

JCATT ファイルフォーマット仕様書

擬似乱数生成関数 Hash-function DRBG

2008年1月18日

独立行政法人 情報処理推進機構

# 目 次

<b>1</b>	<b>はじめに</b>	<b>1</b>
<b>2</b>	<b>擬似乱数生成関数 Hash-function DRBG</b>	<b>2</b>
2.1	パラメータファイル (*.par) . . . . .	3
2.2	リクエストファイル (*.req) . . . . .	4
2.3	Facts ファイル (*.fax) . . . . .	5
2.4	レスポンスファイル (*.rsp) . . . . .	6
2.5	結果ファイル (*.out) . . . . .	7

# 1 はじめに

暗号アルゴリズム試験ツール (以下 JCATT と略記する) が使用する各種ファイルのフォーマット規則を記述する。JCATT が使用するファイルには次のようなものがある。

## ファイルの種類

- パラメータファイル (\*.par)  
試験項目の設定を記述する。JCATT を用いて作成する。
- リクエストファイル (\*.req)  
暗号モジュール開発ベンダに対する要求を記述する。JCATT を用いて作成する。
- Facts ファイル (\*.fax)  
テストベクタを記述する。JCATT を用いて作成する。
- レスポンスファイル (\*.rsp)  
ベンダからの回答を記述する。リクエストファイルおよび本稿で指定するファイルフォーマットに基づいてベンダが作成する。
- 結果ファイル (\*.out)  
試験結果を記述する。JCATT を用いて作成する。

これらのファイルの名前は、次の規則に従ってつけること。

## ファイル名の規則

- 拡張子は、上記 ( ) 内に指定したものを使用すること。
- 拡張子以外の名前は、試験対象暗号モジュールごとに同じ名称をつけること。  
リクエストファイル (\*.req) と Facts ファイル (\*.fax) の生成時には、リクエストファイル (\*.req) と Facts ファイル (\*.fax) に対してパラメータファイル (\*.par) と同じ名称を JCATT が自動的につける。  
試験実行時には、同じ名称のレスポンスファイル (\*.rsp) と Facts ファイル (\*.fax) に対して試験が行われる。また、試験実行時は、結果ファイル (\*.out) に対して、Facts ファイル (\*.fax) と同じ名称を JCATT が自動的につける。

ファイルフォーマット詳細は次章以降に記述する。各ファイルに共通の規則は次の通りである。

## 共通規則

- [ ] で囲まれた“タグ”の次の行に値を記述する。
- タグは各ファイルフォーマットに記述した順番通りに記述すること。
- レスポンスファイルにおいては【出力】と記述したタグが、試験対象モジュールが出力するデータを記述する箇所である。
- 半角英数字を用いること。
- タグおよび値は大文字小文字の区別をするので、大文字小文字を含めて正確に記述すること。ただし、数値を 16 進数で記述する場合は、大文字小文字は区別しない。
- 一文字目が # (半角) で始まるコメント行を自由に書き込むことができる。
- 平文、暗号文、鍵などデータの区切り文字は改行 (CR+LF または LF) とする。
- 平文、暗号文、署名、鍵などデータは 16 進表記とする。
- ビット数、個数などの数値は 10 進表記とする。
- ACSII コードを使用すること。
- 各行には必ず改行を入れること (最後のデータと EOF との間にも改行を入れること)。

## 2 擬似乱数生成関数 Hash-function DRBG

擬似乱数生成関数, Hash-function DRBG (Information technology - Security techniques - Random bit generation, ISO/IEC 18031) の暗号アルゴリズム試験のためのファイルフォーマットを記述する.

各表において, 試験方法に関する以下の略語を使用する.

- VST: The Variable Seed Test
- MCT: Monte Carlo Test

試験方法の詳細は, 暗号アルゴリズム試験仕様書を参照のこと.

各表におけるハッシュ関数の識別子は次表の通り.

表 1: ハッシュ関数識別子

ハッシュ関数識別子	対応するハッシュ関数
M_Hash_SHA1	SHA-1
M_Hash_SHA224	SHA-224
M_Hash_SHA256	SHA-256
M_Hash_SHA384	SHA-384
M_Hash_SHA512	SHA-512
M_Hash_RIPEMD160	RIPEMD-160

## 2.1 パラメータファイル (\*.par)

表 2: 擬似乱数生成関数 Hash-function DRBG パラメータファイル

機能	タグ	内容
擬似乱数生成	[Algorithm Name]	Hash_DRBG
	[Function Name]	PRNG
	[Hash]	PRNG で使用するハッシュ関数の識別子
	[Bitlength of Random Number for VST]	VST 用の擬似乱数生成ビット長 (1 回に出力するサイズ)
	[C for VST]	VST 用の C 値 (ハッシュサイズ分)
	[Bitlength of Additional Input for VST]	VST 用の Additional Input のビット長
	[Additional Input for VST]	VST 用の Additional Input 値
	[Reseed Counter for VST]	VST 用の Reseed Counter 値
	[Bitlength of Random Number for MCT]	MCT 用の擬似乱数生成ビット長 (1 回に出力するサイズ)
	[C for MCT]	MCT 用の C 値 (ハッシュサイズ分)
	[V for MCT]	MCT 用の V 値 (ハッシュサイズ分)
	[Bitlength of Additional Input for MCT]	MCT 用の Additional Input のビット長
	[Additional Input for MCT]	MCT 用の Additional Input 値
	[Reseed Counter for MCT]	MCT 用の Reseed Counter 値
	[Number of Loop for MCT]	MCT のループの回数

## 2.2 リクエストファイル (\*.req)

表 3: 擬似乱数生成関数 Hash-function DRBG リクエストファイル

機能	タグ	内容
擬似乱数生成	[Algorithm Name]	Hash_DRBG
	[Function Name]	PRNG
	[Hash]	PRNG で使用するハッシュ関数の識別子
	[Bitlength of Random Number for VST]	VST 用の擬似乱数生成ビット長 (1 回に出力するサイズ)
	[C for VST]	VST 用の C 値 (ハッシュサイズ分)
	[V for VST]	VST 用の V 値 (ハッシュサイズ分)
	[Bitlength of Additional Input for VST]	VST 用の Additional Input のビット長
	[Additional Input for VST]	VST 用の Additional Input 値
	[Reseed Counter for VST]	VST 用の Reseed Counter 値
	[Bitlength of Random Number for MCT]	MCT 用の擬似乱数生成ビット長 (1 回に出力するサイズ)
	[C for MCT]	MCT 用の C 値 (ハッシュサイズ分)
	[V for MCT]	MCT 用の V 値 (ハッシュサイズ分)
	[Bitlength of Additional Input for MCT]	MCT 用の Additional Input のビット長
	[Additional Input for MCT]	MCT 用の Additional Input 値
	[Reseed Counter for MCT]	MCT 用の Reseed Counter 値
	[Number of Loop for MCT]	MCT のループの回数

## 2.3 Facts ファイル (\*.fax)

表 4: 擬似乱数生成関数 Hash-function DRBGFacts ファイル

機能	タグ	内容
擬似乱数生成	[Algorithm Name]	Hash_DRBG
	[Function Name]	PRNG
	[Hash]	PRNG で使用するハッシュ関数の識別子
	[Bitlength of Random Number for VST]	VST 用の擬似乱数生成ビット長 (1 回に出力するサイズ)
	[C for VST]	VST 用の C 値 (ハッシュサイズ分)
	[V for VST]	VST 用の V 値 (ハッシュサイズ分)
	[Bitlength of Additional Input for VST]	VST 用の Additional Input のビット長
	[Additional Input for VST]	VST 用の Additional Input 値
	[Reseed Counter for VST]	VST 用の Reseed Counter 値
	[Random Number for VST]	VST で生成された乱数
	[Bitlength of Random Number for MCT]	MCT 用の擬似乱数生成ビット長 (1 回に出力するサイズ)
	[C for MCT]	MCT 用の C 値 (ハッシュサイズ分)
	[V for MCT]	MCT 用の V 値 (ハッシュサイズ分)
	[Bitlength of Additional Input for MCT]	MCT 用の Additional Input のビット長
	[Additional Input for MCT]	MCT 用の Additional Input 値
	[Reseed Counter for MCT]	MCT 用の Reseed Counter 値
	[Number of Loop for MCT]	MCT のループの回数
	[Random Number for MCT]	MCT で生成された乱数

## 2.4 レスponseファイル (\*.rsp)

表 5: 擬似乱数生成関数 Hash-function DRBG レスponseファイル

機能	タグ	内容
擬似乱数生成	[Algorithm Name]	Hash_DRBG
	[Function Name]	PRNG
	[Hash]	PRNG で使用するハッシュ関数の識別子
	[Bitlength of Random Number for VST]	VST 用の擬似乱数生成ビット長 (1 回に出力するサイズ)
	[C for VST]	VST 用の C 値 (ハッシュサイズ分)
	[V for VST]	VST 用の V 値 (ハッシュサイズ分)
	[Bitlength of Additional Input for VST]	VST 用の Additional Input のビット長
	[Additional Input for VST]	VST 用の Additional Input 値
	[Reseed Counter for VST]	VST 用の Reseed Counter 値
	[Random Number for VST]	【出力】VST で生成された乱数
	[Bitlength of Random Number for MCT]	MCT 用の擬似乱数生成ビット長 (1 回に出力するサイズ)
	[C for MCT]	MCT 用の C 値 (ハッシュサイズ分)
	[V for MCT]	MCT 用の V 値 (ハッシュサイズ分)
	[Bitlength of Additional Input for MCT]	MCT 用の Additional Input のビット長
	[Additional Input for MCT]	MCT 用の Additional Input 値
	[Reseed Counter for MCT]	MCT 用の Reseed Counter 値
	[Number of Loop for MCT]	MCT のループの回数
	[Random Number for MCT]	【出力】MCT で生成された乱数



## 2.5 結果ファイル (\*.out)

表 6: 擬似乱数生成関数 Hash-function DRBG 結果ファイル

タグ	内容
[Algorithm Name]	暗号名
[Function Name]	試験対象機能名
[Results]	試験結果

### 注

- 試験合格の場合，[Results] に OK と表示される．
- 試験不合格の場合，[Results] に何らかの形式で NG と表示される．また，[Results] には，レスポンスファイル内の不合格となったデータが記述されているタグ名と，そのタグ内の何番目 (No.，#等の記号で番号を表す) のデータが不合格となったかが表示される．不合格となったデータが記述されているタグ名は，前記のレスポンスファイル仕様に【出力】と記述したタグである．ただし【出力】と記述したタグが1つしかない場合，タグ名は省略することがある．