JCATT ファイルフォーマット仕様書

KCipher-2

2018 年 8 月

独立行政法人情報処理推進機構

目次

1 はじめに 3

2 KCipher-2 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使用すること．
- 拡張子以外の名前は，試験対象実装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

- JCATT 互換ファイルフォーマットの選択時, [　　] で囲まれた “タグ” の次の行に値を記述する．
- CAVS 準互換ファイルフォーマットの選択時, 〈 タグ 〉=〈 値 〉 の形式で 1 行で記述する．
- ヘッダ部分については各行について [〈 タグ 〉=〈 値 〉] の形式で 1 行で記述する．
- レスポンスファイルにおいては，【出力】と記述したタグが，試験対象実装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 KCipher-2

KCipher-2 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-Key: Variable Key Known Answer Test
- KAT-IV: Variable IV Known Answer Test
- KAT-Table: Table Look-Up 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 KCipher-2 パラメータファイル

機能	タグ		内容	表記
擬似乱数生成機能	全体ヘッダ	AlgorithmName	KCipher-2	文字列
		NumberOfBlocksToGenerateInKATKey	KAT-Key の生成するブロック数	10 進
		NumberOfBlocksToGenerateInKATIV	KAT-IV の生成するブロック数	10 進
		NumberOfBlocksToGenerateInKATTable	KAT-Table の生成するブロック数	10 進
		NumberOfInnerLoopsInMCT	MCT の内側ループの回数	10 進
		NumberOfOuterLoopsInMCT	MCT の外側ループの回数	10 進
		NumberOfBlocksToGenerateInMCT	内側ループの中で生成する鍵系列のブロック数	10 進
		NumberOfBlocksToCompareInMCT	レスポンスファイルに記録する鍵系列のブロック数	10 進

2.2 リクエストファイル (*.req)

表2: KCipher-2 リクエストファイル

機能	分類		タグ	内容	暗号アルゴリズム実装試験仕様書—共通鍵—上の表記との対応	値の表記	例示
擬似乱数生成機能	全体ヘッダ		AlgorithmName	KCipher-2		文字列	[AlgorithmName = KCipher-2]
			NumberOfBlocksToGenerateInKATKey	KAT-Key の生成するブロック数		10 進表記	[NumberOfBlocksToGenerateInKATKey = 24]
			NumberOfBlocksToGenerateInKATIV	KAT-IV の生成するブロック数		10 進表記	[NumberOfBlocksToGenerateInKATIV = 24]
			NumberOfBlocksToGenerateInKATTable	KAT-Table の生成するブロック数		10 進表記	[NumberOfBlocksToGenerateInKATTable = 3500]
			NumberOfInnerLoopsInMCT	MCT の内側ループの回数	$innerloop$	10 進表記	[NumberOfInnerLoopsInMCT = 1000]
			NumberOfOuterLoopsInMCT	MCT の外側ループの回数	$outerloop$	10 進表記	[NumberOfOuterLoopsInMCT = 100]
			NumberOfBlocksToGenerateInMCT	内側ループの中で生成する鍵系列のブロック数	N_b	10 進表記	[NumberOfBlocksToGenerateInMCT = 10000]
			NumberOfBlocksToCompareInMCT	レスポンスファイルに記録する鍵系列のブロック数	N_c	10 進表記	[NumberOfBlocksToCompareInMCT = 24]
	KAT-KEY	KAT-KEY ヘッダ	InitialIVForKATKey	入力となるビット列 IV		16 進表記	InitialIVForKATKey = 00. . .00
		KAT-KEY 本体 *1	COUNT	0 以上 128 以下の整数		10 進表記	COUNT = 0
			InitialKeyForKATKey	入力となるビット列 Key		16 進表記	InitialKeyForKATKey = fffc . . . 0000
			KeyStream	出力であるビット列		16 進表記	KeyStream = ?
	KAT-IV	KAT-IV ヘッダ	InitialKeyForKATIV	入力となるビット列 Key		16 進表記	InitialKeyForKATIV = 00. . .00
		KAT-IV 本体 *2	COUNT	0 以上 128 以下の整数		10 進表記	COUNT = 0
			InitialIVForKATIV	入力となるビット列 IV		16 進表記	InitialIVForKATIV = fffc . . . 0000
			KeyStream	出力であるビット列		16 進表記	KeyStream = ?
	KAT-Table	KAT-Table ヘッダ	Output Length (bits)	出力となるビット列のビット長		10 進表記	[Output Length (bits) = 224000]
		KAT-Table 本体	COUNT	0		10 進表記	COUNT = 0
			InitialKeyForKATTable	入力となるビット列 Key		16 進表記	InitialKeyForKATTable = 0000 . . . 0000
			InitialIVForKATTable	入力となるビット列 IV		16 進表記	InitialIVForKATTable = 0000 . . . 0000
			KeyStream	出力であるビット列		16 進表記	KeyStream = ?
	MCT	MCT ヘッダ	InitialKeyForMCT	入力となるビット列 Key	Key	16 進表記	InitialKeyForMCT = e47a . . . dbc8
			InitialIVForMCT	入力となるビット列 IV	IV	16 進表記	InitialIVForMCT = 452c . . . aeed
		MCT 本体 *3	COUNT	0 以上 NumberOfOuterLoopsInMCT 未満の整数	j	10 進表記	COUNT = 0
			KeyStream	出力であるビット列	$j = \langle$ COUNT の値 $\rangle$ に対応する Y	16 進表記	KeyStream = ?

*1 129 個の各データの組を以下のように記述する.

```
COUNT = 0                           ♯ COUNT = 0 のデータの組について記述する.
InitialKeyForKATKey = 0000 ... 0000 ♯ COUNT = 0 に対応する Key を記述する.
KeyStream = ?                       ♯ COUNT = 0 に対応する鍵系列のプレースホルダ.

COUNT = 1                           ♯ COUNT = 1 のデータの組について記述する.
InitialKeyForKATKey = 8000 ... 0000 ♯ COUNT = 1 に対応する Key を記述する.
KeyStream = ?                       ♯ COUNT = 1 に対応する鍵系列のプレースホルダ.
.
.
.
COUNT = 128                         ♯ COUNT = 128 のデータの組について記述する.
InitialKeyForKATKey = ffff ... ffff ♯ COUNT = 128 に対応する Key を記述する.
KeyStream = ?                       ♯ COUNT = 128 に対応する鍵系列のプレースホルダ.
```

*2 129 個の各データの組を以下のように記述する.

```
COUNT = 0                           ♯ COUNT = 0 のデータの組について記述する.
InitialIVForKATIV = 0000 ... 0000   ♯ COUNT = 0 に対応する IV を記述する.
KeyStream = ?                       ♯ COUNT = 0 に対応する鍵系列のプレースホルダ.

COUNT = 1                           ♯ COUNT = 1 のデータの組について記述する.
InitialIVForKATIV = 8000 ... 0000   ♯ COUNT = 1 に対応する IV を記述する.
KeyStream = ?                       ♯ COUNT = 1 に対応する鍵系列のプレースホルダ.
.
.
.
COUNT = 128                         ♯ COUNT = 128 のデータの組について記述する.
InitialIVForKATIV = ffff ... ffff   ♯ COUNT = 128 に対応する IV を記述する.
KeyStream = ?                       ♯ COUNT = 128 に対応する鍵系列のプレースホルダ.
```

*3 NumberOfOuterLoopsInMCT 個の各データの組を以下のように記述する.

```
COUNT = 0                                ♯ j = 0 のデータの組について記述する.
KeyStream = ?                            ♯ j = 0 に対応する鍵系列のプレースホルダ.

COUNT = 1                                ♯ j = 1 のデータの組について記述する.
KeyStream = ?                            ♯ j = 1 に対応する鍵系列のプレースホルダ.
.
.
.
COUNT = ⟨ NumberOfOuterLoopsInMCT −1⟩    ♯ j = ⟨ NumberOfOuterLoopsInMCT −1⟩ のデータの組について記述する.
KeyStream = ?                            ♯ j = ⟨ NumberOfOuterLoopsInMCT −1⟩ に対応する鍵系列のプレースホルダ.
```

2.3 Facts ファイル (*.fax)

表3: KCipher-2 Facts ファイル

機能	分類		タグ	内容	暗号アルゴリズム実装試験仕様書—共通鍵—上の表記との対応	値の表記	例示
擬似乱数生成機能	全体ヘッダ		AlgorithmName	KCipher-2		文字列	[AlgorithmName = KCipher-2]
			NumberOfBlocksToGenerateInKATKey	KAT-Key の生成するブロック数		10 進表記	[NumberOfBlocksToGenerateInKATKey = 24]
			NumberOfBlocksToGenerateInKATIV	KAT-IV の生成するブロック数		10 進表記	[NumberOfBlocksToGenerateInKATIV = 24]
			NumberOfBlocksToGenerateInKATTable	KAT-Table の生成するブロック数		10 進表記	[NumberOfBlocksToGenerateInKATTable = 3500]
			NumberOfInnerLoopsInMCT	MCT の内側ループの回数	$innerloop$	10 進表記	[NumberOfInnerLoopsInMCT = 1000]
			NumberOfOuterLoopsInMCT	MCT の外側ループの回数	$outerloop$	10 進表記	[NumberOfOuterLoopsInMCT = 100]
			NumberOfBlocksToGenerateInMCT	内側ループの中で生成する鍵系列のブロック数	N_b	10 進表記	[NumberOfBlocksToGenerateInMCT = 10000]
			NumberOfBlocksToCompareInMCT	レスポンスファイルに記録する鍵系列のブロック数	N_c	10 進表記	[NumberOfBlocksToCompareInMCT = 24]
	KAT-KEY	KAT-KEY ヘッダ	InitialIVForKATKey	入力となるビット列 IV		16 進表記	InitialIVForKATKey = 00. . .00
		KAT-KEY 本体 *1	COUNT	0 以上 128 以下の整数		10 進表記	COUNT = 0
			InitialKeyForKATKey	入力となるビット列 Key		16 進表記	InitialKeyForKATKey = fffc . . . 0000
			KeyStream	出力であるビット列		16 進表記	KeyStream = f871 . . . 3e30
	KAT-IV	KAT-IV ヘッダ	InitialKeyForKATIV	入力となるビット列 Key		16 進表記	InitialKeyForKATIV = 00. . .00
		KAT-IV 本体 *2	COUNT	0 以上 128 以下の整数		10 進表記	COUNT = 0
			InitialIVForKATIV	入力となるビット列 IV		16 進表記	InitialIVForKATIV = fffc . . . 0000
			KeyStream	出力であるビット列		16 進表記	KeyStream = f871 . . . 3e30
	KAT-Table	KAT-Table ヘッダ	Output Length (bits)	出力となるビット列のビット長		10 進表記	[Output Length (bits) = 224000]
		KAT-Table 本体	COUNT	0		10 進表記	COUNT = 0
			InitialKeyForKATTable	入力となるビット列 Key		16 進表記	InitialKeyForKATTable = 0000 . . . 0000
			InitialIVForKATTable	入力となるビット列 IV		16 進表記	InitialIVForKATTable = 0000 . . . 0000
			KeyStream	出力であるビット列		16 進表記	KeyStream = f871 . . . bca0
	MCT	MCT ヘッダ	InitialKeyForMCT	入力となるビット列 Key	Key	16 進表記	InitialKeyForMCT = e47a . . . dbc8
			InitialIVForMCT	入力となるビット列 IV	IV	16 進表記	InitialIVForMCT = 452c . . . aeed
		MCT 本体 *3	COUNT	0 以上 NumberOfOuterLoopsInMCT 未満の整数	j	10 進表記	COUNT = 0
			KeyStream	出力であるビット列	$j = \langle$ COUNT の値 $\rangle$ に対応する Y	16 進表記	KeyStream = 38f6 . . . a4a6

*1 129 個の各データの組を以下のように記述する.

```
COUNT = 0                           ♯ COUNT = 0 のデータの組について記述する.
InitialKeyForKATKey = 0000 ... 0000 ♯ COUNT = 0 に対応する Key を記述する.
KeyStream = f871 ... bca0           ♯ COUNT = 0 に対応する鍵系列の期待値を記述する.

COUNT = 1                           ♯ COUNT = 1 のデータの組について記述する.
InitialKeyForKATKey = 8000 ... 0000 ♯ COUNT = 1 に対応する Key を記述する.
KeyStream = f871 ... bca0           ♯ COUNT = 1 に対応する鍵系列の期待値を記述する.
.
.
.
COUNT = 128                         ♯ COUNT = 128 のデータの組について記述する.
InitialKeyForKATKey = ffff ... ffff ♯ COUNT = 128 に対応する Key を記述する.
KeyStream = f871 ... bca0           ♯ COUNT = 128 に対応する鍵系列の期待値を記述する.
```

*2 129 個の各データの組を以下のように記述する.

```
COUNT = 0                           ♯ COUNT = 0 のデータの組について記述する.
InitialIVForKATIV = 0000 ... 0000   ♯ COUNT = 0 に対応する IV を記述する.
KeyStream = f871 ... bca0           ♯ COUNT = 0 に対応する鍵系列の期待値を記述する.

COUNT = 1                           ♯ COUNT = 1 のデータの組について記述する.
InitialIVForKATIV = 8000 ... 0000   ♯ COUNT = 1 に対応する IV を記述する.
KeyStream = f871 ... bca0           ♯ COUNT = 1 に対応する鍵系列の期待値を記述する.
.
.
.
COUNT = 128                         ♯ COUNT = 128 のデータの組について記述する.
InitialIVForKATIV = ffff ... ffff   ♯ COUNT = 128 に対応する IV を記述する.
KeyStream = f871 ... bca0           ♯ COUNT = 128 に対応する鍵系列の期待値を記述する.
```

*3 NumberOfOuterLoopsInMCT 個の各データの組を以下のように記述する.

```
COUNT = 0                               ♯ j = 0 のデータの組について記述する.
KeyStream = 38f6 ... a4a6               ♯ j = 0 に対応する鍵系列の期待値を記述する.

COUNT = 1                               ♯ j = 1 のデータの組について記述する.
KeyStream = 38f6 ... a4a6               ♯ j = 1 に対応する鍵系列の期待値を記述する.
.
.
.
COUNT = ⟨ NumberOfOuterLoopsInMCT −1⟩   ♯ j = ⟨ NumberOfOuterLoopsInMCT −1⟩ のデータの組について記述する.
KeyStream = 38f6 ... a4a6               ♯ j = ⟨ NumberOfOuterLoopsInMCT −1⟩ に対応する鍵系列の期待値を記述する.
```

2.4 レスポンスファイル (*.rsp)

表4: KCipher-2 レスポンスファイル

機能	分類		タグ	内容	暗号アルゴリズム実装試験仕様書—共通鍵—上の表記との対応	値の表記	例示
擬似乱数生成機能	全体ヘッダ		AlgorithmName	KCipher-2		文字列	[AlgorithmName = KCipher-2]
			NumberOfBlocksToGenerateInKATKey	KAT-Key の生成するブロック数		10 進表記	[NumberOfBlocksToGenerateInKATKey = 24]
			NumberOfBlocksToGenerateInKATIV	KAT-IV の生成するブロック数		10 進表記	[NumberOfBlocksToGenerateInKATIV = 24]
			NumberOfBlocksToGenerateInKATTable	KAT-Table の生成するブロック数		10 進表記	[NumberOfBlocksToGenerateInKATTable = 3500]
			NumberOfInnerLoopsInMCT	MCT の内側ループの回数	$innerloop$	10 進表記	[NumberOfInnerLoopsInMCT = 1000]
			NumberOfOuterLoopsInMCT	MCT の外側ループの回数	$outerloop$	10 進表記	[NumberOfOuterLoopsInMCT = 100]
			NumberOfBlocksToGenerateInMCT	内側ループの中で生成する鍵系列のブロック数	N_b	10 進表記	[NumberOfBlocksToGenerateInMCT = 10000]
			NumberOfBlocksToCompareInMCT	レスポンスファイルに記録する鍵系列のブロック数	N_c	10 進表記	[NumberOfBlocksToCompareInMCT = 24]
	KAT-KEY	KAT-KEY ヘッダ	InitialIVForKATKey	入力となるビット列 IV		16 進表記	InitialIVForKATKey = 00. . .00
		KAT-KEY 本体 *1	COUNT	0 以上 128 以下の整数		10 進表記	COUNT = 0
			InitialKeyForKATKey	入力となるビット列 Key		16 進表記	InitialKeyForKATKey = fffc . . . 0000
			KeyStream	【出力】出力であるビット列		16 進表記	KeyStream = f871 . . . 3e30
	KAT-IV	KAT-IV ヘッダ	InitialKeyForKATIV	入力となるビット列 Key		16 進表記	InitialKeyForKATIV = 00. . .00
		KAT-IV 本体 *2	COUNT	0 以上 128 以下の整数		10 進表記	COUNT = 0
			InitialIVForKATIV	入力となるビット列 IV		16 進表記	InitialIVForKATIV = fffc . . . 0000
			KeyStream	【出力】出力であるビット列		16 進表記	KeyStream = f871 . . . 3e30
	KAT-Table	KAT-Table ヘッダ	Output Length (bits)	出力となるビット列のビット長		10 進表記	[Output Length (bits) = 224000]
		KAT-Table 本体	COUNT	0		10 進表記	COUNT = 0
			InitialKeyForKATTable	入力となるビット列 Key		16 進表記	InitialKeyForKATTable = 0000 . . . 0000
			InitialIVForKATTable	入力となるビット列 IV		16 進表記	InitialIVForKATTable = 0000 . . . 0000
			KeyStream	【出力】出力であるビット列		16 進表記	KeyStream = f871 . . . bca0
	MCT	MCT ヘッダ	InitialKeyForMCT	入力となるビット列 Key	Key	16 進表記	InitialKeyForMCT = e47a . . . dbc8
			InitialIVForMCT	入力となるビット列 IV	IV	16 進表記	InitialIVForMCT = 452c . . . aeed
		MCT 本体 *3	COUNT	0 以上 NumberOfOuterLoopsInMCT 未満の整数	j	10 進表記	COUNT = 0
			KeyStream	【出力】出力であるビット列	$j = \langle$ COUNT の値 $\rangle$ に対応する Y	16 進表記	KeyStream = 38f6 . . . a4a6

*1 129 個の各データの組を以下のように記述する.

```
COUNT = 0                            ♯ COUNT = 0 のデータの組について記述する.
InitialKeyForKATKey = 0000 ... 0000  ♯ COUNT = 0 に対応する Key を記述する.
KeyStream = f871 ... bca0            ♯ COUNT = 0 に対応する鍵系列.

COUNT = 1                            ♯ COUNT = 1 のデータの組について記述する.
InitialKeyForKATKey = 8000 ... 0000  ♯ COUNT = 1 に対応する Key を記述する.
KeyStream = f871 ... bca0            ♯ COUNT = 1 に対応する鍵系列.
.
.
.
COUNT = 128                          ♯ COUNT = 128 のデータの組について記述する.
InitialKeyForKATKey = ffff ... ffff  ♯ COUNT = 128 に対応する Key を記述する.
KeyStream = f871 ... bca0            ♯ COUNT = 128 に対応する鍵系列.
```

*2 129 個の各データの組を以下のように記述する.

```
COUNT = 0                            ♯ COUNT = 0 のデータの組について記述する.
InitialIVForKATIV = 0000 ... 0000    ♯ COUNT = 0 に対応する IV を記述する.
KeyStream = f871 ... bca0            ♯ COUNT = 0 に対応する鍵系列.

COUNT = 1                            ♯ COUNT = 1 のデータの組について記述する.
InitialIVForKATIV = 8000 ... 0000    ♯ COUNT = 1 に対応する IV を記述する.
KeyStream = f871 ... bca0            ♯ COUNT = 1 に対応する鍵系列.
.
.
.
COUNT = 128                          ♯ COUNT = 128 のデータの組について記述する.
InitialIVForKATIV = ffff ... ffff    ♯ COUNT = 128 に対応する IV を記述する.
KeyStream = f871 ... bca0            ♯ COUNT = 128 に対応する鍵系列.
```

*3 NumberOfOuterLoopsInMCT 個の各データの組を以下のように記述する.

```
COUNT = 0                                ♯ j = 0 のデータの組について記述する.
KeyStream = 38f6 ... a4a6                ♯ j = 0 に対応する鍵系列.

COUNT = 1                                ♯ j = 1 のデータの組について記述する.
KeyStream = 38f6 ... a4a6                ♯ j = 1 に対応する鍵系列.
.
.
.
COUNT = ⟨ NumberOfOuterLoopsInMCT −1⟩    ♯ j = ⟨ NumberOfOuterLoopsInMCT −1⟩ のデータの組について記述する.
KeyStream = 38f6 ... a4a6                ♯ j = ⟨ NumberOfOuterLoopsInMCT −1⟩ に対応する鍵系列.
```

2.5　結果ファイル (*.out)

表5: KCipher-2 結果ファイル

機能	分類		タグ	内容	値の表記	例示
擬似乱数生成機能	全体ヘッダ		AlgorithmName	KCipher-2	文字列	[AlgorithmName = KCipher-2]
			NumberOfBlocksToGenerateInKATKey	KAT-Key の生成するブロック数	10 進表記	[NumberOfBlocksToGenerateInKATKey = 24]
			NumberOfBlocksToGenerateInKATIV	KAT-IV の生成するブロック数	10 進表記	[NumberOfBlocksToGenerateInKATIV = 24]
			NumberOfBlocksToGenerateInKATTable	KAT-Table の生成するブロック数	10 進表記	[NumberOfBlocksToGenerateInKATTable = 3500]
			NumberOfInnerLoopsInMCT	MCT の内側ループの回数	10 進表記	[NumberOfInnerLoopsInMCT = 1000]
			NumberOfOuterLoopsInMCT	MCT の外側ループの回数	10 進表記	[NumberOfOuterLoopsInMCT = 100]
			NumberOfBlocksToGenerateInMCT	内側ループの中で生成する鍵系列のブロック数	10 進表記	[NumberOfBlocksToGenerateInMCT = 10000]
			NumberOfBlocksToCompareInMCT	レスポンスファイルに記録する鍵系列のブロック数	10 進表記	[NumberOfBlocksToCompareInMCT = 24]
	KAT-KEY	KAT-KEY ヘッダ	InitialIVForKATKey	入力となるビット列 IV	16 進表記	InitialIVForKATKey = 00...00
			⟨ Results ⟩	OK 又は NG	文字列	OK
	KAT-IV	KAT-IV ヘッダ	InitialKeyForKATIV	入力となるビット列 Key	16 進表記	InitialKeyForKATIV = 00...00
			⟨ Results ⟩	OK 又は NG	文字列	OK
	KAT-Table	KAT-Table ヘッダ	Output Length (bits)	出力となるビット列のビット長	10 進表記	[Output Length (bits) = 224000]
			⟨ Results ⟩	OK 又は NG	文字列	OK
	MCT	MCT ヘッダ	InitialKeyForMCT	入力となるビット列 Key	16 進表記	InitialKeyForMCT = e47a ... dbc8
			InitialIVForMCT	入力となるビット列 IV	16 進表記	InitialIVForMCT = 452c ... aeed
			⟨ Results ⟩	OK 又は NG	文字列	OK

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何番目 (COUNT，# 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．