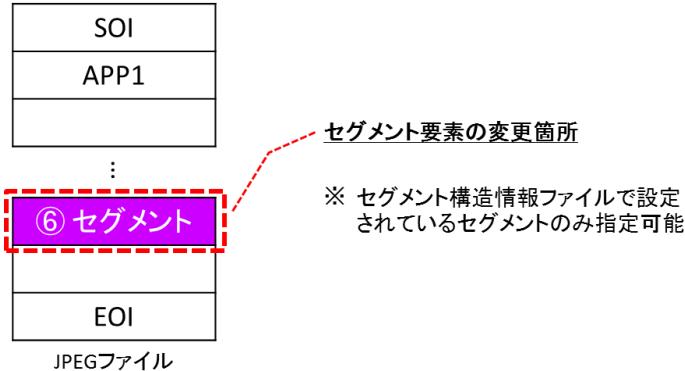


図 14 セグメント要素の変更箇所

セグメント要素を変更箇所とする場合にテストデータ生成ルールファイルで設定できる変更箇所の設定例を表 16 にまとめます。

表 16 セグメント要素の変更箇所の設定例

設定	変更箇所（項番 8）
セグメント内の要素が対象	6:セグメント要素

iFuzzMaker はセグメントの要素を変更箇所に設定した場合、Exif タグを変更箇所として設定した場合と同様に、基となる JPEG ファイルに含まれるすべてのセグメント内の要素のテストデータを生成します。

また、iFuzzMaker はセグメント要素を箇所に設定した、特定のセグメント要素のみを変更箇所として設定することも可能です。この設定は、「変更箇所指定（表 10 の項番 9）」と「対象変更箇所（表 10 の項番 10）」で設定します。

- 指定しない場合  
変更箇所指定を「なし」に設定します。
- セグメント要素指定で SOF0 セグメントの Hi/Vi に設定する場合  
変更箇所指定をセグメント要素に設定し、対象変更箇所にセグメント構造情報ファイルの項目 ID 「SOF0.Hi/Vi」 を設定します。

表 17 にこれらの設定をまとめます。

表 17 変更箇所指定の設定例

設定	変更箇所指定（項番 9）	対象変更箇所（項番 10）
指定しない場合	0:なし	(空白)
SOF0 セグメントの Hi/Vi に設定する場合	3:セグメント要素	SOF0.Hi/Vi (セグメント構造情報ファイルの項目 ID)

- 任意のファイル位置を変更箇所とする場合

任意のファイル位置を変更箇所とする場合は JPEG ファイルの先頭からの位置（バイト単位）を変更箇所として指定します。JPEG ファイル内の変更箇所は図 15 の「⑦ファイル内の任意の位置」です。

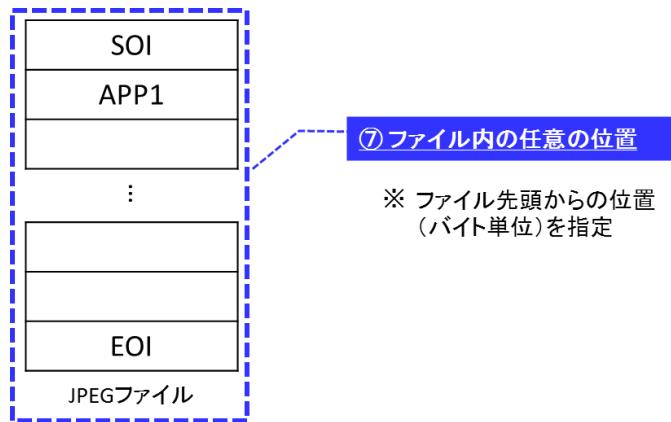


図 15 任意のファイル位置の変更箇所

任意のファイル位置を変更箇所とする場合にテストデータ生成ルールファイルで設定できる変更箇所の設定例を表 18 にまとめます。

表 18 任意のファイル位置の変更箇所の設定例

設定	変更箇所（項番 8）
任意のファイル位置が対象	7:ファイル位置指定

変更箇所が任意のファイル位置の場合は、「変更箇所指定（表 10 の項番 9）」と「対象変更箇所（表 10 の項番 10）」の設定は必須です。

- ファイル位置指定で先頭から 10 バイト目に設定する場合

変更箇所指定をファイル位置に設定し、対象変更箇所に先頭からのバイト数「10」を設定します。

- ファイル位置指定でファイル末尾に設定する場合

変更箇所指定をファイル位置に設定し、対象変更箇所に「-1」を設定します。

表 19 これらの設定をまとめます。

表 19 変更箇所指定の設定例

設定	変更箇所指定（項番 9）	対象変更箇所（項番 10）
ファイル先頭から 10 バイト目に設定する場合	4: ファイル位置	10（先頭からのバイト数）
ファイル位置指定でファイル末尾に設定する場合	4: ファイル位置	-1（-1 を設定した場合はファイル末尾として扱う）

#### （4） 書換モードの設定（どうやって）

「書換モードの設定」はテストデータ生成ルールファイルの「書換モード（表 10 の項番 7）」に設定します。

iFuzzMaker は生成したテスト値と変更箇所を「①置換」、「②上書」、「③挿入」のいずれかのモードで置き換えます。図 16 のような変更箇所のサイズ（4 バイト）に対して、テスト値のサイズが「ア. 小さい（1 バイト）」場合、「イ. 同じ（4 バイト）」場合、「ウ. 大きい（5 バイト）」場合を例に、テスト値の生成イメージを説明します。

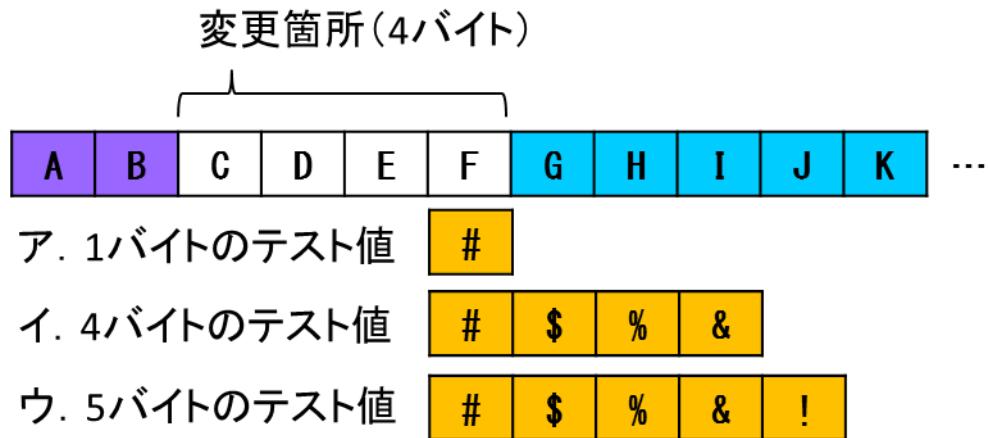


図 16 変更箇所のイメージ

- 置換

書換モードが「置換」の場合、図 17 のように生成したテスト値で変更箇所が置換されます。

ア	A	B	#	G	H	I	J	K	L	M	N	...
イ	A	B	#	\$	%	&	G	H	I	J	K	...
ウ	A	B	#	\$	%	&	!	G	H	I	J	...

図 17 書換モード（置換）

- 上書き

書換モードが「上書き」の場合、図 18 のように生成したテスト値で変更箇所が上書きされます。

テスト値のサイズがファイル末尾を超える場合、超えた分だけファイルは拡張されます。

ア	A	B	#	D	E	F	G	H	I	J	K	...
イ	A	B	#	\$	%	&	G	H	I	J	K	...
ウ	A	B	#	\$	%	&	!	H	I	J	K	...

図 18 書換モード（上書き）

- 挿入

書換モードが「挿入」の場合、図 19 のように生成したテスト値が変更箇所の前に挿入されます。

ア	A	B	#	C	D	E	F	G	H	I	J	...
イ	A	B	#	\$	%	&	C	D	E	F	G	...
ウ	A	B	#	\$	%	&	!	C	D	E	F	...

図 19 書換モード（挿入）

表 20 これらの設定例をまとめます。

表 20 書換モードの設定例

設定		書換モード（項目番号 7）
置換	0: 置換	
上書き	1: 上書き	
挿入	2: カウント	

## (5) その他の設定

最後にテストデータ生成ルールファイルの残りの項目「表示・非表示（表 10 の項番 1）」、「選択・未選択（表 10 の項番 2）」、「ルール名（表 10 の項番 3）」、「説明（表 10 の項番 11）」を設定します。

「表示・非表示」はテストデータ生成ルール選択画面にテストデータ生成ルールを表示するか・しないかを設定します。「選択・未選択」はテストデータ生成ルール選択画面にテストデータ生成ルールが表示されたとき、選択状態であるか・ないかを設定します。「ルール名」はテストデータ生成ルール選択画面で表示される「ルール名」を、「説明」はテストデータ生成ルール選択画面などで表示される「説明」をそれぞれ設定します。

表 21 テストデータ生成ルールファイルの設定例をまとめます。

表 21 テストデータ生成ルールファイルの設定例

項目番号	項目	設定値
1	表示・非表示	1:表示
2	選択・未選択	1:選択
3	ルール名	A * 100
4	データ形式	0:テキスト
5	値	A
6	繰返し数	100
7	書換モード	0:置換
8	変更箇所	4:値
9	変更箇所指定	0:なし
10	対象変更箇所	(空白)
11	説明	'A' を 100 回繰り返し

テストデータ生成ルールの設定が終わったら、テストデータ生成ルールファイルを任意の名前で保存します（サンプルでは.¥TestRule¥sample\TestRule1.txt など）。なお iFuzzMaker では複数のテストデータ生成ルールファイルを使用できます。次節では複数使用できるよう、テストデータ生成ルールリストへの追加方法を説明します。

## (6) ルールリストの設定

利用者はテストデータ生成ルールファイルを作成したら、テストデータ生成ルールリスト定義ファイル（表 22）に、作成したテストデータ生成ルールファイルの画面への「表示方法」と「テストデータ生成ルールファイルのパス」を記述します。

テストデータ生成ルールのリスト定義ファイルは、テストデータ生成ルールファイルと同様に ANSI 文字コードのタブ区切り（0x09）のテキストファイルです。一行（改行コードは 0x0D 0x0A）につき、ひとつのテストデータ生成ルールリストを設定します。

表 22 テストデータ生成ルールリスト定義ファイル

名称	説明	設定値
表示・非表示	テストデータ生成ルール選択画面への表示・非表示	0:非表示 1:表示
表示名	テストデータ生成ルールの表示名	
ファイル名	テストデータ生成ルールファイルのパス（絶対パス、または iFuzzMaker.exe があるフォルダからの相対パスでも指定できます）	

テストデータ生成ルールリスト定義ファイルには複数のテストデータ生成ルールファイルを追加できます。表 23 はテストデータ生成ルールリスト定義ファイルの設定例です。

表 23 テストデータ生成ルールリスト定義ファイルの設定例

名称	設定値
表示・非表示	1:表示
表示名	Stack/Heap Overflows
ファイル名	.¥TestRule¥list¥sample-TestRule1.txt

## 5 一歩進んだ使い方：Exif 仕様にない Exif タグもテストしたい

本章では iFuzzMaker のカスタマイズ方法として、Exif 仕様にない独自で扱う Exif タグの追加と、セグメントの追加方法について説明します。

本章を読み進めるには、JPEG ファイルと Exif タグに関する知識が必要です。これらの知識については、付録 A 「Exif タグと JPEG ファイルの基礎知識」をご参照ください。

### 5.1 メーカー独自の Exif タグをテスト対象に追加する

メーカー独自に実装しているタグも、タグ情報ファイルに追記することで、iFuzzMaker で扱うことが可能になります。Exif タグの追加はタグ情報ファイル（表 24）に Exif タグを追記します。

タグ情報ファイルは、ANSI 文字コードのタブ区切り（0x09）のテキストファイルです。一行（改行コードは 0x0D 0x0A）につき、ひとつの Exif タグを記述します。

表 24 タグ情報ファイル

項目番号	名称	説明	備考
1	タグ(HEX)	タグの ID (16 進数表記)	
2	タグ(NUM)	タグの ID (10 進数表記)	
3	タグ名	タグの名称	
4	表示名	タグの表示名	
5	タイプ	タイプ (空白可)	iFuzzMaker では未使用の項目
6	カウント	カウント (空白可)	iFuzzMaker では未使用の項目
7	デフォルト	デフォルトの設定値 (空白可)	画面表示のみに使用 “¥n” は画面表示時に改行コードに変換される
8	設定値	設定値の補足説明 (空白可)	画面表示のみに使用 “¥n” は画面表示時に改行コードに変換される
9	説明	タグの説明 (空白可)	画面表示のみに使用 “¥n” は画面表示時に改行コードに変換される

本節では、Windows 7 の JPEG ファイルのプロパティから設定できる「評価タグ」（図 20）を例に、iFuzzMaker へタグ情報を追加する手順を説明します。なお、説明で使用する JPEG ファイルは、サンプルの JPEG ファイル「IPA-SAMPLE.JPG」のファイルのプロパティエクスプローラからを開き、評価を「★★★★★」に設定して適用したファイルです。

iFuzzMaker でのタグの追加は以下の手順で説明します。

- ☞ (1) 追加前の確認
- ☞ (2) タグの追加
- ☞ (3) 追加後の確認

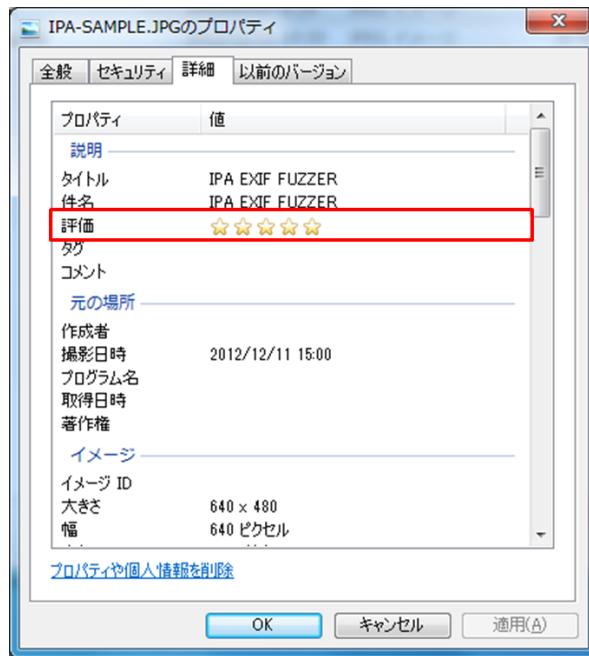


図 20 評価タグのついた JPEG ファイルのプロパティ

### (1) 追加前の確認

iFuzzMaker に含まれるタグ情報ファイルには評価タグは含まれていません。この状態で iFuzzMaker から「評価タグ」のある JPEG ファイルを開くと図 21 のように「Unknown」と表示されます。

The screenshot shows the iFuzzMaker application interface with the 'Segments/Tags' table. A tooltip points to the 'Rating' tag entry, which is labeled '評価タグ' and described as 'タグ情報ファイルにないタグのため、Unknownになっている'.

セグメント/タグ	オフセット	サイズ/エントリ数	マーカー/タグ	名称
SOI	0 (0x00000000)	2 (0x00000002)	FFD8	イメージの開始
APP1	2 (0x00000002)	8136 (0x00001FC8)	FFE1	タイプ1のアプリケーション
Primary	20 (0x00000014)	14 (0x0000000E)		0th IFD
ImageDescription	22 (0x00000016)	12 (0x0000000C)	010E	画像タイトル
Make	34 (0x00000022)	12 (0x0000000C)	010F	画像入力機器のメーカー名
Model	46 (0x0000002E)	12 (0x0000000C)	0110	画像入力機器のモデル名
Orientation	58 (0x0000003A)	12 (0x0000000C)	0112	画像方向
XResolution	70 (0x00000046)	12 (0x0000000C)	011A	画像の幅の解像度
YResolution	82 (0x00000052)	12 (0x0000000C)	011B	画像の高さの解像度
ResolutionUnit	94 (0x0000005E)	12 (0x0000000C)	0128	画像の幅と高さの解像度の単位
DateTime	106 (0x0000006A)	12 (0x0000000C)	0132	ファイル変更日時
YCbCrPositioning	118 (0x00000078)	12 (0x0000000C)	0213	画素構成
Unknown	130 (0x00000082)	12 (0x0000000C)	4746	
Unknown	142 (0x00000090)	12 (0x0000000C)	4749	
ExifIFDPointer	154 (0x0000009A)	12 (0x0000000C)	8769	Exif IFD ポイント
GPSInfoIFDPointer	166 (0x000000A6)	12 (0x0000000C)	8825	GPS IFD ポイント
Unknown	178 (0x000000B2)	12 (0x0000000C)	EA1C	
ExifIFD	2338 (0x00000922)	30 (0x0000001E)	8769	
ExposureTime	2340 (0x00000924)	12 (0x0000000C)	829A	
FNumber	2352 (0x00000930)	12 (0x0000000C)	829D	
PhotographicSensitivity	2364 (0x0000093C)	12 (0x0000000C)	8827	

図 21 評価タグが追加されていない iFuzzMaker

## (2) タグの追加

iFuzzMaker で Exif タグを追加するには、追加する Exif タグの ID やタグ名、どの IFD に含まれるタグかなどの情報が必要です。追記する「評価タグ」の情報を表 25 にまとめます。

表 25 評価タグの情報

名称	設定値
IFD	0th IFD
タグ(HEX)	4746
タグ(NUM)	18246
タグ名	Rating
表示名	評価
タイプ	SHORT
カウント	1
デフォルト	なし
設定値	1 = ★、2 = ★★、3 = ★★★、4 = ★★★★、5 = ★★★★★
説明	画像の評価

追記する Exif タグが、どの IFD に含まれるかで、追記するタグ情報ファイルが異なります。IFD と追記するタグ情報ファイルを表 26 に示します。

表 26 各 IFD に対応したタグ情報ファイル

IFD	タグ情報ファイル
0th IFD	.¥Data¥TIFFRev60.txt
1st IFD	.¥Data¥TIFFRev60.txt
ExifIFD	.¥Data¥ExifIFD.txt
GPSIFD	.¥Data¥GPSInfoIFD.txt
互換性 IFD	.¥Data¥Interoperability.txt

「評価タグ」の情報は「.¥Data¥TIFFRev60.txt」に追記して保存します。追記する内容例を表 27 に示します。保存が終われば、タグ情報の追加は完了です。iFuzzMaker が起動している場合は、iFuzzMaker を再起動してください。

表 27 追記する評価タグの内容例

項目番号	名称	設定値
1	タグ(HEX)	4746
2	タグ(NUM)	18246

項目番号	名称	設定値
3	タグ名	Rating
4	表示名	評価
5	タイプ	SHORT
6	カウント	1
7	デフォルト	なし
8	設定値	1 = ★¥n2 = ★★¥n3 = ★★★¥n4 = ★★★★¥n5 = ★★★★★¥n
9	説明	画像の評価

### (3) 追加後の確認

iFuzzMaker から「評価タグ」のある JPEG ファイルを開くと図 21 のように「評価タグ」が表示され、追加されていることが確認できます。

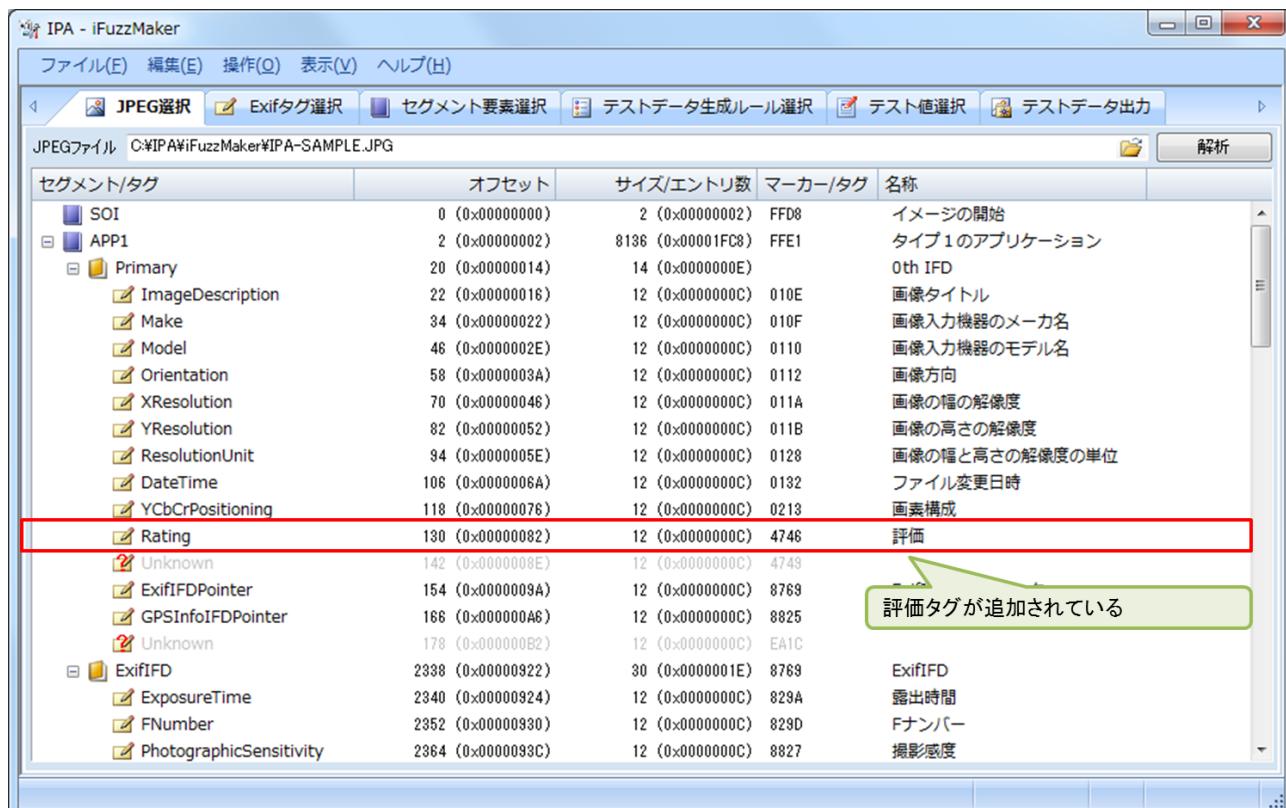


図 22 評価タグ追加後の JPEG 選択画面

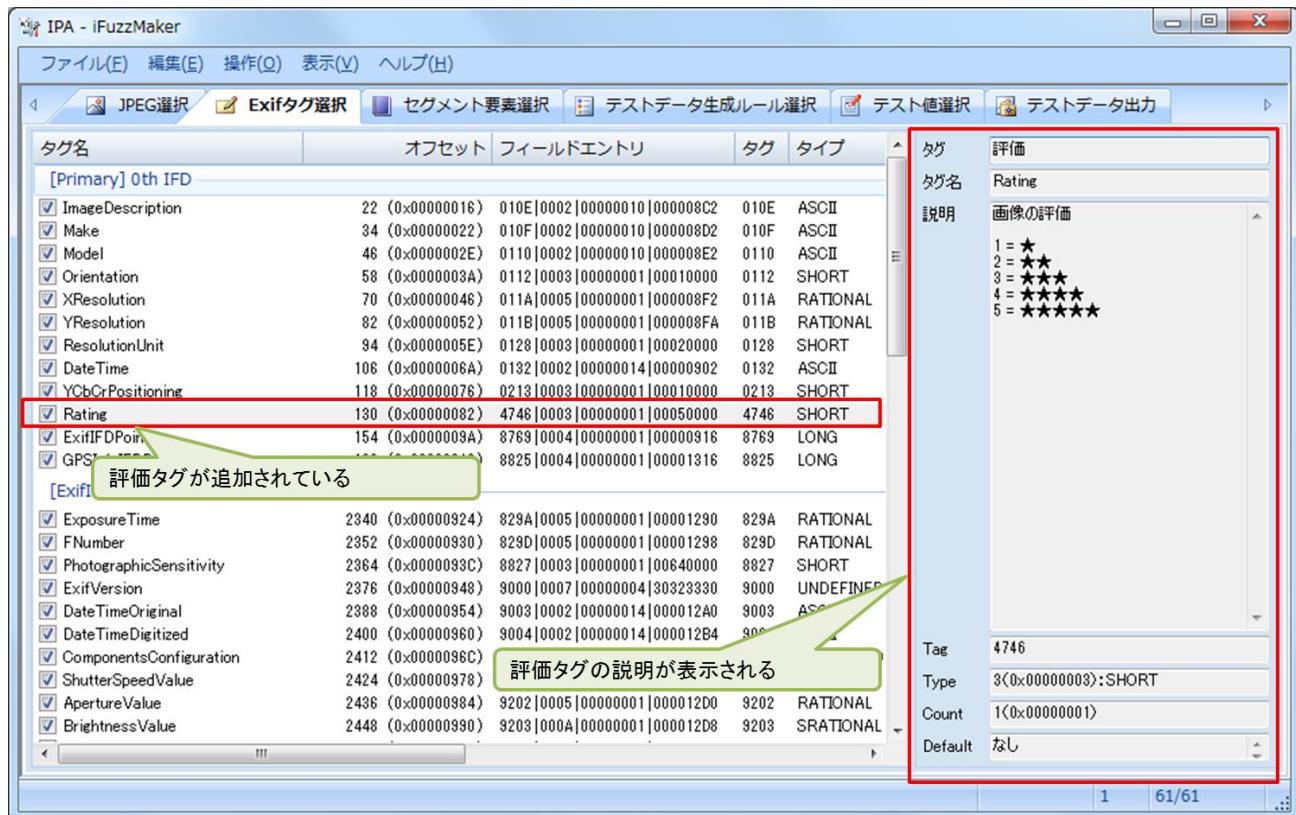


図 23 評価タグ追加後の Exif タグ選択画面

## 5.2 SOF0 以外のセグメントもテスト対象に追加する

SOF0 以外のセグメントも、セグメント構造情報ファイルにセグメント要素を追記することで、iFuzzMaker で扱うことが可能になります。セグメントの追加はセグメント構造情報ファイル（表 28）にセグメント要素を追記します。

セグメント構造情報ファイルは、ANSI 文字コードのタブ区切り（0x09）のテキストファイルです。一行（改行コードは 0x0D 0x0A）につき、ひとつのセグメント要素を記述します。

表 28 セグメント構造情報ファイル

項目番	名称	説明	設定値
1	項目 ID	セグメント情報ファイルで一意となるよう、セグメント要素に任意の値を設定	
2	項目名称	セグメント要素の名称	
3	説明	セグメント要素の説明	
4	サイズ	セグメント要素のデータサイズ（バイト数を設定）	
5	表示データ型	表示データの型	0:構造定義ファイル 1:8 ビットの数値型(BYTE) 2:8 ビットのキャラクタ型(ASCII) 3:16 ビットの数値型(SHORT) 4:32 ビットの数値型(LONG)
6	カウント項目 ID	情報の繰り返し数を表す数値を設定した項目 ID を設定、ない場合は空白	
7	セグメント構造情報ファイル	データ型が 0:構造定義ファイルのみ設定、それ以外は空白	

iFuzzMaker は次のような構造のセグメントを、セグメント構造情報ファイルに追加できます。

- A) 固定長のセグメント（例：SOI セグメント）
- B) 同じ構成の要素を繰り返す構造で、繰り返し回数が要素にあるセグメント（例：SOS セグメント）

セグメントの追加手順は「SOS セグメント（Start of scan segment）」を例に説明します。「SOS セグメント」の構造は図 24 のようになっています。

iFuzzMaker でのセグメントの追加は以下の手順でおこないます。

- ☞ (1) 構成要素部分のセグメント構造情報ファイルの作成
- ☞ (2) 残りの部分のセグメント構造情報ファイルの作成
- ☞ (3) セグメント情報ファイルへの追加
- ☞ (4) 追加後の確認

サイズ	項目	説明
2	Marker	SOSマーカー
2	Ls	セグメント長
1	Ns	構成要素の数
1	Csn	構成要素のID
1	Tdn/Tan	DC/AC構成要素のDHT識別子
⋮		
⋮		
1	Ss	スペクトル選択開始
1	Se	スペクトル選択終了
1	Ah/AI	スペクトル選択の上位／下位ビット

構成要素の数分繰り返し

図 24 SOS セグメントの構造<sup>5</sup>

「SOS」セグメントは [Csn] と [Tdn/Tan] をあわせた構成要素が [Ns] に設定されている構成要素の数分繰り返される構造になっています。このような構造のセグメントを iFuzzMaker で扱うには、セグメント構造情報ファイルを 2 つ作成します。例では図 25 のように「SOS.txt」と「SOS-Param.txt」とします。

<sup>5</sup> 以下のサイトを参考に IPA が作成

<http://www14.ocn.ne.jp/~setsuki/ext/segment/sos.htm>

<http://hp.vector.co.jp/authors/VA032610/JPEGFormat/marker/SOS.htm>

サイズ	項目	説明
2	Marker	SOSマーカー
2	Ls	セグメント長
1	Ns	構成要素の数
1	Csn	構成要素のID
1	Tdn/Tan	DC/AC構成要素のDHT識別子
⋮		
⋮		
1	Ss	スペクトル選択開始
1	Se	スペクトル選択終了
1	Ah/AI	スペクトル選択の上位／下位ビット

図 25 SOS セグメントのセグメント構造情報ファイル

### (1) 構成要素部分のセグメント構造情報ファイルの作成

「SOS セグメント」の中で、繰り返される構成要素部分のセグメント構造情報ファイルを作成します。項目 ID には iFuzzMaker で扱う Exif タグの ID や、セグメントの項目 ID と重複しない任意の ID を設定します（例では SOS.Csn など）。表示データ型には iFuzzMaker のセグメント要素選択画面でデータ値として表示する際のデータ型を設定します。「41 42 43 44」といった 4 バイトのデータの場合の表示例を表 29 に示します。

表 29 データ型ごとのデータ値

名称	データ値
0:構造定義ファイル	—（後述）
1:8 ビットの数値型(BYTE)	41 42 43 44
2:8 ビットのキャラクタ型(ASCII)	A B C D
3:16 ビットの数値型(SHORT)	16961 17475
4:32 ビットの数値型(LONG)	1145258561

〔Can〕、〔Tdn/Tan〕はそれぞれ表 30 のように設定し、「SOS-Param.txt」として「.YData」フォルダに保存します。表 30 のタイトル行の数字は、表 28 の表の項番に対応しています。

表 30 構成要素部分の設定

1	2	3	4	5	6	7
SOS.Csn	Csn	構成要素の ID	1	1		
SOS.Tdn/Tan	Tdn/Tan	DC/AC 構成要素の DHT 識別子	1	1		

## (2) 残りの部分のセグメント構造情報ファイルの作成

構成要素の部分以外の設定は、最終的に表 31 のようになります。

表 31 SOS セグメントの設定

1	2	3	4	5	6	7
SOS. Marker	Marker	SOS マーカー	2	3		
SOS. Ls	Ls	セグメント長	2	3		
SOS. Ns	Ns	構成要素の数	1	1		
SOS. Param	Param	構成要素	0	0	SOS. Ns	.¥data¥SOS-Param.txt
SOS. Ss	Ss	スペクトル選択開始	1	1		
SOS. Se	Se	スペクトル選択終了	1	1		
SOS. Ah/AI	Ah/AI	スペクトル選択の上位／下位ビット	1	1		

まず、構成要素の部分以外は [Ns] までを「SOS-Param.txt」と同じように各要素を設定します。構成要素の部分は任意の項目 ID 付与し（例では SOS.Pram）、項目番 6 のカウント ID に [Ns] に付与した ID（例では SOS.Ns）を設定します。項目番 7 のセグメント構造情報ファイルに（1）で保存したファイル名「SOS-Param.txt」を設定します。図 26 は SOS セグメントの設定イメージです。

残り部分も同じように設定していき「SOS.txt」として「.¥Data」フォルダに保存します。

サイズ	項目	説明
2	Marker	SOSマーカー
2	Ls	セグメント長
1	Ns	構成要素の数
1	Csn	構成要素のID
1	Tdn/Tan	DC/AC構成要素のDHT識別子
⋮		
⋮		
1	Ss	スペクトル選択開始
1	Se	スペクトル選択終了
1	Ah/AI	スペクトル選択の上位／下位ビット

図 26 SOS セグメントのセグメント構造情報ファイルの設定イメージ

### (3) セグメント情報ファイルへの追加

iFuzzMaker へ「SOS セグメント」を扱えるようにするには、セグメント情報ファイル(表 32)の「SOS セグメント」の設定を変更します。

セグメント情報ファイルも、ANSI 文字コードのタブ区切り (0x09) のテキストファイルです。一行(改行コードは 0x0D 0x0A)につき、ひとつのセグメントを記述します。

表 32 セグメント情報ファイル

項目番	名称	説明	設定値
1	マーカー	マーカー値 (16 進数表記)	
2	マーカー名	マーカーの名称	
3	セグメント	セグメント表示名	
4	説明	セグメントの説明	
5	レンジスフィールド	レンジスフィールドの有無	0:なし 1:あり
6	次セグメント画像フラグ	次のセグメント領域をイメージ画像とみなす フラグ (現在は SOS マーカーにのみ設定)	0:無効 1:有効
7	セグメント解析フラグ	セグメント情報解析の有効・無効	0:無効 1:有効
8	セグメント構造情報ファイル	セグメント情報の構造定義ファイルのパス	

表 33 のようにセグメント情報ファイルの「SOS セグメント」の「項番 7 セグメント解析フラグ」を「1:有効」にし、「項番 8 セグメント構造情報ファイル」に(2)で作成した「¥Data¥SOS.txt」を追記して保存します。保存が終われば、セグメントの追加は完了です。iFuzzMaker が起動している場合は、iFuzzMaker を再起動してください。

表 33 セグメント情報ファイルの変更項目

項目番	名称	設定値
7	セグメント解析フラグ	1:有効
8	セグメント構造情報ファイル	.¥Data¥SOS. txt

## (4) 追加後の確認

iFuzzMaker から JPEG ファイルを開くと図 27 のように「SOS セグメント」が表示され、追加されていることが確認できます。

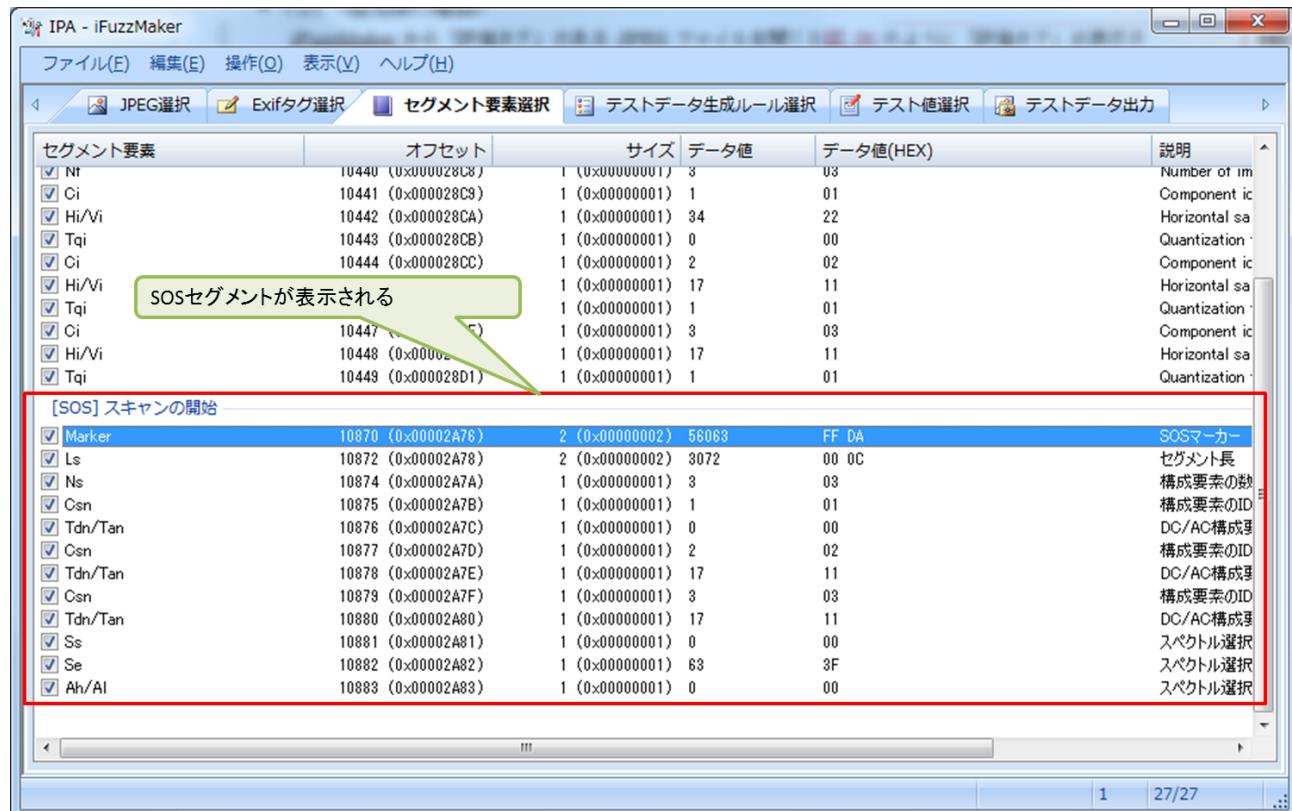


図 27 SOS セグメント追加後のセグメント要素選択画面

## 6 仕様

### 6.1 動作環境

IPA にて確認した iFuzzMaker の動作環境を表 34 に示します。同等の環境であれば iFuzzMaker は動作するものと考えます。

表 34 動作環境

項目	内容
OS	Windows XP SP3(32bit)
	Windows 7 SP1(32bit)
CPU	1GHz 以上の x86 互換プロセッサ
メモリ	1GB 以上の空きメモリ
HDD	1GB 以上の空き領域 <sup>6</sup>

### 6.2 コンパイル環境

IPA にて確認した iFuzzMaker のコンパイル環境を表 35 に示します。

表 35 コンパイル環境

項目	内容
OS	Windows XP SP3(32bit)
	Windows 7 SP1(32bit)
開発言語	Microsoft Visual Studio 2010 Visual C++ (MFC を使用)

<sup>6</sup> テストデータの量によってはさらに空き容量が必要になる場合があります。

### 6.3 ファイル構成

iFuzzMaker のファイル構成を表 36 に示します。

表 36 ファイル構成

ファイル	概要
<b>iFuzzMaker.exe</b>	iFuzzMaker 本体
<b>IFuzzMaker.config</b>	iFuzzMaker 設定ファイル
<b>IPA-SAMPLE.JPG</b>	サンプル JPEG ファイル
<b>RegDel.bat</b>	アンインストール用バッチ
<b>Data¥TagType.txt</b>	タグタイプ定義ファイル
<b>Data¥IFDList.txt</b>	IFD リスト定義ファイル
<b>Data¥Segments.txt</b>	セグメント情報ファイル
<b>Data¥SOF0.txt</b>	セグメント構造情報ファイル (SOF0 の構造情報)
<b>Data¥SOF0-Param.txt</b>	セグメント構造情報ファイル (SOF0 で繰り返される構成要素の構造情報)
<b>Data¥TIFFRev60.txt</b>	タグ情報ファイル (TIFF6.0 タグ)
<b>Data¥ExifIFD.txt</b>	タグ情報ファイル (Exif タグ)
<b>Data¥Interoperability.txt</b>	タグ情報ファイル (互換性タグ)
<b>Data¥GPSInfoIFD.txt</b>	タグ情報ファイル (GPS タグ)
<b>TestRule¥sample-TestRule-List.txt</b>	テストデータ生成ルールリスト定義ファイル
<b>TestRule¥list¥sample-TestRule1.txt</b>	テストデータ生成ルールファイル (サンプルテストデータ生成ルール : バッファオーバーフロー)
<b>TestRule¥list¥sample-TestRule2.txt</b>	テストデータ生成ルールファイル (サンプルテストデータ生成ルール : 整数オーバーフロー)
<b>TestRule¥list¥sample-TestRule3.txt</b>	テストデータ生成ルールファイル (サンプルテストデータ生成ルール : 書式文字列)

### 6.3.1 iFuzzMaker 設定ファイル

iFuzzMaker の設定ファイルです。主に iFuzzMaker で使用する定義ファイルを Windows の INI ファイル形式で設定します。ファイル名は固定 (iFuzzMaker.config) です。iFuzzMaker 設定ファイルは、通常お使いいただくうえでは変更の必要はありません。

表 37 iFuzzMaker 設定ファイル

セクション	キー	説明
[DATA]	SEGMENT	セグメント情報ファイルのパスを設定
	IFD	IFD 定義ファイルのパスを設定
	TAGTYPE	タグタイプ定義ファイルのパスを設定
[BROWS]	JPEGSELFOLDER	JPEG 選択画面のファイル選択初期フォルダを設定
	PATTERNSELFOLDER	テストデータ生成ルール選択画面のファイル選択初期フォルダを設定
	FUZZOUTPUTFOLDER	テストデータの出力フォルダパスを設定

### 6.3.2 IFD 定義ファイル

JPEG ファイルのセグメントを設定します。このファイルの設定値は、主に JPEG 選択画面のセグメントの名称や説明書き表示に反映されます。

表 38 IFD 定義ファイル

項目番号	名称	説明	設定値
1	IFD	将来的に、Exif 固有の IFD が増えた場合に拡張可能 IFD へのポインタの場合は、ポインタを示すタグの ID (16 進数表記)、その他、Unknown、Primary、Thumbnail は固定値を設定	Unknown : 不明な IFD Primary : 0th IFD Thumbnail : 1st IFD 8769 : ExifIFD 8825 : GPSInfoIFD A005 : InteroperabilityIFD
2	IFD 名	IFD の名称	
3	表示名	IFD の表示名	
4	順序		0 : 不明な IFD 1 : 0th IFD 2 : 1st IFD n : ExifIFD、GPSInfoIFD、InteroperabilityIFD
5	タグ情報ファイル		

### 6.3.3 タグタイプ定義ファイル

Exif で使われるタグのタイプを設定します。このファイルの設定値は、主に Exif 選択画面のタイプの表示に反映されます。

表 39 タグタイプ定義ファイル

項目番号	名称	説明	設定値
1	タイプ	EXIF の規格で定義されているタイプ (10 進数表記)	
2	サイズ	タイプのサイズ (バイト数)	
3	タイプ名	タイプ名	
4	説明	タグタイプの説明	

## 付録A Exif タグと JPEG ファイルの基礎知識

本付録では、iFuzzMaker のテストデータ生成ルール作成に必要となる、Exif タグについての基礎知識や、JPEG ファイルの構造などを解説します。

### (1) Exif とは

Exif (Exchangeable image file format) とは、写真に関する付帯情報（撮影日時やカメラの製造元などの）を含む画像ファイルフォーマットです。主にデジタルカメラや携帯電話などで撮影した画像ファイルに使われています。Exif を含む画像ファイルは「Exif 画像ファイル」とよばれています。

### (2) Exif タグとは

Exif タグとは Exif に含まれる、撮影日時やカメラの製造元などの画像に関する各付帯情報です。Windows であれば、JPEG ファイルのプロパティから各付帯情報を確認できます（図 28）。

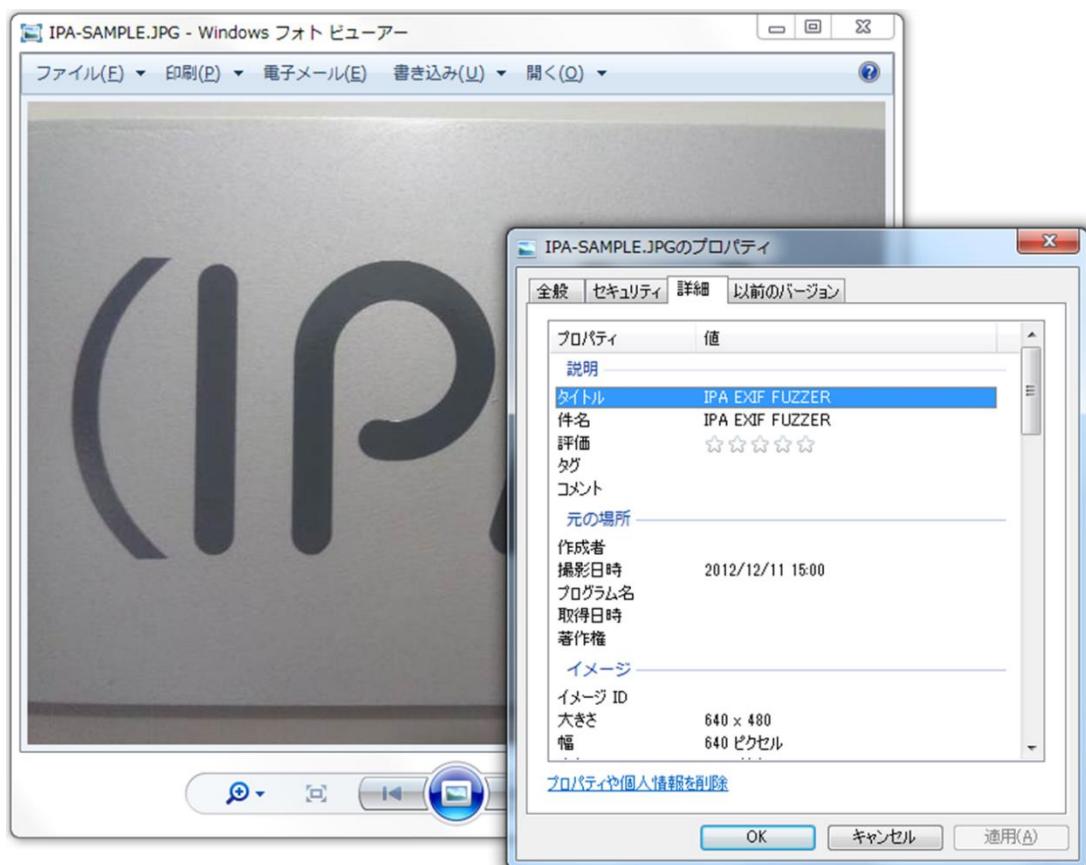


図 28 Exif タグの表示例

### (3) Exif 画像ファイルの種類

Exif 画像ファイルには「JPEG ファイル」と「TIFF ファイル」の 2 種類があります（表 40）。これらは画像データの圧縮形式に違いがあります。iFuzzMaker で扱うことのできる Exif 画像ファイルは「JPEG ファイル」のみです。

表 40 Exif 画像ファイルの圧縮形式

画像ファイル	圧縮形式	拡張子	iFuzzMaker での操作
JPEG ファイル	圧縮データ形式	.JPG .JPEG	○
TIFF ファイル	非圧縮データ形式	.TIF	×

### (4) JPEG ファイルの全体構造

図 29 は JPEG ファイルの全体構造です。次から JPEG ファイルの構造について説明します。

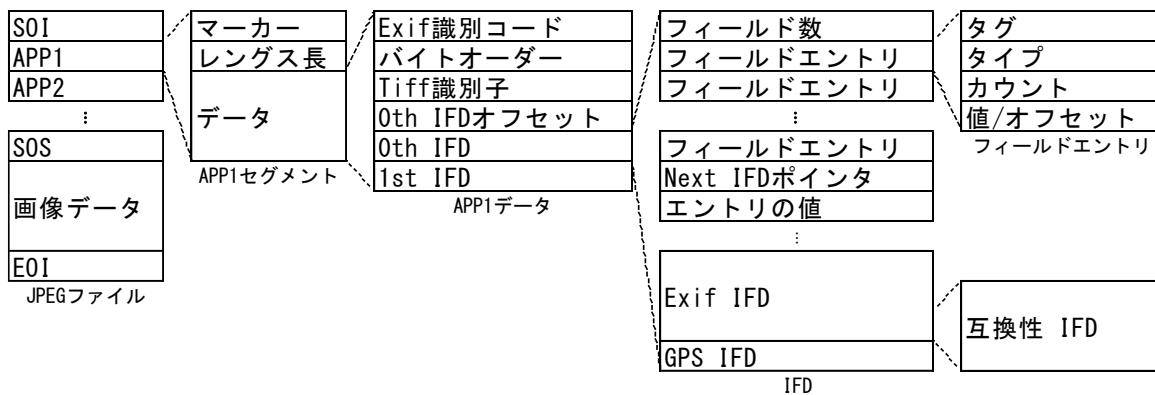


図 29 JPEG ファイルの全体構造

### (5) JPEG ファイルの構造

本節からは JPEG ファイルの内部構造について解説します。JPEG ファイルを構成する領域は、大きく分けて 5 つあります（図 30）。

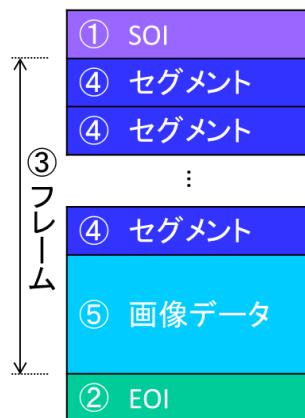


図 30 JPEG ファイルの構造

JPEG ファイルは先頭に「① SOI」、終端に「② EOI」という領域を持ちます。SOI と EOI の間に挟まれた領域を「③ フレーム」といいます。フレームは、複数の「④ セグメント」と「⑤ 画像データ」を持った構造になっています。JPEG ファイルを構成する領域を表 41 にまとめます。

表 41 JPEG ファイルの領域

領域	内容
① SOI	JPEG ファイルの先頭を示す
② EOI	JPEG ファイルの終端を示す
③ フレーム	SOI マーカーと EOI マーカーに挟まれた領域
④ セグメント	JPEG ファイルの様々な情報が格納される領域。どのようなデータが格納されているかはマーカーで識別する。
⑤ 画像データ	JPEG の主画像

## (6) セグメントの構造

セグメントは JPEG ファイルの様々な情報を格納する領域です。セグメントを構成する領域は 3 つあります（図 31）。

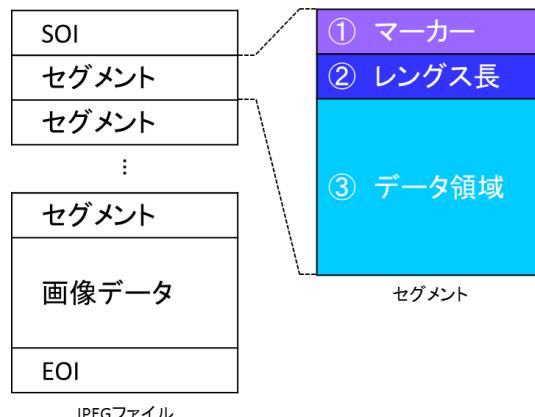


図 31 セグメントの構造

セグメントの種類を示す「① マーカー」は 1 バイト目が 0xFF で始まる 2 バイトの領域です。データの長さを示す「② レンジス長」も同じく 2 バイトの領域です。レンジス長には「N バイト（「③ データ領域」のサイズ） + 2 バイト」が格納されます。セグメントを構成する領域を表 42 にまとめます。

表 42 セグメントの領域

領域	サイズ	内容
① マーカー	2	セグメントの種類を示すマーカー値が格納される。 1バイト目はかならず「FF」でなければならない。
② レングス長	2	データの長さ（バイト数）を示す。n（データ領域のサイズ）+2が格納される。
③ データ領域	n	実際のセグメントデータが格納される領域。どのようなデータが格納されるかはセグメントにより異なる。

JPEG ファイルの先頭と終端にある SOI と EOI はマーカーのみを持った（レンジス長と、データ領域を持たない）特殊なセグメントです。表 43 に JPEG ファイルの主なセグメントを示します。画像の付帯情報が格納される Exif タグは、「タイプ 1 のアプリケーション (APP1 セグメント)」のデータ領域に含まれます。APP1 セグメントのデータ構造については(7)で解説します。

表 43 JPEG ファイルの主なセグメント

セグメント名	マーカー値	マーカー名	備考
イメージ開始	FFD8	SOI	マーカーのみ
タイプ 1 のアプリケーション	FFE1	APP1	Exif が格納されるセグメント、APP1 のデータ領域が Exif
量子化テーブル定義	FFDB	DQT	
ハフマン法テーブル定義	FFC4	DHT	
フレームタイプ 0 開始	FFC0	SOF0	JPEG ファイルの画像サイズなどが格納される
スキャン開始	FFDA	SOS	
イメージ終了	FFD9	EOI	マーカーのみ

## (7) APP1 セグメントのデータ構造

「タイプ 1 のアプリケーション (APP1)」セグメントのデータを構成する領域は 7 つあります(図 32)。

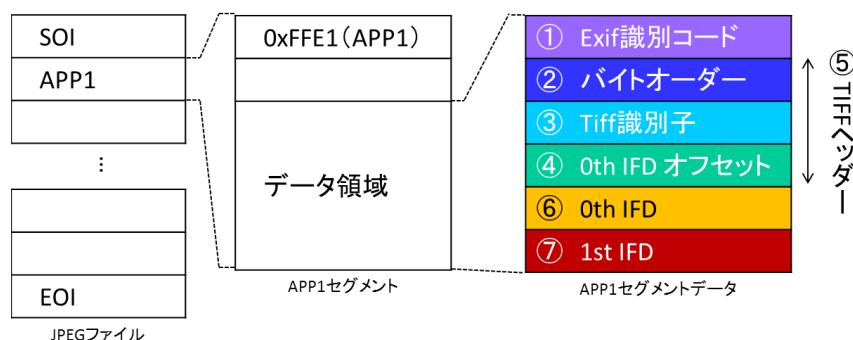


図 32 APP1 セグメントのデータ構造

APP1 セグメントのデータを構成する領域を表 44 にまとめます。

表 44 APP1 セグメントのデータ領域

領域	サイズ	内容
① Exif 識別子	6	ASCII 文字で「Exif NULL NULL」が格納される
② バイトオーダー	2	数値データのバイトオーダーを示す ASCII 文字が格納される。 「II」の場合はインテル形式（リトルエンディアン）、「MM」の場合はモトローラ形式（ビッグエンディアン）を示す。
③ Tiff 識別子	2	バイトオーダーに合わせて 0x002A が格納される。
④ 0th IFDへのオフセット	4	「⑥ 0th IFD」への「⑤ Tiff ヘッダー」からのオフセットを示す。通常は Tiff ヘッダーのすぐ後に 0th IFD があるため「0x0000 0008」が格納される
⑤ Tiff ヘッダー	8	「② バイトオーダー」、「③ Tiff 識別子」、「④ 0th IFDへのオフセット」を合わせて Tiff ヘッダーとよぶ。
⑥ 0th IFD	n	主画像に関するメタ情報を格納する IFD。
⑦ 1st IFD	n	サムネイル画像に関する情報を格納する IFD。

Exif で使われるバイトオーダーは「インテル形式」のリトルエンディアンと、モトローラ形式ビッグエンディアンの 2 種類があります。どちらを使用するかは「② バイトオーダー」にて設定します。2バイト以上の数値データは、指定されたバイトオーダーで格納されます（図 33）。

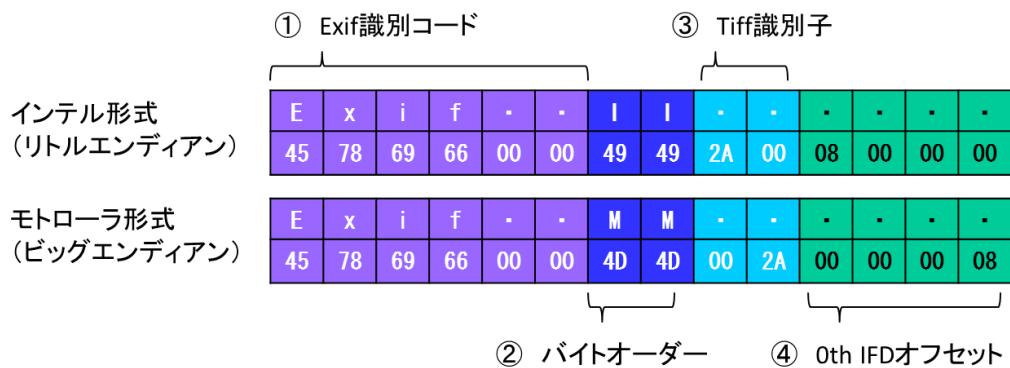


図 33 バイトオーダー

## (8) IFD の構造

IFD (Image File Directory) は画像の情報を示すタグを格納する領域です。JPEG で使われる IFD は全部で 5 種類あります（表 45）。IFD は Windows のディレクトリと似たような構造になっています。Exif のディレクトリ構成については(10)で解説します。

表 45 JPEG で使われる IFD

IFD	備考
0th IFD	主画像に関するメタ情報を格納する IFD
1st IFD	サムネイル画像に関する情報を格納する IFD
Exif IFD	Exif 固有の付属情報を格納する IFD、「0th IFD」の中に格納される
GPS IFD	GPS などの位置情報を格納する IFD、「0th IFD」の中に格納される
互換性 IFD	互換性を保証するために必要な情報を格納する IFD、「Exif IFD」の中に格納される

0th IFD を例に、IFD の構成を説明します。IFD を構成する領域は大きく 4 つあります（図 34）。

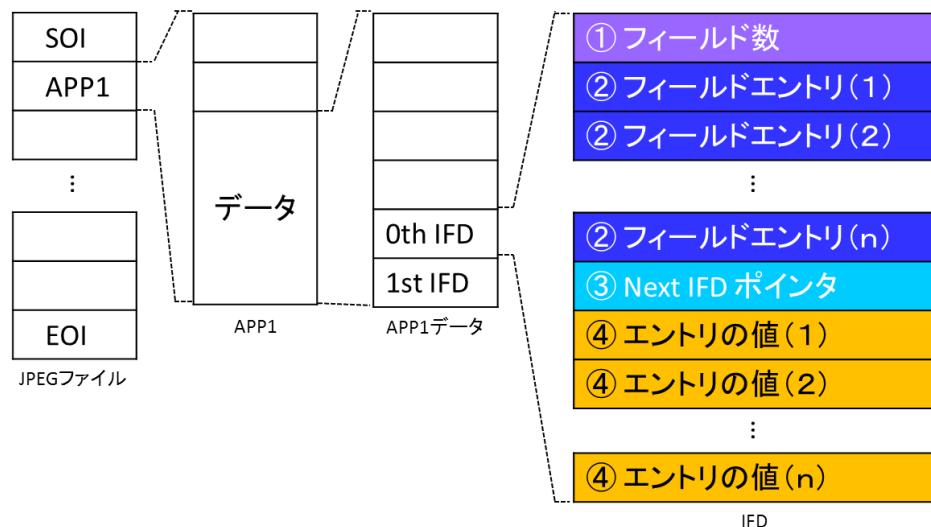


図 34 0th IFD の構造

IFD を構成する領域を表 46 にまとめます。

表 46 Exif の領域

領域	サイズ	内容
① フィールド数	2	「② フィールドエントリ」の数
② フィールドエントリ	12	タグ情報が格納される。
③ Next IFD ポインタ	2	0th IFD のみ使われ、1th IFD へのオフセットが格納される。その他の IFD では「0」が格納される。
④ エントリの値	n	「② フィールドエントリ」の値が 5 バイト以上の場合、この領域に値が格納される。

## (9) フィールドエントリの構造

フィールドエントリは画像に関するメタ情報を格納する領域です。フィールドエントリを構成する領域は4つあります。

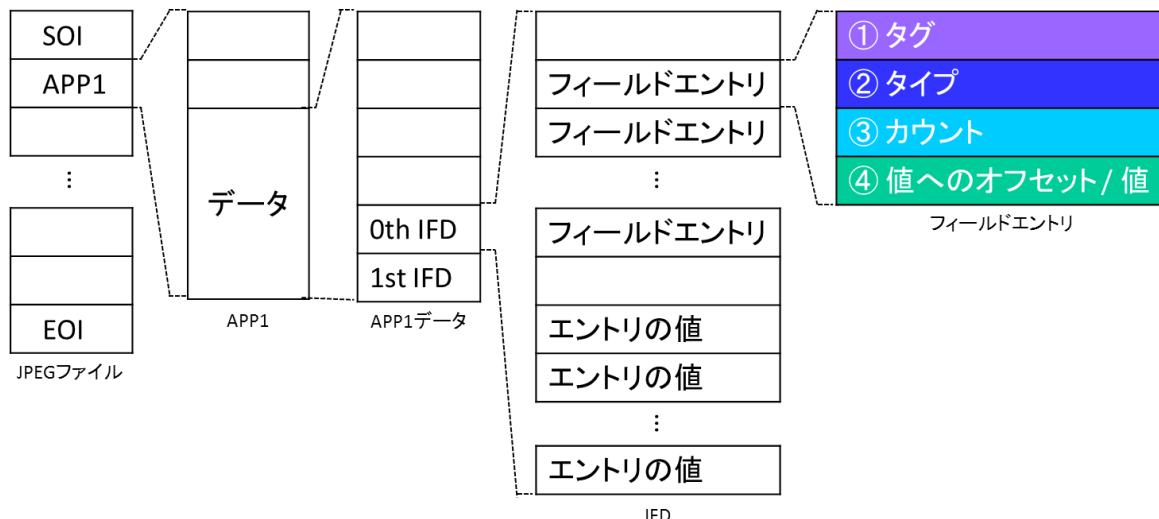


図 35 フィールドエントリの構造

フィールドエントリを構成する領域を表 47 にまとめます。

表 47 フィールドエントリの領域

領域	サイズ	内容
① タグ	2	フィールドを識別するための ID
② タイプ	2	値のデータ形式（型）を示す
③ カウント	4	値の個数
④ 値へのオフセット/値	4	値が 5 バイト以上のは、TIFF ヘッダーの先頭からのオフセットが格納される。値が 4 バイトに納まる場合は値そのものが格納される。値が 4 バイトより小さい場合は左詰めで格納される。

フィールドによって値は文字列であったり、数値や分数であったりとタイプが異なります。Exif で用いられるタイプを表 48 に示します。

表 48 Exif タイプ一覧

タイプ	設定値	内容
BYTE	1(0x01)	1 バイト (8 ビット) の符号なし整数
ASCII	2(0x02)	1 バイトの ASCII コード。最後のバイトは NULL (0x00) で終端する。ASCII のカウントは NULL も含めた値とする。
SHORT	3(0x03)	2 バイト (16 ビット) の符号なし整数
LONG	4(0x04)	4 バイト (32 ビット) の符号なし整数
RATIONAL	5(0x05)	LONG 値 2 つで分数を表す。最初の LONG は分子、2 個目の LONG は分母を表す。
UNDEFINED	7(0x07)	フィールドの定義によりどんな値をとってもよい 1 バイト (8 ビット) の値
SLONG	9(0x09)	4 バイト (32 ビット) の符号付き整数
SRATIONAL	10(0x0A)	SLONG 値 2 つで分数を表す。最初の SLONG は分子、2 個目の SLONG は分母を表す。

カウントはバイト数ではなく、値の個数です。例えば、タイプが SHORT の値がひとつあるタグでは、データのサイズは 2 バイトですが、カウントは 1 です。LONG の値がふたつあるタグでは、データのサイズは 8 バイトですが、カウントは 2 です。

エントリの値が 5 バイト以上の場合、IFD のエントリの値領域にデータを格納します。この場合、フィールドエントリの「値へのオフセット」には、実際の値が格納されている領域の、TIFF ヘッダーの先頭からのオフセットが格納されます。図 36 は値へのオフセットとエントリの値の参照のイメージ図です。

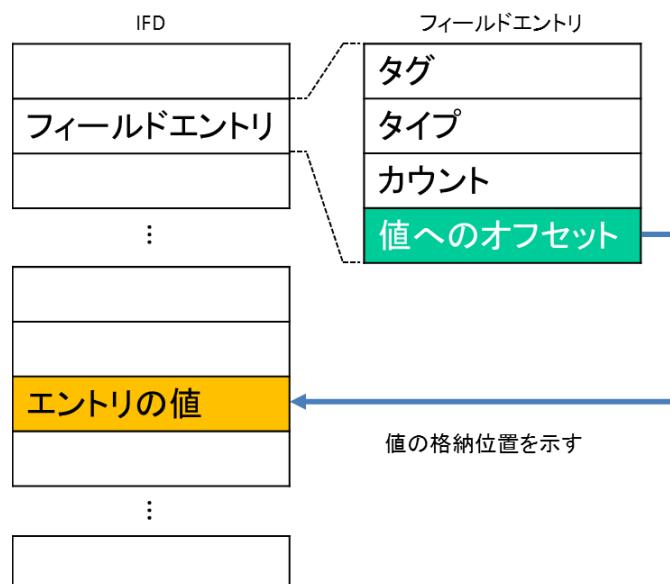


図 36 オフセットとエントリの値

エントリの値が4バイトより小さい場合は左詰めで格納されます。例えば、タイプが「SHORT」で値が「1」、バイトオーダーがビッグエンディアンの場合、値は「0x 00 01 00 00」となります(図37)。

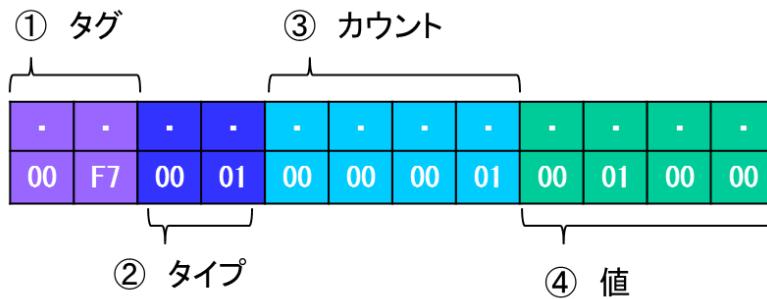


図37 4バイトより小さいエントリ値

#### (10) Exif のディレクトリ構成

Exif のディレクトリ構成は図38のような構成になっています。「0th IFD」と「1st IFD」はディレクトリ構成のルートに格納されています。「0th IFD」の子ノードに「Exif IFD」と「GPS IFD」が格納されています。さらに「Exif IFD」の子ノードに「互換性 IFD」が格納されます。

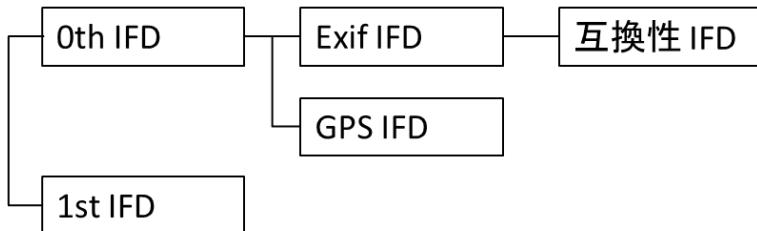


図38 Exif のディレクトリ構成

このディレクトリ構成なかで「Exif IFD」や「GPS IFD」が「0th IFD」のどこに格納されるか、「互換性 IFD」が「Exif IFD」のどこに格納されるかは、ポインタとよばれる特殊なフィールドエントリ(表49)でTiffヘッダーからのオフセットが定義されます。

表49 特殊なフィールドエントリ

タグ	名称	タイプ	カウント
8769	Exif IFDへのポインタ	LONG	1
8825	GPS IFDへのポインタ	LONG	1
A005	互換性 IFDへのポインタ	LONG	1

## (11) IFD を示すポインタとオフセット

Exif 内のどこに IFD が格納されているかを示すものには表 49 のポインタ以外にも、Tiff ヘッダーの「0th IFD へのオフセット」と 0th IFD の「Next IFD ポインタ」があります。これらを表 50 にまとめます。

表 50 IFD を示すポインタとオフセット

定義場所	
① 0th IFD へのオフセット	Tiff ヘッダー
② Exif IFD へのポインタ	0th IFD 内のフィールドエントリ
③ GPS IFD へのポインタ	0th IFD 内のフィールドエントリ
④ Next IFD ポインタ	0th IFD
⑤ 互換性 IFD へのポインタ	Exif IFD 内のフィールドエントリ

図 39 はポインタ・オフセットが示す IFD への参照イメージ図です。

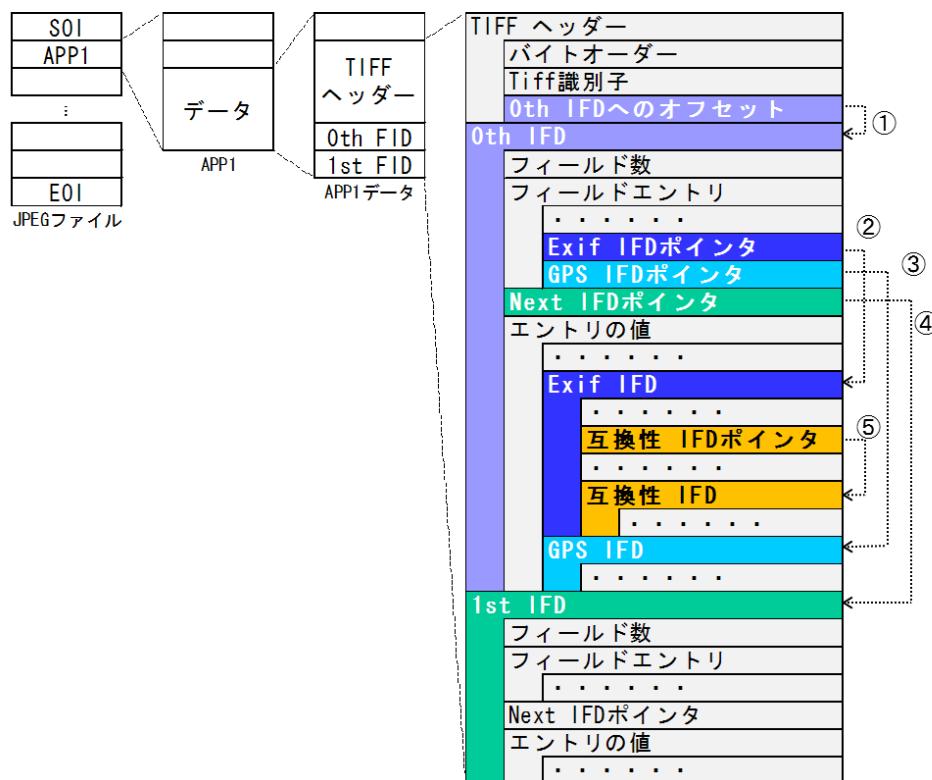


図 39 IFD の参照イメージ

## 参考資料

本付録では iFuzzMaker の開発や操作手順所作成時に参考とした資料やウェブサイトを記載します。

- デジタルスチルカメラ用 画像ファイルフォーマット規格 Exif 2.3  
[http://www.cipa.jp/hyoujunka/kikaku/pdf/DC-008-2010\\_J.pdf](http://www.cipa.jp/hyoujunka/kikaku/pdf/DC-008-2010_J.pdf)  
カメラ映像機器工業会がまとめた Exif 規格の仕様書です。Exif に関する仕様が書かれています。なお、iFuzzMaker のタグ情報ファイルはカメラ映像機器工業会様から許可を得たうえで、「デジタルスチルカメラ用 画像ファイルフォーマット規格 Exif 2.3」から転載利用しています。
- むしやべらり の HSP ページ (2013/7/10 閲覧)  
<http://www14.ocn.ne.jp/~setsuki/ext/jpg.htm>  
JPEG ファイルフォーマットについて書かれています。
- dinop.com (2013/7/10 閲覧)  
<http://www.dinop.com/vc/exif01.html>  
JPEG ファイル解析のロジックについて書かれています。
- F6 Exif ~EXIF 編集ソフト～ (2013/7/10 閉鎖中)  
<http://www.ryouto.jp/f6exif/index.html>  
JPEG 解析ツール「F6 Exif」のホームページです。JPEG ファイルや Exif の構造などが詳しく書かれています。
- JpegAnalyzer Plus オンラインヘルプ (2013/7/10 閲覧)  
<http://hp.vector.co.jp/authors/VA032610/contents.htm>  
JPEG 解析ツール「JpegAnalyzer Plus」のオンラインヘルプです。JPEG ファイルや Exif の構造について書かれています。



## JPEG テスト支援ツール iFuzzMaker 操作手順書

---

[発行] 2013年7月30日

[著作・制作] 独立行政法人情報処理推進機構 セキュリティセンター

編集責任 金野 千里

執筆者 澤田 迅

協力者 板橋 博之 勝海 直人 岡崎 圭輔 山下 勇太