

# JCATT ファイルフォーマット仕様書

## ブロック暗号

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>ブロック暗号</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) . . . . .	6
2.4	レスポンスファイル (*.rsp) . . . . .	8
2.5	結果ファイル (*.out) . . . . .	10

# 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 ブロック暗号

ブロック暗号 MISTY1 , Hierocrypt-L1 , CIPHERUNICORN-E , Camellia , Hierocrypt-3 , SC2000 , CIPHERUNICORN-A の試験のためのファイルフォーマットを記述する . これらのブロック暗号に対するファイルフォーマットは , Algorithm Name の他は同じである .

Algorithm Name は , それぞれ下記の通り .

- MISTY1
- Hierocrypt-L1
- CIPHERUNICORN-E
- Camellia
- Hierocrypt-3
- SC2000
- CIPHERUNICORN-A

各表において , 試験方法に関する以下の略語を使用する .

- KAT-Text: Variable Plaintext(Ciphertext) Known Answer Test
- KAT-Key: Variable Key Known Answer Test
- KAT-Sbox: Sbox Known Answer Test
- MMT: Multi-block Message Test
- MCT: Monte Carlo Test

これらの試験方法の詳細は , 暗号アルゴリズム試験仕様書を参照のこと .

## 2.1 パラメータファイル (\*.par)

表 1: ブロック暗号パラメータファイル

機能	タグ	内容
(共通)	[Algorithm Name]	(暗号名)
暗号化	[Function Name]	Encryption
	[Modes of Operation]	ECB , CBC , CFB, OFB , CTR のうちいずれか 1 つ
	[Bitlength of Key]	鍵のビット長
	[Number of Blocks for MMT]	MMT のブロック数
	[Key for MMT]	MMT 用鍵
	[IV for MMT]	MMT 用 IV
	[Plaintext for MMT]	MMT 用平文
	[Number of Inner-loop for MCT]	MCT の内側ループの回数
	[Number of Outer-loop for MCT]	MCT の外側ループの回数
	[Initial Key for MCT]	MCT 用鍵の初期値
	[Initial Plaintext for MCT]	MCT 用平文の初期値
	[Initial IV for MCT]	MCT 用 IV の初期値
	[Initial Value of Counter for MMT]	MMT 用カウンタ初期値 (Mode に CTR を指定した場合のみこのタグを記述する)
	[Initial Value of Counter for MCT]	MCT 用カウンタ初期値 (Mode に CTR を指定した場合のみこのタグを記述する)
	[Bitlength of Counter]	カウンタのビット幅 (Mode に CTR を指定した場合のみこのタグを記述する)
復号	[Function Name]	Decryption
	[Modes of Operation]	暗号化と同じ
	[Bitlength of Key]	
	[Number of Blocks for MMT]	
	[Key for MMT]	
	[IV for MMT]	
	[Ciphertext for MMT]	MMT 用暗号文
	[Number of Inner-loop for MCT]	暗号化と同じ
	[Number of Outer-loop for MCT]	
	[Initial Key for MCT]	
	[Initial Ciphertext for MCT]	MCT 用暗号文の初期値
	[Initial IV for MCT]	暗号化と同じ
	[Initial Value of Counter for MMT]	
	[Initial Value of Counter for MCT]	
	[Bitlength of Counter]	

## 2.2 リクエストファイル (\*.req)

表 2: ブロック暗号リクエストファイル (暗号化)

機能	タグ	内容
(共通)	[Algorithm Name]	(暗号名)
暗号化	[Function Name]	Encryption
	[Modes of Operation]	ECB , CBC , CFB, OFB , CTR のうちいずれか 1 つ
	[Bitlength of Key]	鍵のビット長
	[Bitlength of Counter]	カウンタのビット幅 (Mode に CTR を指定した場合のみこのタグを記述する)
	[Key for KAT-Text]	KAT-Text 用鍵
	[IV for KAT-Text]	KAT-Text 用 IV
	[Counter for KAT-Text]	KAT-Text 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Plaintext for KAT-Text]	KAT-Text 用平文
	[Key for KAT-Key]	KAT-Key 用鍵
	[IV for KAT-Key]	KAT-Key 用 IV
	[Counter for KAT-Key]	KAT-Key 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Plaintext for KAT-Key]	KAT-Key 用平文
	[Key for KAT-Sbox]	KAT-Sbox 用鍵
	[IV for KAT-Sbox]	KAT-Sbox 用 IV
	[Counter for KAT-Sbox]	KAT-Sbox 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Plaintext for KAT-Sbox]	KAT-Sbox 用平文
	[Number of Blocks for MMT]	MMT のブロック数
	[Key for MMT]	MMT 用鍵
	[IV for MMT]	MMT 用 IV
	[Initial Value of Counter for MMT]	MMT 用カウンタ初期値 (Mode に CTR を指定した場合のみこのタグを記述する)
	[Plaintext for MMT]	MMT 用平文
	[Number of Inner-loop for MCT]	MCT の内側ループの回数
	[Number of Outer-loop for MCT]	MCT の外側ループの回数
	[Initial Key for MCT]	MCT 用鍵の初期値
	[Initial IV for MCT]	MCT 用 IV の初期値
	[Initial Value of Counter for MCT]	MCT 用カウンタ初期値 (Mode に CTR を指定した場合のみこのタグを記述する)
	[Initial Plaintext for MCT]	MCT 用平文の初期値

表 3: ブロック暗号リクエストファイル (復号)

機能	タグ	内容
(共通)	[Algorithm Name]	(暗号名)
復号	[Function Name]	Decryption
	[Modes of Operation]	暗号化と同じ
	[Bitlength of Key]	
	[Bitlength of Counter]	
	[Key for KAT-Text]	KAT-Text 用鍵
	[IV for KAT-Text]	KAT-Text 用 IV
	[Counter for KAT-Text]	KAT-Text 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Ciphertext for KAT-Text]	KAT-Text 用暗号文
	[Key for KAT-Key]	KAT-Key 用鍵
	[IV for KAT-Key]	KAT-Key 用 IV
	[Counter for KAT-Key]	KAT-Key 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Ciphertext for KAT-Key]	KAT-Key 用暗号文
	[Key for KAT-Sbox]	KAT-Sbox 用鍵
	[IV for KAT-Sbox]	KAT-Sbox 用 IV
	[Counter for KAT-Sbox]	KAT-Sbox 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Ciphertext for KAT-Sbox]	KAT-Sbox 用暗号文
	[Number of Blocks for MMT]	暗号化と同じ
	[Key for MMT]	
	[IV for MMT]	
	[Initial Value of Counter for MMT]	
	[Ciphertext for MMT]	MMT 用暗号文
	[Number of Inner-loop for MCT]	暗号化と同じ
	[Number of Outer-loop for MCT]	
	[Initial Key for MCT]	
	[Initial IV for MCT]	
	[Initial Value of Counter for MCT]	MCT 用暗号文の初期値
	[Initial Ciphertext for MCT]	

## 2.3 Facts ファイル (\*.fax)

表 4: ブロック暗号 Facts ファイル (暗号化)

機能	タグ	内容
(共通)	[Algorithm Name]	(暗号名)
暗号化	[Function Name]	Encryption
	[Modes of Operation]	ECB , CBC , CFB, OFB , CTR のうちいずれか 1 つ
	[Bitlength of Key]	鍵のビット長
	[Bitlength of Counter]	カウンタのビット幅 (Mode に CTR を指定した場合のみこのタグを記述する)
	[Key for KAT-Text]	KAT-Text 用鍵
	[IV for KAT-Text]	KAT-Text 用 IV
	[Counter for KAT-Text]	KAT-Text 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Plaintext for KAT-Text]	KAT-Text 用平文
	[Ciphertext for KAT-Text]	上記パラメータに対する期待値暗号文
	[Key for KAT-Key]	KAT-Key 用鍵
	[IV for KAT-Key]	KAT-Key 用 IV
	[Counter for KAT-Key]	KAT-Key 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Plaintext for KAT-Key]	KAT-Key 用平文
	[Ciphertext for KAT-Key]	上記パラメータに対する期待値暗号文
	[Key for KAT-Sbox]	KAT-Sbox 用鍵
	[IV for KAT-Sbox]	KAT-Sbox 用 IV
	[Counter for KAT-Sbox]	KAT-Sbox 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Plaintext for KAT-Sbox]	KAT-Sbox 用平文
	[Ciphertext for KAT-Sbox]	上記パラメータに対する期待値暗号文
	[Number of Blocks for MMT]	MMT のブロック数
	[Key for MMT]	MMT 用鍵
	[IV for MMT]	MMT 用 IV
	[Initial Value of Counter for MMT]	MMT 用カウンタ初期値 (Mode に CTR を指定した場合のみこのタグを記述する)
	[Plaintext for MMT]	MMT 用平文
	[Ciphertext for MMT]	MMT 期待値暗号文
	[Number of Inner-loop for MCT]	MCT の内側ループの回数
	[Number of Outer-loop for MCT]	MCT の外側ループの回数
	[Initial Key for MCT]	MCT 用鍵の初期値
	[Initial IV for MCT]	MCT 用 IV の初期値
	[Initial Value of Counter for MCT]	MCT 用カウンタ初期値 (Mode に CTR を指定した場合のみこのタグを記述する)
	[Initial Plaintext for MCT]	MCT 用平文の初期値
	[Ciphertext for MCT]	MCT 期待値暗号文



表 5: ブロック暗号 Facts ファイル (復号)

機能	タグ	内容
(共通)	[Algorithm Name]	(暗号名)
復号	[Function Name]	Decryption
	[Modes of Operation]	暗号化と同じ
	[Bitlength of Key]	
	[Bitlength of Counter]	
	[Key for KAT-Text]	KAT-Text 用鍵
	[IV for KAT-Text]	KAT-Text 用 IV
	[Counter for KAT-Text]	KAT-Text 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Ciphertext for KAT-Text]	KAT-Text 用暗号文
	[Plaintext for KAT-Text]	上記パラメータに対する期待値平文
	[Key for KAT-Key]	KAT-Key 用鍵
	[IV for KAT-Key]	KAT-Key 用 IV
	[Counter for KAT-Key]	KAT-Key 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Ciphertext for KAT-Key]	KAT-Key 用暗号文
	[Plaintext for KAT-Key]	上記パラメータに対する期待値平文
	[Key for KAT-Sbox]	KAT-Sbox 用鍵
	[IV for KAT-Sbox]	KAT-Sbox 用暗号文
	[Counter for KAT-Sbox]	KAT-Sbox 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Ciphertext for KAT-Sbox]	KAT-Sbox 用暗号文
	[Plaintext for KAT-Sbox]	上記パラメータに対する期待値平文
	[Number of Blocks for MMT]	暗号化と同じ
	[Key for MMT]	
	[IV for MMT]	
	[Initial Value of Counter for MMT]	
	[Ciphertext for MMT]	MMT 用暗号文
	[Plaintext for MMT]	MMT 期待値平文
	[Number of Inner-loop for MCT]	暗号化と同じ
	[Number of Outer-loop for MCT]	
	[Initial Key for MCT]	
	[Initial IV for MCT]	
	[Initial Value of Counter for MCT]	
	[Initial Ciphertext for MCT]	MCT 用暗号文の初期値
	[Plaintext for MCT]	MCT 期待値平文

## 2.4 レスponseファイル (\*.rsp)

表 6: ブロック暗号レスponseファイル (暗号化)

機能	タグ	内容
(共通)	[Algorithm Name]	(暗号名)
暗号化	[Function Name]	Encryption
	[Modes of Operation]	ECB , CBC , CFB, OFB , CTR のうちいずれか 1 つ
	[Bitlength of Key]	鍵のビット長
	[Bitlength of Counter]	カウンタのビット幅 (Mode に CTR を指定した場合のみこのタグを記述する)
	[Key for KAT-Text]	KAT-Text 用鍵
	[IV for KAT-Text]	KAT-Text 用 IV
	[Counter for KAT-Text]	KAT-Text 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Plaintext for KAT-Text]	KAT-Text 用平文
	[Ciphertext for KAT-Text]	【出力】上記パラメータに対する暗号文
	[Key for KAT-Key]	KAT-Key 用鍵
	[IV for KAT-Key]	KAT-Key 用 IV
	[Counter for KAT-Key]	KAT-Key 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Plaintext for KAT-Key]	KAT-Key 用平文
	[Ciphertext for KAT-Key]	【出力】上記パラメータに対する暗号文
	[Key for KAT-Sbox]	KAT-Sbox 用鍵
	[IV for KAT-Sbox]	KAT-Sbox 用 IV
	[Counter for KAT-Sbox]	KAT-Sbox 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Plaintext for KAT-Sbox]	KAT-Sbox 用平文
	[Ciphertext for KAT-Sbox]	【出力】上記パラメータに対する暗号文
	[Number of Blocks for MMT]	MMT のブロック数
	[Key for MMT]	MMT 用鍵
	[IV for MMT]	MMT 用 IV
	[Initial Value of Counter for MMT]	MMT 用カウンタ初期値 (Mode に CTR を指定した場合のみこのタグを記述する)
	[Plaintext for MMT]	MMT 用平文
	[Ciphertext for MMT]	【出力】MMT で生成された暗号文
	[Number of Inner-loop for MCT]	MCT の内側ループの回数
	[Number of Outer-loop for MCT]	MCT の外側ループの回数
	[Initial Key for MCT]	MCT 用鍵の初期値
	[Initial IV for MCT]	MCT 用 IV の初期値
	[Initial Value of Counter for MCT]	MCT 用カウンタ初期値 (Mode に CTR を指定した場合のみこのタグを記述する)
	[Initial Plaintext for MCT]	MCT 用平文の初期値
	[Ciphertext for MCT]	【出力】MCT で生成された暗号文

表 7: ブロック暗号レスポンスファイル (復号)

機能	タグ	内容
(共通)	[Algorithm Name]	(暗号名)
復号	[Function Name]	Decryption
	[Modes of Operation]	暗号化と同じ
	[Bitlength of Key]	暗号化と同じ
	[Bitlength of Counter]	
	[Key for KAT-Text]	KAT-Text 用鍵
	[IV for KAT-Text]	KAT-Text 用 IV
	[Counter for KAT-Text]	KAT-Text 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Ciphertext for KAT-Text]	KAT-Text 用暗号文
	[Plaintext for KAT-Text]	【出力】上記パラメータに対する平文
	[Key for KAT-Key]	KAT-Key 用鍵
	[IV for KAT-Key]	KAT-Key 用 IV
	[Counter for KAT-Key]	KAT-Key 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Ciphertext for KAT-Key]	KAT-Key 用暗号文
	[Plaintext for KAT-Key]	【出力】上記パラメータに対する平文
	[Key for KAT-Sbox]	KAT-Sbox 用鍵
	[IV for KAT-Sbox]	KAT-Sbox 用暗号文
	[Counter for KAT-Sbox]	KAT-Sbox 用カウンタ (Mode に CTR を指定した場合のみこのタグを記述する)
	[Ciphertext for KAT-Sbox]	KAT-Sbox 用暗号文
	[Plaintext for KAT-Sbox]	【出力】上記パラメータに対する平文
	[Number of Blocks for MMT]	暗号化と同じ
	[Key for MMT]	
	[IV for MMT]	
	[Initial Value of Counter for MMT]	
	[Ciphertext for MMT]	
	[Plaintext for MMT]	【出力】MMT で生成された平文
	[Number of Inner-loop for MCT]	暗号化と同じ
	[Number of Outer-loop for MCT]	
	[Initial Key for MCT]	
	[Initial IV for MCT]	
	[Initial Value of Counter for MCT]	
	[Initial Ciphertext for MCT]	
	[Plaintext for MCT]	【出力】MCT で生成された平文

## 2.5 結果ファイル (\*.out)

表 8: ブロック暗号結果ファイル

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．