

# JCATT ファイルフォーマット仕様書

## RSASSA-PKCS1-v1\_5

2008年4月11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>RSASSA-PKCS1-v1_5</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) . . . . .	7
2.5	結果ファイル (*.out) . . . . .	10

# 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 RSASSA-PKCS1-v1\_5

RSASSA-PKCS1-v1\_5 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．  
各表中，プライベート鍵識別子，公開鍵  $e$  識別子，ハッシュ関数識別子は下表の通りである．

表 1: プライベート鍵識別子

識別子	対応するプライベート鍵
TYPE1	プライベート鍵は $(p, q, dP, dQ, qInv)$
TYPE2	プライベート鍵は $(d, n)$

表 2: 公開鍵  $e$  識別子

識別子	対応する公開鍵 $e$
TYPE1	$e = 65, 537$
TYPE2	$e$ はランダム

表 3: 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_SHA256	SHA-256
M_Hash_SHA384	SHA-384
M_Hash_SHA512	SHA-512

## 2.1 パラメータファイル (\*.par)

表 4: RSASSA-PKCS1-v1\_5 パラメータファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSASSA-PKCS1-v1_5
署名生成	[Function Name]	Sign
	[Bitlength of Modulus]	法 $n$ のビット長
	[Hash]	ハッシュ関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 $e$ 識別子
	[Seed P]	ランダムな平文を生成するための擬似乱数生成関数用乱数シード
	[Bitlength of Seed P]	Seed P のビット長
	[Seed K]	鍵ペア生成のための擬似乱数生成用乱数シード
	[Bitlength of Seed K]	Seed K のビット長
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Plaintexts]	平文の数
署名検証	[Function Name]	Verification
	[Bitlength of Modulus]	署名生成と同じ
	[Hash]	
	[Secret Key Type]	
	[Public Key Type]	
	[Seed P]	
	[Bitlength of Seed P]	
	[Seed K]	
	[Bitlength of Seed K]	
	[Bitlength of Plaintexts]	
	[Number of Plaintexts]	
	[Rate of Fail Data]	署名検証が不合格になる割合
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of Modulus]	法 $n$ のビット長
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 $e$ 識別子
	[Number of Keys]	鍵の数

## 2.2 リクエストファイル (\*.req)

表 5: RSASSA-PKCS1-v1\_5 リクエストファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSASSA-PKCS1-v1_5
署名生成	[Function Name]	Sign
	[Bitlength of Modulus]	法 $n$ のビット長 [10 進数表記]
	[Hash]	ハッシュ関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[p] <sup>1</sup>	素数 $p$ [16 進数表記]
	[q] <sup>1</sup>	素数 $q$ [16 進数表記]
	[d] <sup>1</sup>	プライベート鍵 $d$ [16 進数表記]
	[n] <sup>1</sup>	法 $n$ [16 進数表記]
	[dP] <sup>1</sup>	$d \bmod p - 1$ [16 進数表記]
	[dQ] <sup>1</sup>	$d \bmod q - 1$ [16 進数表記]
	[qInv] <sup>1</sup>	$q^{-1} \bmod p$ [16 進数表記]
	[Bitlength of Plaintexts]	平文のビット長 [10 進数表記]
	[Number of Plaintexts]	平文の数 [10 進数表記]
	[Plaintexts] <sup>2</sup>	平文 [16 進数表記]
署名検証	[Function Name]	Verification
	[Bitlength of Modulus]	法 $n$ のビット長 [10 進数表記]
	[Hash]	ハッシュ関数識別子
	[n]	法 $n$ [16 進数表記]
	[Number of Signatures]	署名の数 [10 進数表記]
	[e] <sup>3</sup>	公開鍵 $e$ [16 進数表記]
	[Signatures] <sup>3</sup>	署名 [16 進数表記]
	[Bitlength of Plaintexts]	平文のビット長 [10 進数表記]
	[Plaintexts] <sup>3</sup>	平文 [16 進数表記]
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of Modulus]	法 $n$ のビット長 [10 進数表記]
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 $e$ 識別子
	[Number of Keys]	鍵の数 [10 進数表記]

### 注

1. プライベート鍵識別子に応じて,  $([d],[n])$  の組または  $([p],[q],[dP],[dQ],[qInv])$  の組いずれか一方を記述する.
2. [Number of Plaintexts] 個の平文を記述する.
3. [Number of Signatures] 個の公開鍵  $e$ , 署名および平文を記述する.

## 2.3 Facts ファイル (\*.fax)

表 6: RSASSA-PKCS1-v1\_5 Facts ファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSASSA-PKCS1-v1_5
署名生成	[Function Name]	Sign
	[Bitlength of Modulus]	法 $n$ のビット長
	[Hash]	ハッシュ関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 $e$ 識別子
	[p] <sup>1</sup>	素数 $p$
	[q] <sup>1</sup>	素数 $q$
	[d] <sup>1</sup>	プライベート鍵 $d$
	[n] <sup>1</sup>	法 $n$
	[dP] <sup>1</sup>	$d \bmod p - 1$
	[dQ] <sup>1</sup>	$d \bmod q - 1$
	[qInv] <sup>1</sup>	$q^{-1} \bmod p$
	[e]	公開鍵 $e$
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Plaintexts]	平文の数
	[Plaintexts] <sup>2</sup>	平文
	[Signatures] <sup>2</sup>	署名

### 注

1. プライベート鍵識別子に応じて,  $([d],[n])$  の組または  $([p],[q],[n],[dP],[dQ],[qInv])$  の組いずれか一方を記述する .
2. [Number of Plaintexts] 個の平文および署名を記述する .

表 7: RSASSA-PKCS1-v1\_5 Facts ファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSASSA-PKCS1-v1_5
署名検証	[Function Name]	Verification
	[Bitlength of Modulus]	法 $n$ のビット長
	[Hash]	ハッシュ関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 $e$ 識別子
	$[p]^1$	素数 $p$
	$[q]^1$	素数 $q$
	$[d]^1$	プライベート鍵 $d$
	$[n]^1$	法 $n$
	$[dP]^1$	$d \bmod p - 1$
	$[dQ]^1$	$d \bmod q - 1$
	$[qInv]^1$	$q^{-1} \bmod p$
	[Number of Signatures]	署名の数
	$[e]^2$	公開鍵 $e$
	[Signatures] <sup>2</sup>	署名
	[Bitlength of Plaintexts]	平文のビット長
	[Plaintexts] <sup>2</sup>	平文
	[Results] <sup>2</sup>	署名検証結果．署名検証合格の場合 0 , 不合格の場合 1 と記述する．[Signatures] および [Plaintexts] に記述した検証対象署名および平文の順に 1 または 0 を記述すること．
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of Modulus]	法 $n$ のビット長
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 $e$ 識別子
	[Number of Keys]	鍵の数

## 注

1. プライベート鍵識別子に応じて ,  $([d],[n])$  の組または  $([p],[q],[n],[dP],[dQ],[qInv])$  の組いずれか一方を記述する．
2. [Number of Signatures] 個の公開鍵  $e$  , 署名 , 平文 , および署名検証結果を記述する．



## 2.4 レスポンスファイル (\*.rsp)

表 8: RSASSA-PKCS1-v1\_5 レスポンスファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSASSA-PKCS1-v1_5
署名生成	[Function Name]	Sign
	[Bitlength of Modulus]	法 $n$ のビット長 [10 進数表記]
	[Hash]	ハッシュ関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[p] <sup>1</sup>	素数 $p$ [16 進数表記]
	[q] <sup>1</sup>	素数 $q$ [16 進数表記]
	[d] <sup>1</sup>	プライベート鍵 $d$ [16 進数表記]
	[n] <sup>1</sup>	法 $n$ [16 進数表記]
	[dP] <sup>1</sup>	$d \bmod p - 1$ [16 進数表記]
	[dQ] <sup>1</sup>	$d \bmod q - 1$ [16 進数表記]
	[qInv] <sup>1</sup>	$q^{-1} \bmod p$ [16 進数表記]
	[Bitlength of Plaintexts]	平文のビット長 [10 進数表記]
	[Number of Plaintexts]	平文の数 [10 進数表記]
	[Plaintexts] <sup>2</sup>	平文 [16 進数表記]
	[Signatures] <sup>2</sup>	【出力】署名 [16 進数表記]
署名検証	[Function Name]	Verification
	[Bitlength of Modulus]	法 $n$ のビット長 [10 進数表記]
	[Hash]	ハッシュ関数識別子
	[n]	法 $n$ [16 進数表記]
	[Number of Signatures]	署名の数 [10 進数表記]
	[e] <sup>3</sup>	公開鍵 $e$ [16 進数表記]
	[Signatures] <sup>3</sup>	署名 [16 進数表記]
	[Bitlength of Plaintexts]	平文のビット長 [10 進数表記]
	[Plaintexts] <sup>3</sup>	平文 [16 進数表記]
	[Results] <sup>3</sup>	【出力】署名検証結果．検証合格の時 0，不合格の時 1 と記述する．

### 注

1. プライベート鍵識別子に応じて， $([d],[n])$  の組または  $([p],[q],[dP],[dQ],[qInv])$  の組いずれか一方を記述する．
2. [Number of Plaintexts] 個の平文および署名を記述する．
3. [Number of Signatures] 個の公開鍵  $e$ ，署名，平文，および署名検証結果を記述する．

表 9: RSASSA-PKCS1-v1\_5 レスポンスファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSASSA-PKCS1-v1_5
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of Modulus]	法 $n$ のビット長 [10 進数表記]
	[Secret Key Type]	プライベート鍵識別子
	[Number of Keys]	鍵の数 [10 進数表記]
	$[p]^1$	【出力】素数 $p$ [16 進数表記]
	$[q]^1$	【出力】素数 $q$ [16 進数表記]
	$[d]^1$	【出力】プライベート鍵 $d$ [16 進数表記]
	$[e]^1$	【出力】公開鍵 $e$ [16 進数表記]
	$[n]^1$	【出力】法 $n$ [16 進数表記]
	$[dP]^1$	【出力】 $d \bmod p - 1$ [16 進数表記]
	$[dQ]^1$	【出力】 $d \bmod q - 1$ [16 進数表記]
	$[qInv]^1$	【出力】 $q^{-1} \bmod p$ [16 進数表記]

## 注

1. プライベート鍵のタイプに応じて、 $([p], [q], [d], [e], [n])$  の組または  $([p], [q], [dP], [dQ], [qInv], [e], [n])$  の組いずれか一方を [Number of Keys] 個記述する。

プライベート鍵識別子に TYPE1 が指定されているとき、鍵  $([p], [q], [dP], [dQ], [qInv], [e], [n])$  は次の例に従って記述すること。すなわち、2 組以上の鍵を記述する時は、まず 1 組目の  $([p], [q], [dP], [dQ], [qInv], [e], [n])$  をこの順番で記述し、次に 2 組目の  $([p], [q], [dP], [dQ], [qInv], [e], [n])$  をこの順番で記述する。(以降同様)

$[p]$   
... # 1 組目の素数  $p$  を記述する。

$[q]$   
... # 1 組目の素数  $q$  を記述する。

$[dP]$   
... # 1 組目の  $d \bmod p - 1$  を記述する。

$[dQ]$   
... # 1 組目の  $d \bmod q - 1$  を記述する。

$[qInv]$   
... # 1 組目の  $q^{-1} \bmod p$  を記述する。

$[e]$   
... # 1 組目の公開鍵  $e$  を記述する。

$[n]$   
... # 1 組目の法  $n$  を記述する。

$[p]$   
... # 2 組目の素数  $p$  を記述する。

$[q]$   
... # 2 組目の素数  $q$  を記述する。

$[dP]$   
... # 2 組目の  $d \bmod p - 1$  を記述する。

[dQ]  
... # 2 組目の  $d \bmod q - 1$  を記述する .

[qInv]  
... # 2 組目の  $q^{-1} \bmod p$  を記述する .

[e]  
... # 2 組目の公開鍵  $e$  を記述する .

[n]  
... # 2 組目の法  $n$  を記述する .

## 2.5 結果ファイル (\*.out)

表 10: RSASSA-PKCS1-v1\_5 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．
- 鍵ペア生成機能に対する試験において試験不合格の場合，下記のようにどの条件が合格 (ok) でどの条件が不合格 (NG) となったかも表示される．  
NG(#1 : p is prime ?)  
ok(#1 : q is prime ?)  
例えば，ok(#1 : q is prime ?) は， $q$  は素数であるという条件を満たしていることを示し，NG(#1 : p is prime ?) は， $p$  は素数であるという条件を満たしていないことを示す．詳細は別紙の試験項目を記述した文書を参照のこと．