JCATT ファイルフォーマット仕様書

決定論的乱数生成器 NIST SP800-90A

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

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　決定論的乱数生成器 NIST SP800-90A

NIST SP800-90A に記載された決定論的乱数生成器 Hash_DRBG, HMAC_DRBG, CTR_DRBG with DF, CTR_DRBG without DF 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．これらの決定論的乱数生成器に対するフォーマットは, Algorithm Name を除いて同じである．

Algorithm Name は, それぞれ下記の通り．

- `Hash_DRBG`
- `HMAC_DRBG`
- `CTR_DRBG use DF`
- `CTR_DRBG no DF`

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．

Hash_DRBG を選択時, 暗号プリミティブ識別子は, 表1に記載された通りである．

表1　暗号プリミティブ識別子 (Hash_DRBG 選択時)

暗号プリミティブ識別子	対応するハッシュ関数
SHA-1	`SHA-1`
SHA-224	`SHA-224`
SHA-256	`SHA-256`
SHA-384	`SHA-384`
SHA-512	`SHA-512`
SHA-512/224	`SHA-512/224`
SHA-512/256	`SHA-512/256`

HMAC_DRBG を選択時, 暗号プリミティブ識別子は, 表2に記載された通りである．

表2　暗号プリミティブ識別子 (HMAC_DRBG 選択時)

暗号プリミティブ識別子	対応するハッシュ関数
SHA-1	`SHA-1`
SHA-224	`SHA-224`
SHA-256	`SHA-256`
SHA-384	`SHA-384`
SHA-512	`SHA-512`
SHA-512/224	`SHA-512/224`
SHA-512/256	`SHA-512/256`

CTR_DRBG with DF (`CTR_DRBG use DF`) 又は CTR_DRBG without DF(`CTR_DRBG no DF`) を選択時, 暗号プリミティブ識別子は, 表3に記載された通りである．

表3　暗号プリミティブ識別子 (`CTR_DRBG use DF` 又は `CTR_DRBG no DF` 選択時)

暗号プリミティブ識別子	対応するブロック暗号
AES-128	`AES-128`
AES-192	`AES-192`
AES-256	`AES-256`

2.1 パラメータファイル (*.par)

表4 決定論的乱数生成器 NIST SP800-90A パラメータファイル

機能	タグ		内容	表記
全機能試験	全体ヘッダ	AlgorithmName	(乱数生成器名)	文字列
		UnderlyingAlgorithm	暗号プリミティブ関数識別子	文字列
		SecurityStrength	セキュリティ強度	10 進
		WithReseedCapability	Reseed 機能の有無 (有:True, 無:False)	文字列
		PredictionResistance	Prediction resistance の有効化の有無 (有:True, 無:False)	文字列
		EntropyInputLen	*entropy_input* のビット長	10 進
		NonceLen	*nonce* のビット長	10 進
		PersonalizationStringMinLen	*personalization_string* のビット長 · 最小値	10 進
		PersonalizationStringMaxLen	*personalization_string* のビット長 · 最大値	10 進
		AdditionalInputMinLen	*additional_input* のビット長 · 最小値	10 進
		AdditionalInputMaxLen	*additional_input* のビット長 · 最大値	10 進
		RequestedNumberOfBits	1 回で生成する乱数のビット長	10 進
		NumberOfTrials	DRBG インスタンスを生成する回数	10 進

2.2 リクエストファイル (*.req)

表5: NIST SP800-90A に記載された HMAC_DRBG, Hash_DRBG, 及び CTR_DRBG

機能	分類	タグ	内容	暗号アルゴリズム実装試験仕様書—乱数生成器—上の表記との対応	値の表記	例示
全機能試験	全体ヘッダ	AlgorithmName	乱数生成器名. 次のいずれかを選択: HMAC_DRBG, Hash_DRBG, CTR_DRBG use df, CTR_DRBG no df		文字列	[AlgorithmName = HMAC_DRBG]
		UnderlyingAlgorithm	暗号プリミティブ識別子. HMAC_DRBG 又は Hash_DRBG の選択時, 次のいずれかを選択: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. CTR_DRBG use df 又は CTR_DRBG no df の選択時, 次のいずれかを選択: AES-128, AES-192, AES-256		文字列	[UnderlyingAlgorithm = SHA-256]
		SecurityStrength	セキュリティ強度	*strength*	10 進	[SecurityStrength = 256]
		WithReseedCapability	Reseed 機能の有無 (有:True, 無:False)		文字列	[WithReseedCapability = True]
		PredictionResistance	Prediction resistance の有効化の有無 (有:True, 無:False)		文字列	[PredictionResistance = True]
		EntropyInputLen	*entropy_input* のビット長		10 進表記	[EntropyInputLen = 512]
		NonceLen	*nonce* のビット長		10 進表記	[NonceLen = 128]
		PersonalizationStringMinLen	*personalization_string* のビット長の最小値		10 進表記	[PersonalizationStringMinLen = 0]
		PersonalizationStringMaxLen	*personalization_string* のビット長の最大値		10 進表記	[PersonalizationStringMaxLen = 2048]
		AdditionalInputMinLen	*additional_input* のビット長の最小値		10 進表記	[AdditionalInputMinLen = 0]
		AdditionalInputMaxLen	*additional_input* のビット長の最大値		10 進表記	[AdditionalInputMaxLen = 2048]
		RequestedNumberOfBits	*returned_bits* のビット長	*requested_number_of_bits*	10 進表記	[RequestedNumberOfBits = 512]
		NumberOfTrials	DRBG インスタンスを生成する回数	*number_of_trials*	10 進表記	[NumberOfTrials = 100]
	試験 1 *1 / 試験 1 ヘッダ	⟨UnderlyingAlgorithm の値⟩	共通ヘッダ UnderlyingAlgorithm の値 (CTR_DRBG の選択時, 導出関数の有の場合 " use df" を, 無の場合 " no df" を付加)		文字列	[HMAC-SHA-512/224]
		PredictionResistance	PredictionResistance を有効にする場合 True, 無効にする場合 False		文字列	[PredictionResistance = True]
		EntropyInputLen	*entropy_input* のビット長		10 進表記	[EntropyInputLen = 512]
		NonceLen	*nonce* のビット長		10 進表記	[NonceLen = 128]
		PersonalizationStringLen	*personalization_string* のビット長		10 進表記	[PersonalizationStringLen = 2048]
		AdditionalInputLen	*additional_input* のビット長		10 進表記	[AdditionalInputLen = 2048]
	試験 1 本体 *2	COUNT	0 以上 NumberOfTrials 未満の整数	i	10 進表記	COUNT = 0
		EntropyInput	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $entropy\_input_i$	16 進表記	EntropyInput = 0102 . . . 3f40
		Nonce	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $nonce_i$	16 進表記	Nonce = 0102 . . . 0f10
		PersonalizationString	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $personalization\_string_i$	16 進表記	PersonalizationString = 0102 . . . ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 . . . ff00
		EntropyInputPR	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $entropy\_input\_PR_{i,j}$	16 進表記	EntropyInputPR = 0102 . . . 3f40
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 . . . ff00
		EntropyInputPR	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $entropy\_input\_PR_{i,j}$	16 進表記	EntropyInputPR = 0102 . . . 3f40
		ReturnedBits	Generate 関数の出力であるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $pseudorandom\_bits_{i,j}$	16 進表記	ReturnedBits = ?
	試験 2 *1 / 試験 2 ヘッダ	⟨UnderlyingAlgorithm の値⟩	共通ヘッダ UnderlyingAlgorithm の値 (CTR_DRBG の選択時, 導出関数の有の場合 " use df" を, 無の場合 " no df" を付加)		文字列	[HMAC-SHA-512/224]
		PredictionResistance	PredictionResistance を有効にする場合 True, 無効にする場合 False		文字列	[PredictionResistance = False]
		EntropyInputLen	*entropy_input* のビット長		10 進表記	[EntropyInputLen = 512]
		NonceLen	*nonce* のビット長		10 進表記	[NonceLen = 128]
		PersonalizationStringLen	*personalization_string* のビット長		10 進表記	[PersonalizationStringLen = 2048]
		AdditionalInputLen	*additional_input* のビット長		10 進表記	[AdditionalInputLen = 2048]
	試験 2 本体 *3	COUNT	0 以上 NumberOfTrials 未満の整数	i	10 進表記	COUNT = 0
		EntropyInput	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $entropy\_input_i$	16 進表記	EntropyInput = 0102 . . . 3f40
		Nonce	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $nonce_i$	16 進表記	Nonce = 0102 . . . 0f10
		PersonalizationString	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $personalization\_string_i$	16 進表記	PersonalizationString = 0102 . . . ff00
		EntropyInputReseed	Reseed 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $entropy\_input\_on\_reseed_{i,j}$	16 進表記	EntropyInputReseed = 0102 . . . 3f40
		AdditionalInputReseed	Reseed 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $additional\_input\_on\_reseed_{i,j}$	16 進表記	AdditionalInputReseed = 0102 . . . ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 . . . ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 2$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 . . . ff00
		ReturnedBits	Generate 関数の出力であるビット列	$i = \langle$COUNT の値$\rangle$, $j = 2$ に対応する $pseudorandom\_bits_{i,j}$	16 進表記	ReturnedBits = ?
	試験 3 *1 / 試験 3 ヘッダ	⟨UnderlyingAlgorithm の値⟩	共通ヘッダ UnderlyingAlgorithm の値 (CTR_DRBG の選択時, 導出関数の有の場合 " use df" を, 無の場合 " no df" を付加)		文字列	[HMAC-SHA-512/224]
		PredictionResistance	PredictionResistance を有効にする場合 True, 無効にする場合 False		文字列	[PredictionResistance = False]
		EntropyInputLen	*entropy_input* のビット長		10 進表記	[EntropyInputLen = 512]
		NonceLen	*nonce* のビット長		10 進表記	[NonceLen = 128]
		PersonalizationStringLen	*personalization_string* のビット長		10 進表記	[PersonalizationStringLen = 2048]
		AdditionalInputLen	*additional_input* のビット長		10 進表記	[AdditionalInputLen = 2048]
	試験 3 本体 *4	COUNT	0 以上 NumberOfTrials 未満の整数	i	10 進表記	COUNT = 0
		EntropyInput	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $entropy\_input_i$	16 進表記	EntropyInput = 0102 . . . 3f40
		Nonce	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $nonce_i$	16 進表記	Nonce = 0102 . . . 0f10
		PersonalizationString	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $personalization\_string_i$	16 進表記	PersonalizationString = 0102 . . . ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 . . . ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 . . . ff00
		ReturnedBits	Generate 関数の出力であるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $pseudorandom\_bits_{i,j}$	16 進表記	ReturnedBits = ?

*1 WithReseedCapability 及び PredictionResistance の値の組みあわせに対応して, 試験 1, 試験 2, 又は試験 3 のいずれか 1 つが選択される. その上で, PersonalizationStringMinLen, PersonalizationStringMaxLen, AdditionalInputMinLen 及び AdditionalInputMaxLen の値の組みあわせに対応して, 1〜4 回, 選択された試験 1, 試験 2, 又は試験 3 を記述する.

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

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
EntropyInput = 0102 ... 3f40       ♯ i = 0 に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10              ♯ i = 0 に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00   ♯ i = 0 に対応する personalization_string_i を記述する.
AdditionalInput = 0102 ... ff00    ♯ i = 0, j = 0 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40     ♯ i = 0, j = 0 に対応する entropy_input_PR_{i,j} を記述する.
AdditionalInput = 0102 ... ff00    ♯ i = 0, j = 1 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40     ♯ i = 0, j = 1 に対応する entropy_input_PR_{i,j} を記述する.
ReturnedBits = ?                   ♯ i = 0, j = 1 に対応する pseudorandom_bits_{i,j} のプレースホルダ.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
EntropyInput = 0102 ... 3f40       ♯ i = 1 に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10              ♯ i = 1 に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00   ♯ i = 1 に対応する personalization_string_i を記述する.
AdditionalInput = 0102 ... ff00    ♯ i = 1, j = 0 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40     ♯ i = 1, j = 0 に対応する entropy_input_PR_{i,j} を記述する.
AdditionalInput = 0102 ... ff00    ♯ i = 1, j = 1 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40     ♯ i = 1, j = 1 に対応する entropy_input_PR_{i,j} を記述する.
ReturnedBits = ?                   ♯ i = 1, j = 1 に対応する pseudorandom_bits_{i,j} のプレースホルダ.

.
.
.
COUNT = ⟨ NumberOfTrials −1⟩       ♯ i = ⟨ NumberOfTrials −1⟩ のデータの組について記述する.
EntropyInput = 0102 ... 3f40       ♯ i = ⟨ NumberOfTrials −1⟩ に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10              ♯ i = ⟨ NumberOfTrials −1⟩ に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00   ♯ i = ⟨ NumberOfTrials −1⟩ に対応する personalization_string_i を記述する.
AdditionalInput = 0102 ... ff00    ♯ i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40     ♯ i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する entropy_input_PR_{i,j} を記述する.
AdditionalInput = 0102 ... ff00    ♯ i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40     ♯ i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する entropy_input_PR_{i,j} を記述する.
ReturnedBits = ?                   ♯ i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する pseudorandom_bits_{i,j} のプレースホルダ.
```

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

```
COUNT = 0                              ♯ i = 0 のデータの組について記述する．
EntropyInput = 0102 ... 3f40           ♯ i = 0 に対応する entropy_input_i を記述する．
Nonce = 0102 ... 0f10                  ♯ i = 0 に対応する nonce_i を記述する．
PersonalizationString = 0102 ... ff00  ♯ i = 0 に対応する personalization_string_i を記述する．
EntropyInputReseed = 0102 ... 3f40     ♯ i = 0, j = 0 に対応する entropy_input_on_reseed_{i,j} を記述する．
AdditionalInputReseed = 0102 ... ff00  ♯ i = 0, j = 0 に対応する additional_input_on_reseed_{i,j} を記述する．
AdditionalInput = 0102 ... ff00        ♯ i = 0, j = 1 に対応する additional_input_{i,j} を記述する．
AdditionalInput = 0102 ... ff00        ♯ i = 0, j = 2 に対応する additional_input_{i,j} を記述する．
ReturnedBits = ?                       ♯ i = 0, j = 2 に対応する pseudorandom_bits_{i,j} のプレースホルダ．

COUNT = 1                              ♯ i = 1 のデータの組について記述する．
EntropyInput = 0102 ... 3f40           ♯ i = 1 に対応する entropy_input_i を記述する．
Nonce = 0102 ... 0f10                  ♯ i = 1 に対応する nonce_i を記述する．
PersonalizationString = 0102 ... ff00  ♯ i = 1 に対応する personalization_string_i を記述する．
EntropyInputReseed = 0102 ... 3f40     ♯ i = 1, j = 0 に対応する entropy_input_on_reseed_{i,j} を記述する．
AdditionalInputReseed = 0102 ... ff00  ♯ i = 1, j = 0 に対応する additional_input_on_reseed_{i,j} を記述する．
AdditionalInput = 0102 ... ff00        ♯ i = 1, j = 1 に対応する additional_input_{i,j} を記述する．
AdditionalInput = 0102 ... ff00        ♯ i = 1, j = 2 に対応する additional_input_{i,j} を記述する．
ReturnedBits = ?                       ♯ i = 1, j = 2 に対応する pseudorandom_bits_{i,j} のプレースホルダ．
.
.
.
COUNT = ⟨ NumberOfTrials −1⟩           ♯ i = ⟨ NumberOfTrials −1⟩ のデータの組について記述する．
EntropyInput = 0102 ... 3f40           ♯ i = ⟨ NumberOfTrials −1⟩ に対応する entropy_input_i を記述する．
Nonce = 0102 ... 0f10                  ♯ i = ⟨ NumberOfTrials −1⟩ に対応する nonce_i を記述する．
PersonalizationString = 0102 ... ff00  ♯ i = ⟨ NumberOfTrials −1⟩ に対応する personalization_string_i を記述する．
EntropyInputReseed = 0102 ... 3f40     ♯ i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する entropy_input_on_reseed_{i,j} を記述する．
AdditionalInputReseed = 0102 ... ff00  ♯ i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する additional_input_on_reseed_{i,j} を記述する．
AdditionalInput = 0102 ... ff00        ♯ i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する additional_input_{i,j} を記述する．
AdditionalInput = 0102 ... ff00        ♯ i = ⟨ NumberOfTrials −1⟩, j = 2 に対応する additional_input_{i,j} を記述する．
ReturnedBits = ?                       ♯ i = ⟨ NumberOfTrials −1⟩, j = 2 に対応する pseudorandom_bits_{i,j} のプレースホルダ．
```

∗4 NumberOfTrials 個の各データの組を以下のように記述する．

```
COUNT = 0                              ♯ i = 0 のデータの組について記述する．
EntropyInput = 0102 ... 3f40           ♯ i = 0 に対応する entropy_input_i を記述する．
Nonce = 0102 ... 0f10                  ♯ i = 0 に対応する nonce_i を記述する．
PersonalizationString = 0102 ... ff00  ♯ i = 0 に対応する personalization_string_i を記述する．
AdditionalInput = 0102 ... ff00        ♯ i = 0, j = 0 に対応する additional_input_{i,j} を記述する．
AdditionalInput = 0102 ... ff00        ♯ i = 0, j = 1 に対応する additional_input_{i,j} を記述する．
ReturnedBits = ?                       ♯ i = 0, j = 1 に対応する pseudorandom_bits_{i,j} のプレースホルダ．

COUNT = 1                              ♯ i = 1 のデータの組について記述する．
EntropyInput = 0102 ... 3f40           ♯ i = 1 に対応する entropy_input_i を記述する．
Nonce = 0102 ... 0f10                  ♯ i = 1 に対応する nonce_i を記述する．
PersonalizationString = 0102 ... ff00  ♯ i = 1 に対応する personalization_string_i を記述する．
AdditionalInput = 0102 ... ff00        ♯ i = 1, j = 0 に対応する additional_input_{i,j} を記述する．
AdditionalInput = 0102 ... ff00        ♯ i = 1, j = 1 に対応する additional_input_{i,j} を記述する．
ReturnedBits = ?                       ♯ i = 1, j = 1 に対応する pseudorandom_bits_{i,j} のプレースホルダ．
.
.
.
COUNT = ⟨ NumberOfTrials −1⟩           ♯ i = ⟨ NumberOfTrials −1⟩ のデータの組について記述する．
EntropyInput = 0102 ... 3f40           ♯ i = ⟨ NumberOfTrials −1⟩ に対応する entropy_input_i を記述する．
Nonce = 0102 ... 0f10                  ♯ i = ⟨ NumberOfTrials −1⟩ に対応する nonce_i を記述する．
PersonalizationString = 0102 ... ff00  ♯ i = ⟨ NumberOfTrials −1⟩ に対応する personalization_string_i を記述する．
AdditionalInput = 0102 ... ff00        ♯ i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する additional_input_{i,j} を記述する．
AdditionalInput = 0102 ... ff00        ♯ i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する additional_input_{i,j} を記述する．
ReturnedBits = ?                       ♯ i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する pseudorandom_bits_{i,j} のプレースホルダ．
```

2.3 Facts ファイル (*.fax)

表6: NIST SP800-90A に記載された HMAC_DRBG, Hash_DRBG, 及び CTR_DRBG

機能	分類	タグ	内容	暗号アルゴリズム実装試験仕様書—乱数生成器—上の表記との対応	値の表記	例示
全機能試験	全体ヘッダ	AlgorithmName	乱数生成器名. 次のいずれかを選択: HMAC_DRBG, Hash_DRBG, CTR_DRBG use df, CTR_DRBG no df		文字列	[AlgorithmName = HMAC_DRBG]
		UnderlyingAlgorithm	暗号プリミティブ識別子. HMAC_DRBG 又は Hash_DRBG の選択時, 次のいずれかを選択: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. CTR_DRBG use df 又は CTR_DRBG no df の選択時, 次のいずれかを選択: AES-128, AES-192, AES-256		文字列	[UnderlyingAlgorithm = SHA-256]
		SecurityStrength	セキュリティ強度	*strength*	10 進	[SecurityStrength = 256]
		WithReseedCapability	Reseed 機能の有無 (有:True, 無:False)		文字列	[WithReseedCapability = True]
		PredictionResistance	Prediction resistance の有効化の有無 (有:True, 無:False)		文字列	[PredictionResistance = True]
		EntropyInputLen	*entropy_input* のビット長		10 進表記	[EntropyInputLen = 512]
		NonceLen	*nonce* のビット長		10 進表記	[NonceLen = 128]
		PersonalizationStringMinLen	*personalization_string* のビット長の最小値		10 進表記	[PersonalizationStringMinLen = 0]
		PersonalizationStringMaxLen	*personalization_string* のビット長の最大値		10 進表記	[PersonalizationStringMaxLen = 2048]
		AdditionalInputMinLen	*additional_input* のビット長の最小値		10 進表記	[AdditionalInputMinLen = 0]
		AdditionalInputMaxLen	*additional_input* のビット長の最大値		10 進表記	[AdditionalInputMaxLen = 2048]
		RequestedNumberOfBits	*returned_bits* のビット長	*requested_number_of_bits*	10 進表記	[RequestedNumberOfBits = 512]
		NumberOfTrials	DRBG インスタンスを生成する回数	*number_of_trials*	10 進表記	[NumberOfTrials = 100]
	試験 1 *1 / 試験 1 ヘッダ	⟨UnderlyingAlgorithm の値⟩	共通ヘッダ UnderlyingAlgorithm の値 (CTR_DRBG の選択時, 導出関数の有の場合 " use df" を, 無の場合 " no df" を付加)		文字列	[HMAC-SHA-512/224]
		PredictionResistance	PredictionResistance を有効にする場合 True, 無効にする場合 False		文字列	[PredictionResistance = True]
		EntropyInputLen	*entropy_input* のビット長		10 進表記	[EntropyInputLen = 512]
		NonceLen	*nonce* のビット長		10 進表記	[NonceLen = 128]
		PersonalizationStringLen	*personalization_string* のビット長		10 進表記	[PersonalizationStringLen = 2048]
		AdditionalInputLen	*additional_input* のビット長		10 進表記	[AdditionalInputLen = 2048]
	試験 1 本体 *2	COUNT	0 以上 NumberOfTrials 未満の整数	i	10 進表記	COUNT = 0
		EntropyInput	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $entropy\_input_i$	16 進表記	EntropyInput = 0102 ... 3f40
		Nonce	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $nonce_i$	16 進表記	Nonce = 0102 ... 0f10
		PersonalizationString	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $personalization\_string_i$	16 進表記	PersonalizationString = 0102 ... ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 ... ff00
		EntropyInputPR	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $entropy\_input\_PR_{i,j}$	16 進表記	EntropyInputPR = 0102 ... 3f40
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 ... ff00
		EntropyInputPR	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $entropy\_input\_PR_{i,j}$	16 進表記	EntropyInputPR = 0102 ... 3f40
		ReturnedBits	Generate 関数の出力であるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $pseudorandom\_bits_{i,j}$	16 進表記	ReturnedBits = 3afb ... d291
	試験 2 *1 / 試験 2 ヘッダ	⟨UnderlyingAlgorithm の値⟩	共通ヘッダ UnderlyingAlgorithm の値 (CTR_DRBG の選択時, 導出関数の有の場合 " use df" を, 無の場合 " no df" を付加)		文字列	[HMAC-SHA-512/224]
		PredictionResistance	PredictionResistance を有効にする場合 True, 無効にする場合 False		文字列	[PredictionResistance = False]
		EntropyInputLen	*entropy_input* のビット長		10 進表記	[EntropyInputLen = 512]
		NonceLen	*nonce* のビット長		10 進表記	[NonceLen = 128]
		PersonalizationStringLen	*personalization_string* のビット長		10 進表記	[PersonalizationStringLen = 2048]
		AdditionalInputLen	*additional_input* のビット長		10 進表記	[AdditionalInputLen = 2048]
	試験 2 本体 *3	COUNT	0 以上 NumberOfTrials 未満の整数	i	10 進表記	COUNT = 0
		EntropyInput	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $entropy\_input_i$	16 進表記	EntropyInput = 0102 ... 3f40
		Nonce	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $nonce_i$	16 進表記	Nonce = 0102 ... 0f10
		PersonalizationString	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $personalization\_string_i$	16 進表記	PersonalizationString = 0102 ... ff00
		EntropyInputReseed	Reseed 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $entropy\_input\_on\_reseed_{i,j}$	16 進表記	EntropyInputReseed = 0102 ... 3f40
		AdditionalInputReseed	Reseed 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $additional\_input\_on\_reseed_{i,j}$	16 進表記	AdditionalInputReseed = 0102 ... ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 ... ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 2$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 ... ff00
		ReturnedBits	Generate 関数の出力であるビット列	$i = \langle$COUNT の値$\rangle$, $j = 2$ に対応する $pseudorandom\_bits_{i,j}$	16 進表記	ReturnedBits = 3afb ... d291
	試験 3 *1 / 試験 3 ヘッダ	⟨UnderlyingAlgorithm の値⟩	共通ヘッダ UnderlyingAlgorithm の値 (CTR_DRBG の選択時, 導出関数の有の場合 " use df" を, 無の場合 " no df" を付加)		文字列	[HMAC-SHA-512/224]
		PredictionResistance	PredictionResistance を有効にする場合 True, 無効にする場合 False		文字列	[PredictionResistance = False]
		EntropyInputLen	*entropy_input* のビット長		10 進表記	[EntropyInputLen = 512]
		NonceLen	*nonce* のビット長		10 進表記	[NonceLen = 128]
		PersonalizationStringLen	*personalization_string* のビット長		10 進表記	[PersonalizationStringLen = 2048]
		AdditionalInputLen	*additional_input* のビット長		10 進表記	[AdditionalInputLen = 2048]
	試験 3 本体 *4	COUNT	0 以上 NumberOfTrials 未満の整数	i	10 進表記	COUNT = 0
		EntropyInput	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $entropy\_input_i$	16 進表記	EntropyInput = 0102 ... 3f40
		Nonce	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $nonce_i$	16 進表記	Nonce = 0102 ... 0f10
		PersonalizationString	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $personalization\_string_i$	16 進表記	PersonalizationString = 0102 ... ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 ... ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 ... ff00
		ReturnedBits	Generate 関数の出力であるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $pseudorandom\_bits_{i,j}$	16 進表記	ReturnedBits = 3afb ... d291

*1 WithReseedCapability 及び PredictionResistance の値の組みあわせに対応して, 試験 1, 試験 2, 又は試験 3 のいずれか 1 つが選択される. その上で, PersonalizationStringMinLen, PersonalizationStringMaxLen, AdditionalInputMinLen 及び AdditionalInputMaxLen の値の組みあわせに対応して, 1〜4 回, 選択された試験 1, 試験 2, 又は試験 3 を記述する.

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

```
COUNT = 0                              ♯ i = 0 のデータの組について記述する.
EntropyInput = 0102 ... 3f40           ♯ i = 0 に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10                  ♯ i = 0 に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00  ♯ i = 0 に対応する personalization_string_i を記述する.
AdditionalInput = 0102 ... ff00        ♯ i = 0, j = 0 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40         ♯ i = 0, j = 0 に対応する entropy_input_PR_{i,j} を記述する.
AdditionalInput = 0102 ... ff00        ♯ i = 0, j = 1 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40         ♯ i = 0, j = 1 に対応する entropy_input_PR_{i,j} を記述する.
ReturnedBits = 3afb ... d291           ♯ i = 0, j = 1 に対応する pseudorandom_bits_{i,j} の期待値を記述する.

COUNT = 1                              ♯ i = 1 のデータの組について記述する.
EntropyInput = 0102 ... 3f40           ♯ i = 1 に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10                  ♯ i = 1 に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00  ♯ i = 1 に対応する personalization_string_i を記述する.
AdditionalInput = 0102 ... ff00        ♯ i = 1, j = 0 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40         ♯ i = 1, j = 0 に対応する entropy_input_PR_{i,j} を記述する.
AdditionalInput = 0102 ... ff00        ♯ i = 1, j = 1 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40         ♯ i = 1, j = 1 に対応する entropy_input_PR_{i,j} を記述する.
ReturnedBits = 3afb ... d291           ♯ i = 1, j = 1 に対応する pseudorandom_bits_{i,j} の期待値を記述する.

.
.
.
COUNT = ⟨ NumberOfTrials −1⟩           ♯ i = ⟨ NumberOfTrials −1⟩ のデータの組について記述する.
EntropyInput = 0102 ... 3f40           ♯ i = ⟨ NumberOfTrials −1⟩ に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10                  ♯ i = ⟨ NumberOfTrials −1⟩ に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00  ♯ i = ⟨ NumberOfTrials −1⟩ に対応する personalization_string_i を記述する.
AdditionalInput = 0102 ... ff00        ♯ i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40         ♯ i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する entropy_input_PR_{i,j} を記述する.
AdditionalInput = 0102 ... ff00        ♯ i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40         ♯ i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する entropy_input_PR_{i,j} を記述する.
ReturnedBits = 3afb ... d291           ♯ i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する pseudorandom_bits_{i,j} の期待値を記述する.
```

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

```
COUNT = 0                                  # i = 0 のデータの組について記述する．
EntropyInput = 0102 ... 3f40               # i = 0 に対応する entropy_input_i を記述する．
Nonce = 0102 ... 0f10                      # i = 0 に対応する nonce_i を記述する．
PersonalizationString = 0102 ... ff00      # i = 0 に対応する personalization_string_i を記述する．
EntropyInputReseed = 0102 ... 3f40         # i = 0, j = 0 に対応する entropy_input_on_reseed_{i,j} を記述する．
AdditionalInputReseed = 0102 ... ff00      # i = 0, j = 0 に対応する additional_input_on_reseed_{i,j} を記述する．
AdditionalInput = 0102 ... ff00            # i = 0, j = 1 に対応する additional_input_{i,j} を記述する．
AdditionalInput = 0102 ... ff00            # i = 0, j = 2 に対応する additional_input_{i,j} を記述する．
ReturnedBits = 3afb ... d291               # i = 0, j = 2 に対応する pseudorandom_bits_{i,j} の期待値を記述する．

COUNT = 1                                  # i = 1 のデータの組について記述する．
EntropyInput = 0102 ... 3f40               # i = 1 に対応する entropy_input_i を記述する．
Nonce = 0102 ... 0f10                      # i = 1 に対応する nonce_i を記述する．
PersonalizationString = 0102 ... ff00      # i = 1 に対応する personalization_string_i を記述する．
EntropyInputReseed = 0102 ... 3f40         # i = 1, j = 0 に対応する entropy_input_on_reseed_{i,j} を記述する．
AdditionalInputReseed = 0102 ... ff00      # i = 1, j = 0 に対応する additional_input_on_reseed_{i,j} を記述する．
AdditionalInput = 0102 ... ff00            # i = 1, j = 1 に対応する additional_input_{i,j} を記述する．
AdditionalInput = 0102 ... ff00            # i = 1, j = 2 に対応する additional_input_{i,j} を記述する．
ReturnedBits = 3afb ... d291               # i = 1, j = 2 に対応する pseudorandom_bits_{i,j} の期待値を記述する．
.
.
.
COUNT = ⟨ NumberOfTrials −1⟩               # i = ⟨ NumberOfTrials −1⟩ のデータの組について記述する．
EntropyInput = 0102 ... 3f40               # i = ⟨ NumberOfTrials −1⟩ に対応する entropy_input_i を記述する．
Nonce = 0102 ... 0f10                      # i = ⟨ NumberOfTrials −1⟩ に対応する nonce_i を記述する．
PersonalizationString = 0102 ... ff00      # i = ⟨ NumberOfTrials −1⟩ に対応する personalization_string_i を記述する．
EntropyInputReseed = 0102 ... 3f40         # i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する entropy_input_on_reseed_{i,j} を記述する．
AdditionalInputReseed = 0102 ... ff00      # i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する additional_input_on_reseed_{i,j} を記述する．
AdditionalInput = 0102 ... ff00            # i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する additional_input_{i,j} を記述する．
AdditionalInput = 0102 ... ff00            # i = ⟨ NumberOfTrials −1⟩, j = 2 に対応する additional_input_{i,j} を記述する．
ReturnedBits = 3afb ... d291               # i = ⟨ NumberOfTrials −1⟩, j = 2 に対応する pseudorandom_bits_{i,j} の期待値を記述する．
```

∗4 NumberOfTrials 個の各データの組を以下のように記述する．

```
COUNT = 0                                  # i = 0 のデータの組について記述する．
EntropyInput = 0102 ... 3f40               # i = 0 に対応する entropy_input_i を記述する．
Nonce = 0102 ... 0f10                      # i = 0 に対応する nonce_i を記述する．
PersonalizationString = 0102 ... ff00      # i = 0 に対応する personalization_string_i を記述する．
AdditionalInput = 0102 ... ff00            # i = 0, j = 0 に対応する additional_input_{i,j} を記述する．
AdditionalInput = 0102 ... ff00            # i = 0, j = 1 に対応する additional_input_{i,j} を記述する．
ReturnedBits = 3afb ... d291               # i = 0, j = 1 に対応する pseudorandom_bits_{i,j} の期待値を記述する．

COUNT = 1                                  # i = 1 のデータの組について記述する．
EntropyInput = 0102 ... 3f40               # i = 1 に対応する entropy_input_i を記述する．
Nonce = 0102 ... 0f10                      # i = 1 に対応する nonce_i を記述する．
PersonalizationString = 0102 ... ff00      # i = 1 に対応する personalization_string_i を記述する．
AdditionalInput = 0102 ... ff00            # i = 1, j = 0 に対応する additional_input_{i,j} を記述する．
AdditionalInput = 0102 ... ff00            # i = 1, j = 1 に対応する additional_input_{i,j} を記述する．
ReturnedBits = 3afb ... d291               # i = 1, j = 1 に対応する pseudorandom_bits_{i,j} の期待値を記述する．
.
.
.
COUNT = ⟨ NumberOfTrials −1⟩               # i = ⟨ NumberOfTrials −1⟩ のデータの組について記述する．
EntropyInput = 0102 ... 3f40               # i = ⟨ NumberOfTrials −1⟩ に対応する entropy_input_i を記述する．
Nonce = 0102 ... 0f10                      # i = ⟨ NumberOfTrials −1⟩ に対応する nonce_i を記述する．
PersonalizationString = 0102 ... ff00      # i = ⟨ NumberOfTrials −1⟩ に対応する personalization_string_i を記述する．
AdditionalInput = 0102 ... ff00            # i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する additional_input_{i,j} を記述する．
AdditionalInput = 0102 ... ff00            # i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する additional_input_{i,j} を記述する．
ReturnedBits = 3afb ... d291               # i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する pseudorandom_bits_{i,j} の期待値を記述する．
```

2.4 レスポンスファイル (*.rsp)

表7: NIST SP800-90A に記載された HMAC_DRBG, Hash_DRBG, 及び CTR_DRBG

機能	分類	タグ	内容	暗号アルゴリズム実装試験仕様書—乱数生成器—上の表記との対応	値の表記	例示
全機能試験	全体ヘッダ	AlgorithmName	乱数生成器名. 次のいずれかを選択: HMAC_DRBG, Hash_DRBG, CTR_DRBG use df, CTR_DRBG no df		文字列	[AlgorithmName = HMAC_DRBG]
		UnderlyingAlgorithm	暗号プリミティブ識別子. HMAC_DRBG 又は Hash_DRBG の選択時, 次のいずれかを選択: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. CTR_DRBG use df 又は CTR_DRBG no df の選択時, 次のいずれかを選択: AES-128, AES-192, AES-256		文字列	[UnderlyingAlgorithm = SHA-256]
		SecurityStrength	セキュリティ強度	*strength*	10 進	[SecurityStrength = 256]
		WithReseedCapability	Reseed 機能の有無 (有:True, 無:False)		文字列	[WithReseedCapability = True]
		PredictionResistance	Prediction resistance の有効化の有無 (有:True, 無:False)		文字列	[PredictionResistance = True]
		EntropyInputLen	*entropy_input* のビット長		10 進表記	[EntropyInputLen = 512]
		NonceLen	*nonce* のビット長		10 進表記	[NonceLen = 128]
		PersonalizationStringMinLen	*personalization_string* のビット長の最小値		10 進表記	[PersonalizationStringMinLen = 0]
		PersonalizationStringMaxLen	*personalization_string* のビット長の最大値		10 進表記	[PersonalizationStringMaxLen = 2048]
		AdditionalInputMinLen	*additional_input* のビット長の最小値		10 進表記	[AdditionalInputMinLen = 0]
		AdditionalInputMaxLen	*additional_input* のビット長の最大値		10 進表記	[AdditionalInputMaxLen = 2048]
		RequestedNumberOfBits	*returned_bits* のビット長	*requested_number_of_bits*	10 進表記	[RequestedNumberOfBits = 512]
		NumberOfTrials	DRBG インスタンスを生成する回数	*number_of_trials*	10 進表記	[NumberOfTrials = 100]
	試験 1 *1 / 試験 1 ヘッダ	〈UnderlyingAlgorithm の値〉	共通ヘッダ UnderlyingAlgorithm の値 (CTR_DRBG の選択時, 導出関数の有の場合 " use df" を, 無の場合 " no df" を付加)		文字列	[HMAC-SHA-512/224]
		PredictionResistance	PredictionResistance を有効にする場合 True, 無効にする場合 False		文字列	[PredictionResistance = True]
		EntropyInputLen	*entropy_input* のビット長		10 進表記	[EntropyInputLen = 512]
		NonceLen	*nonce* のビット長		10 進表記	[NonceLen = 128]
		PersonalizationStringLen	*personalization_string* のビット長		10 進表記	[PersonalizationStringLen = 2048]
		AdditionalInputLen	*additional_input* のビット長		10 進表記	[AdditionalInputLen = 2048]
	試験 1 本体 *2	COUNT	0 以上 NumberOfTrials 未満の整数	i	10 進表記	COUNT = 0
		EntropyInput	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $entropy\_input_i$	16 進表記	EntropyInput = 0102 . . . 3f40
		Nonce	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $nonce_i$	16 進表記	Nonce = 0102 . . . 0f10
		PersonalizationString	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $personalization\_string_i$	16 進表記	PersonalizationString = 0102 . . . ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 . . . ff00
		EntropyInputPR	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $entropy\_input\_PR_{i,j}$	16 進表記	EntropyInputPR = 0102 . . . 3f40
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 . . . ff00
		EntropyInputPR	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $entropy\_input\_PR_{i,j}$	16 進表記	EntropyInputPR = 0102 . . . 3f40
		ReturnedBits	【出力】Generate 関数の出力であるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $pseudorandom\_bits_{i,j}$	16 進表記	ReturnedBits = 3afb . . . d291
	試験 2 *1 / 試験 2 ヘッダ	〈UnderlyingAlgorithm の値〉	共通ヘッダ UnderlyingAlgorithm の値 (CTR_DRBG の選択時, 導出関数の有の場合 " use df" を, 無の場合 " no df" を付加)		文字列	[HMAC-SHA-512/224]
		PredictionResistance	PredictionResistance を有効にする場合 True, 無効にする場合 False		文字列	[PredictionResistance = False]
		EntropyInputLen	*entropy_input* のビット長		10 進表記	[EntropyInputLen = 512]
		NonceLen	*nonce* のビット長		10 進表記	[NonceLen = 128]
		PersonalizationStringLen	*personalization_string* のビット長		10 進表記	[PersonalizationStringLen = 2048]
		AdditionalInputLen	*additional_input* のビット長		10 進表記	[AdditionalInputLen = 2048]
	試験 2 本体 *3	COUNT	0 以上 NumberOfTrials 未満の整数	i	10 進表記	COUNT = 0
		EntropyInput	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $entropy\_input_i$	16 進表記	EntropyInput = 0102 . . . 3f40
		Nonce	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $nonce_i$	16 進表記	Nonce = 0102 . . . 0f10
		PersonalizationString	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $personalization\_string_i$	16 進表記	PersonalizationString = 0102 . . . ff00
		EntropyInputReseed	Reseed 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $entropy\_input\_on\_reseed_{i,j}$	16 進表記	EntropyInputReseed = 0102 . . . 3f40
		AdditionalInputReseed	Reseed 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $additional\_input\_on\_reseed_{i,j}$	16 進表記	AdditionalInputReseed = 0102 . . . ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 . . . ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 2$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 . . . ff00
		ReturnedBits	【出力】Generate 関数の出力であるビット列	$i = \langle$COUNT の値$\rangle$, $j = 2$ に対応する $pseudorandom\_bits_{i,j}$	16 進表記	ReturnedBits = 3afb . . . d291
	試験 3 *1 / 試験 3 ヘッダ	〈UnderlyingAlgorithm の値〉	共通ヘッダ UnderlyingAlgorithm の値 (CTR_DRBG の選択時, 導出関数の有の場合 " use df" を, 無の場合 " no df" を付加)		文字列	[HMAC-SHA-512/224]
		PredictionResistance	PredictionResistance を有効にする場合 True, 無効にする場合 False		文字列	[PredictionResistance = False]
		EntropyInputLen	*entropy_input* のビット長		10 進表記	[EntropyInputLen = 512]
		NonceLen	*nonce* のビット長		10 進表記	[NonceLen = 128]
		PersonalizationStringLen	*personalization_string* のビット長		10 進表記	[PersonalizationStringLen = 2048]
		AdditionalInputLen	*additional_input* のビット長		10 進表記	[AdditionalInputLen = 2048]
	試験 3 本体 *4	COUNT	0 以上 NumberOfTrials 未満の整数	i	10 進表記	COUNT = 0
		EntropyInput	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $entropy\_input_i$	16 進表記	EntropyInput = 0102 . . . 3f40
		Nonce	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $nonce_i$	16 進表記	Nonce = 0102 . . . 0f10
		PersonalizationString	Instantiate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$ に対応する $personalization\_string_i$	16 進表記	PersonalizationString = 0102 . . . ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 0$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 . . . ff00
		AdditionalInput	Generate 関数の入力となるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $additional\_input_{i,j}$	16 進表記	AdditionalInput = 0102 . . . ff00
		ReturnedBits	【出力】Generate 関数の出力であるビット列	$i = \langle$COUNT の値$\rangle$, $j = 1$ に対応する $pseudorandom\_bits_{i,j}$	16 進表記	ReturnedBits = 3afb . . . d291

∗1 WithReseedCapability 及び PredictionResistance の値の組みあわせに対応して, 試験 1, 試験 2, 又は試験 3 のいずれか 1 つが選択される. その上で, PersonalizationStringMinLen, PersonalizationStringMaxLen, AdditionalInputMinLen 及び AdditionalInputMaxLen の値の組みあわせに対応して, 1〜4 回, 選択された試験 1, 試験 2, 又は試験 3 を記述する.

∗2 NumberOfTrials 個の各データの組を以下のように記述する.

```
COUNT = 0                                  # i = 0 のデータの組について記述する.
EntropyInput = 0102 ... 3f40               # i = 0 に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10                      # i = 0 に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00      # i = 0 に対応する personalization_string_i を記述する.
AdditionalInput = 0102 ... ff00            # i = 0, j = 0 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40             # i = 0, j = 0 に対応する entropy_input_PR_{i,j} を記述する.
AdditionalInput = 0102 ... ff00            # i = 0, j = 1 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40             # i = 0, j = 1 に対応する entropy_input_PR_{i,j} を記述する.
ReturnedBits = 3afb ... d291               # i = 0, j = 1 に対応して生成された pseudorandom_bits_{i,j}.

COUNT = 1                                  # i = 1 のデータの組について記述する.
EntropyInput = 0102 ... 3f40               # i = 1 に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10                      # i = 1 に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00      # i = 1 に対応する personalization_string_i を記述する.
AdditionalInput = 0102 ... ff00            # i = 1, j = 0 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40             # i = 1, j = 0 に対応する entropy_input_PR_{i,j} を記述する.
AdditionalInput = 0102 ... ff00            # i = 1, j = 1 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40             # i = 1, j = 1 に対応する entropy_input_PR_{i,j} を記述する.
ReturnedBits = 3afb ... d291               # i = 1, j = 1 に対応して生成された pseudorandom_bits_{i,j}.
.
.
.
COUNT = ⟨ NumberOfTrials −1⟩               # i = ⟨ NumberOfTrials −1⟩ のデータの組について記述する.
EntropyInput = 0102 ... 3f40               # i = ⟨ NumberOfTrials −1⟩ に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10                      # i = ⟨ NumberOfTrials −1⟩ に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00      # i = ⟨ NumberOfTrials −1⟩ に対応する personalization_string_i を記述する.
AdditionalInput = 0102 ... ff00            # i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40             # i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する entropy_input_PR_{i,j} を記述する.
AdditionalInput = 0102 ... ff00            # i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する additional_input_{i,j} を記述する.
EntropyInputPR = 0102 ... 3f40             # i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する entropy_input_PR_{i,j} を記述する.
ReturnedBits = 3afb ... d291               # i = ⟨ NumberOfTrials −1⟩, j = 1 に対応して生成された pseudorandom_bits_{i,j}.
```

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

```
COUNT = 0                                  # i = 0 のデータの組について記述する.
EntropyInput = 0102 ... 3f40               # i = 0 に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10                      # i = 0 に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00      # i = 0 に対応する personalization_string_i を記述する.
EntropyInputReseed = 0102 ... 3f40         # i = 0, j = 0 に対応する entropy_input_on_reseed_{i,j} を記述する.
AdditionalInputReseed = 0102 ... ff00      # i = 0, j = 0 に対応する additional_input_on_reseed_{i,j} を記述する.
AdditionalInput = 0102 ... ff00            # i = 0, j = 1 に対応する additional_input_{i,j} を記述する.
AdditionalInput = 0102 ... ff00            # i = 0, j = 2 に対応する additional_input_{i,j} を記述する.
ReturnedBits = 3afb ... d291               # i = 0, j = 2 に対応して生成された pseudorandom_bits_{i,j}.

COUNT = 1                                  # i = 1 のデータの組について記述する.
EntropyInput = 0102 ... 3f40               # i = 1 に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10                      # i = 1 に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00      # i = 1 に対応する personalization_string_i を記述する.
EntropyInputReseed = 0102 ... 3f40         # i = 1, j = 0 に対応する entropy_input_on_reseed_{i,j} を記述する.
AdditionalInputReseed = 0102 ... ff00      # i = 1, j = 0 に対応する additional_input_on_reseed_{i,j} を記述する.
AdditionalInput = 0102 ... ff00            # i = 1, j = 1 に対応する additional_input_{i,j} を記述する.
AdditionalInput = 0102 ... ff00            # i = 1, j = 2 に対応する additional_input_{i,j} を記述する.
ReturnedBits = 3afb ... d291               # i = 1, j = 2 に対応して生成された pseudorandom_bits_{i,j}.
.
.
.
COUNT = ⟨ NumberOfTrials −1⟩               # i = ⟨ NumberOfTrials −1⟩ のデータの組について記述する.
EntropyInput = 0102 ... 3f40               # i = ⟨ NumberOfTrials −1⟩ に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10                      # i = ⟨ NumberOfTrials −1⟩ に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00      # i = ⟨ NumberOfTrials −1⟩ に対応する personalization_string_i を記述する.
EntropyInputReseed = 0102 ... 3f40         # i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する entropy_input_on_reseed_{i,j} を記述する.
AdditionalInputReseed = 0102 ... ff00      # i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する additional_input_on_reseed_{i,j} を記述する.
AdditionalInput = 0102 ... ff00            # i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する additional_input_{i,j} を記述する.
AdditionalInput = 0102 ... ff00            # i = ⟨ NumberOfTrials −1⟩, j = 2 に対応する additional_input_{i,j} を記述する.
ReturnedBits = 3afb ... d291               # i = ⟨ NumberOfTrials −1⟩, j = 2 に対応して生成された pseudorandom_bits_{i,j}.
```

∗4 NumberOfTrials 個の各データの組を以下のように記述する.

```
COUNT = 0                                  # i = 0 のデータの組について記述する.
EntropyInput = 0102 ... 3f40               # i = 0 に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10                      # i = 0 に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00      # i = 0 に対応する personalization_string_i を記述する.
AdditionalInput = 0102 ... ff00            # i = 0, j = 0 に対応する additional_input_{i,j} を記述する.
AdditionalInput = 0102 ... ff00            # i = 0, j = 1 に対応する additional_input_{i,j} を記述する.
ReturnedBits = 3afb ... d291               # i = 0, j = 1 に対応して生成された pseudorandom_bits_{i,j}.

COUNT = 1                                  # i = 1 のデータの組について記述する.
EntropyInput = 0102 ... 3f40               # i = 1 に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10                      # i = 1 に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00      # i = 1 に対応する personalization_string_i を記述する.
AdditionalInput = 0102 ... ff00            # i = 1, j = 0 に対応する additional_input_{i,j} を記述する.
AdditionalInput = 0102 ... ff00            # i = 1, j = 1 に対応する additional_input_{i,j} を記述する.
ReturnedBits = 3afb ... d291               # i = 1, j = 1 に対応して生成された pseudorandom_bits_{i,j}.
.
.
.
COUNT = ⟨ NumberOfTrials −1⟩               # i = ⟨ NumberOfTrials −1⟩ のデータの組について記述する.
EntropyInput = 0102 ... 3f40               # i = ⟨ NumberOfTrials −1⟩ に対応する entropy_input_i を記述する.
Nonce = 0102 ... 0f10                      # i = ⟨ NumberOfTrials −1⟩ に対応する nonce_i を記述する.
PersonalizationString = 0102 ... ff00      # i = ⟨ NumberOfTrials −1⟩ に対応する personalization_string_i を記述する.
AdditionalInput = 0102 ... ff00            # i = ⟨ NumberOfTrials −1⟩, j = 0 に対応する additional_input_{i,j} を記述する.
AdditionalInput = 0102 ... ff00            # i = ⟨ NumberOfTrials −1⟩, j = 1 に対応する additional_input_{i,j} を記述する.
ReturnedBits = 3afb ... d291               # i = ⟨ NumberOfTrials −1⟩, j = 1 に対応して生成された pseudorandom_bits_{i,j}.
```

2.5 結果ファイル (*.out)

表8: NIST SP800-90A に記載された HMAC_DRBG, Hash_DRBG, 及び CTR_DRBG

機能	分類		タグ	内容	値の表記	例示
全機能試験	全体ヘッダ		AlgorithmName	乱数生成器名. 次のいずれかを選択: HMAC_DRBG, Hash_DRBG, CTR_DRBG use df, CTR_DRBG no df	文字列	[AlgorithmName = HMAC_DRBG]
			UnderlyingAlgorithm	暗号プリミティブ識別子. HMAC_DRBG 又は Hash_DRBG の選択時, 次のいずれかを選択: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. CTR_DRBG use df 又は CTR_DRBG no df の選択時, 次のいずれかを選択: AES-128, AES-192, AES-256	文字列	[UnderlyingAlgorithm = SHA-256]
			SecurityStrength	セキュリティ強度	10 進	[SecurityStrength = 256]
			WithReseedCapability	Reseed 機能の有無 (有:True, 無:False)	文字列	[WithReseedCapability = True]
			PredictionResistance	Prediction resistance の有効化の有無 (有:True, 無:False)	文字列	[PredictionResistance = True]
			EntropyInputLen	*entropy_input* のビット長	10 進表記	[EntropyInputLen = 512]
			NonceLen	*nonce* のビット長	10 進表記	[NonceLen = 128]
			PersonalizationStringMinLen	*personalization_string* のビット長の最小値	10 進表記	[PersonalizationStringMinLen = 0]
			PersonalizationStringMaxLen	*personalization_string* のビット長の最大値	10 進表記	[PersonalizationStringMaxLen = 2048]
			AdditionalInputMinLen	*additional_input* のビット長の最小値	10 進表記	[AdditionalInputMinLen = 0]
			AdditionalInputMaxLen	*additional_input* のビット長の最大値	10 進表記	[AdditionalInputMaxLen = 2048]
			RequestedNumberOfBits	*returned_bits* のビット長	10 進表記	[RequestedNumberOfBits = 512]
			NumberOfTrials	DRBG インスタンスを生成する回数	10 進表記	[NumberOfTrials = 100]
	試験 1 *1	試験 1 ヘッダ	⟨UnderlyingAlgorithm の値⟩	共通ヘッダ UnderlyingAlgorithm の値 (CTR_DRBG の選択時, 導出関数の有の場合 " use df" を, 無の場合 " no df" を付加)	文字列	[HMAC-SHA-512/224]
			PredictionResistance	PredictionResistance を有効にする場合 True, 無効にする場合 False	文字列	[PredictionResistance = True]
			EntropyInputLen	*entropy_input* のビット長	10 進表記	[EntropyInputLen = 512]
			NonceLen	*nonce* のビット長	10 進表記	[NonceLen = 128]
			PersonalizationStringLen	*personalization_string* のビット長	10 進表記	[PersonalizationStringLen = 2048]
			AdditionalInputLen	*additional_input* のビット長	10 進表記	[AdditionalInputLen = 2048]
			⟨ Results ⟩	OK 又は NG	文字列	OK
	試験 2 *1	試験 2 ヘッダ	⟨UnderlyingAlgorithm の値⟩	共通ヘッダ UnderlyingAlgorithm の値 (CTR_DRBG の選択時, 導出関数の有の場合 " use df" を, 無の場合 " no df" を付加)	文字列	[HMAC-SHA-512/224]
			PredictionResistance	PredictionResistance を有効にする場合 True, 無効にする場合 False	文字列	[PredictionResistance = False]
			EntropyInputLen	*entropy_input* のビット長	10 進表記	[EntropyInputLen = 512]
			NonceLen	*nonce* のビット長	10 進表記	[NonceLen = 128]
			PersonalizationStringLen	*personalization_string* のビット長	10 進表記	[PersonalizationStringLen = 2048]
			AdditionalInputLen	*additional_input* のビット長	10 進表記	[AdditionalInputLen = 2048]
			⟨ Results ⟩	OK 又は NG	文字列	OK
	試験 3 *1	試験 3 ヘッダ	⟨UnderlyingAlgorithm の値⟩	共通ヘッダ UnderlyingAlgorithm の値 (CTR_DRBG の選択時, 導出関数の有の場合 " use df" を, 無の場合 " no df" を付加)	文字列	[HMAC-SHA-512/224]
			PredictionResistance	PredictionResistance を有効にする場合 True, 無効にする場合 False	文字列	[PredictionResistance = False]
			EntropyInputLen	*entropy_input* のビット長	10 進表記	[EntropyInputLen = 512]
			NonceLen	*nonce* のビット長	10 進表記	[NonceLen = 128]
			PersonalizationStringLen	*personalization_string* のビット長	10 進表記	[PersonalizationStringLen = 2048]
			AdditionalInputLen	*additional_input* のビット長	10 進表記	[AdditionalInputLen = 2048]
			⟨ Results ⟩	OK 又は NG	文字列	OK

*1 WithReseedCapability 及び PredictionResistance の値の組みあわせに対応して, 試験 1, 試験 2, 又は試験 3 のいずれか 1 つが選択される. その上で, PersonalizationStringMinLen, PersonalizationStringMaxLen, AdditionalInputMinLen 及び AdditionalInputMaxLen の値の組みあわせに対応して, 1〜4 回, 選択された試験 1, 試験 2, 又は試験 3 を記述する.

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．