

企業・個人の情報セキュリティ対策事業  
暗号アルゴリズム実装試験ツールの機能追加

JCATT ファイルフォーマット仕様書

MULTI-S01

2008 年 4 月

独立行政法人 情報処理推進機構

# 目次

|     |                              |   |
|-----|------------------------------|---|
| 1   | はじめに                         | 3 |
| 2   | MULTI-S01                    | 4 |
| 2.1 | パラメータファイル (*.par) . . . . .  | 4 |
| 2.2 | リクエストファイル (*.req) . . . . .  | 5 |
| 2.3 | Facts ファイル (*.fax) . . . . . | 6 |
| 2.4 | レスポンスファイル (*.rsp) . . . . .  | 7 |
| 2.5 | 結果ファイル (*.out) . . . . .     | 8 |

## 1 はじめに

暗号アルゴリズム実装試験ツール(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、鍵などの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、鍵などのデータは 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 MULTI-S01

MULTI-S01 の暗号アルゴリズム実装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。

- KAT-Text: Variable Plaintext(Ciphertext) Known Answer Test
- KAT-Key: Variable Key Known Answer Test
- MCT: Monte Carlo Test

試験方法の詳細は、暗号アルゴリズム実装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: MULTI-S01 パラメータファイル

| 機能   | タグ                                 | 内容                      |
|------|------------------------------------|-------------------------|
| (共通) | [Algorithm Name]                   | MULTI-S01               |
| 暗号化  | [Function Name]                    | Encryption              |
|      | [Bitlength of Plaintexts for KAT]  | KAT-Text の平文ビット数        |
|      | [Initial Value for KAT-Text]       | KAT-Text 用初期値 (256 ビット) |
|      | [Redundancy for KAT-Text]          | KAT-Text 用冗長性 (64 ビット)  |
|      | [Initial Value for KAT-Key]        | KAT-Key 用初期値 (256 ビット)  |
|      | [Redundancy for KAT-Key]           | KAT-Key 用冗長性 (64 ビット)   |
|      | [Initial Value for MCT]            | MCT 用初期値 (256 ビット)      |
|      | [Redundancy for MCT]               | MCT 用冗長性 (64 ビット)       |
|      | [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             |
| 復号   | [Function Name]                    | Decryption              |
|      | [Bitlength of Ciphertexts for KAT] | KAT-Text の暗号文ビット数       |
|      | [Initial Value for KAT-Text]       | KAT-Text 用初期値 (256 ビット) |
|      | [Redundancy for KAT-Text]          | KAT-Text 用冗長性 (64 ビット)  |

## 2.2 リクエストファイル (\*.req)

表 2: MULTI-S01 リクエストファイル

| 機能                          | タグ                                 | 内容                                |
|-----------------------------|------------------------------------|-----------------------------------|
| (共通)                        | [Algorithm Name]                   | MULTI-S01                         |
| 暗号化                         | [Function Name]                    | Encryption                        |
|                             | [Bitlength of Plaintexts for KAT]  | KAT-Text の平文ビット数 [10 進数表記]        |
|                             | [Initial Value for KAT-Text]       | KAT-Text 用初期値 (256 ビット) [16 進数表記] |
|                             | [Redundancy for KAT-Text]          | KAT-Text 用冗長性 (64 ビット) [16 進数表記]  |
|                             | [Key for KAT-Text]                 | KAT-Text 用鍵 [16 進数表記]             |
|                             | [Plaintext for KAT-Text]           | KAT-Text 用平文 [16 進数表記]            |
|                             | [Initial Value for KAT-Key]        | KAT-Key 用初期値 (256 ビット) [16 進数表記]  |
|                             | [Redundancy for KAT-Key]           | KAT-Key 用冗長性 (64 ビット) [16 進数表記]   |
|                             | [Plaintext for KAT-Key]            | KAT-Key 用平文 [16 進数表記]             |
|                             | [Key for KAT-Key]                  | KAT-Key 用鍵 [16 進数表記]              |
|                             | [Initial Value for MCT]            | MCT 用初期値 (256 ビット) [16 進数表記]      |
|                             | [Redundancy for MCT]               | MCT 用冗長性 (64 ビット) [16 進数表記]       |
|                             | [Number of Inner-loop for MCT]     | MCT の内側ループの回数 [10 進数表記]           |
|                             | [Number of Outer-loop for MCT]     | MCT の外側ループの回数 [10 進数表記]           |
| [Initial Key for MCT]       | MCT 用鍵の初期値 [16 進数表記]               |                                   |
| [Initial Plaintext for MCT] | MCT 用平文の初期値 [16 進数表記]              |                                   |
| 復号                          | [Function Name]                    | Decryption                        |
|                             | [Bitlength of Ciphertexts for KAT] | KAT-Text の暗号文ビット数 [10 進数表記]       |
|                             | [Initial Value for KAT-Text]       | KAT-Text 用初期値 (256 ビット) [16 進数表記] |
|                             | [Redundancy for KAT-Text]          | KAT-Text 用冗長性 (64 ビット) [16 進数表記]  |
|                             | [Key for KAT-Text]                 | KAT-Key 用鍵 [16 進数表記]              |
|                             | [Ciphertext for KAT-Text]          | KAT-Text 用暗号文 [16 進数表記]           |

## 2.3 Facts ファイル (\*.fax)

表 3: MULTI-S01Facts ファイル

| 機能                          | タグ                                    | 内容                      |
|-----------------------------|---------------------------------------|-------------------------|
| (共通)                        | [Algorithm Name]                      | MULTI-S01               |
| 暗号化                         | [Function Name]                       | Encryption              |
|                             | [Bitlength of Plaintexts for KAT]     | KAT-Text の平文ビット数        |
|                             | [Initial Value for KAT-Text]          | KAT-Text 用初期値 (256 ビット) |
|                             | [Redundancy for KAT-Text]             | KAT-Text 用冗長性 (64 ビット)  |
|                             | [Key for KAT-Text]                    | Variable Text KAT 用鍵    |
|                             | [Plaintext for KAT-Text]              | KAT-Text 用平文            |
|                             | [Ciphertext for KAT-Text]             | KAT-Text で生成された暗号文      |
|                             | [Initial Value for KAT-Key]           | KAT-Key 用初期値 (256 ビット)  |
|                             | [Redundancy for KAT-Key]              | KAT-Key 用冗長性 (64 ビット)   |
|                             | [Plaintext for KAT-Key]               | KAT-Key 用平文             |
|                             | [Key for KAT-Key]                     | KAT-Key 用鍵              |
|                             | [Ciphertext for KAT-Key]              | KAT-Key で生成された暗号文       |
|                             | [Initial Value for MCT]               | MCT 用初期値 (256 ビット)      |
|                             | [Redundancy for MCT]                  | MCT 用冗長性 (64 ビット)       |
|                             | [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                           |                         |
| [Ciphertext for MCT]        | MCT で生成された暗号文                         |                         |
| 復号                          | [Function Name]                       | Decryption              |
|                             | [Bitlength of Ciphertexts for KAT]    | KAT-Text の暗号文ビット数       |
|                             | [Initial Value for KAT-Text]          | KAT-Text 用初期値 (256 ビット) |
|                             | [Redundancy for KAT-Text]             | KAT-Text 用冗長性 (64 ビット)  |
|                             | [Key for KAT-Text]                    | Variable Text KAT 用鍵    |
|                             | [Ciphertext for KAT-Text]             | KAT-Text 用暗号文           |
|                             | [Plaintext for KAT-Text] <sup>1</sup> | KAT-Text で生成された平文       |

注

1. 復号で改竄検出信号を検出した場合は, [Plaintext for KAT-Text] データの該当行に MAC NG と記述する .

## 2.4 レスponseファイル (\*.rsp)

表 4: MULTI-S01 レスponseファイル

| 機能                          | タグ                                    | 内容                                |
|-----------------------------|---------------------------------------|-----------------------------------|
| (共通)                        | [Algorithm Name]                      | MULTI-S01                         |
| 暗号化                         | [Function Name]                       | Encryption                        |
|                             | [Bitlength of Plaintexts for KAT]     | KAT-Text の平文ビット数 [10 進数表記]        |
|                             | [Initial Value for KAT-Text]          | KAT-Text 用初期値 (256 ビット) [16 進数表記] |
|                             | [Redundancy for KAT-Text]             | KAT-Text 用冗長性 (64 ビット) [16 進数表記]  |
|                             | [Key for KAT-Text]                    | KAT-Text 用鍵 [16 進数表記]             |
|                             | [Plaintext for KAT-Text]              | KAT-Text 用平文 [16 進数表記]            |
|                             | [Ciphertext for KAT-Text]             | 【出力】KAT-Text で生成された暗号文 [16 進数表記]  |
|                             | [Initial Value for KAT-Key]           | KAT-Key 用初期値 (256 ビット) [16 進数表記]  |
|                             | [Redundancy for KAT-Key]              | KAT-Key 用冗長性 (64 ビット) [16 進数表記]   |
|                             | [Plaintext for KAT-Key]               | KAT-Key 用平文 [16 進数表記]             |
|                             | [Key for KAT-Key]                     | KAT-Key 用鍵 [16 進数表記]              |
|                             | [Ciphertext for KAT-Key]              | 【出力】KAT-Key で生成された暗号文 [16 進数表記]   |
|                             | [Initial Value for MCT]               | MCT 用初期値 (256 ビット) [16 進数表記]      |
|                             | [Redundancy for MCT]                  | MCT 用冗長性 (64 ビット) [16 進数表記]       |
|                             | [Number of Inner-loop for MCT]        | MCT の内側ループの回数 [10 進数表記]           |
|                             | [Number of Outer-loop for MCT]        | MCT の外側ループの回数 [10 進数表記]           |
|                             | [Initial Key for MCT]                 | MCT 用鍵の初期値 [16 進数表記]              |
| [Initial Plaintext for MCT] | MCT 用平文の初期値 [16 進数表記]                 |                                   |
| [Ciphertext for MCT]        | 【出力】MCT で生成された暗号文 [16 進数表記]           |                                   |
| 復号                          | [Function Name]                       | Decryption                        |
|                             | [Bitlength of Ciphertexts for KAT]    | KAT-Text の暗号文ビット数 [10 進数表記]       |
|                             | [Initial Value for KAT-Text]          | KAT-Text 用初期値 (256 ビット) [16 進数表記] |
|                             | [Redundancy for KAT-Text]             | KAT-Text 用冗長性 (64 ビット) [16 進数表記]  |
|                             | [Key for KAT-Text]                    | Variable Text KAT 用鍵 [16 進数表記]    |
|                             | [Ciphertext for KAT-Text]             | KAT-Text 用暗号文 [16 進数表記]           |
|                             | [Plaintext for KAT-Text] <sup>1</sup> | 【出力】KAT-Text で生成された平文 [16 進数表記]   |

### 注

1. 復号で改竄検出信号を検出した場合は, [Plaintext for KAT-Text] データの該当行に MAC NG と記述する .

## 2.5 結果ファイル (\*.out)

表 5: MULTI-S01 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．