JCATT ファイルフォーマット仕様書

NIST SP800-108 に記載された鍵導出関数

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　NIST SP800-108 に記載された鍵導出関数

鍵導出関数 KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode 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.

`Algorithm Name` は，KDF_in_NIST_SP800_108.

各表において，試験方法に関する以下の略語を使用する.

- PRF: Pseudorandom Function

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　CAVS 準互換ファイルフォーマット

この章で取り扱うファイルフォーマットでは, 鍵導出関数識別子として, 表1に記載された表現を用いる.

表1　鍵導出関数識別子

鍵導出関数識別子	対応する鍵導出関数
KDFinCounterMode	`KDF in Counter Mode`
KDFinFeedbackMode	`KDF in Feedback Mode`
KDFinDoublePipelineIterationMode	`KDF in Double-Pipeline Iteration Mode`

PRF 識別子は, 表2に記載された通りである.

表2　PRF 識別子

PRF 識別子	対応する PRF
HMAC_SHA1	`HMAC-SHA-1`
HMAC_SHA224	`HMAC-SHA-224`
HMAC_SHA256	`HMAC-SHA-256`
HMAC_SHA384	`HMAC-SHA-384`
HMAC_SHA512	`HMAC-SHA-512`
HMAC_SHA512/224	`HMAC-SHA-512/224`
HMAC_SHA512/256	`HMAC-SHA-512/256`
CMAC_AES128	`CMAC-AES-128`
CMAC_AES192	`CMAC-AES-192`
CMAC_AES256	`CMAC-AES-256`

2.1.1　パラメータファイル (*.par)

表3　NIST SP800-108 に記載された鍵導出関数 パラメータファイル

機能	タグ		内容	表記
鍵導出関数	ヘッダ	AlgorithmName	KDF_in_NIST_SP800_108	文字列
		KDFMode	(鍵導出関数識別子)	文字列
		PRF	(PRF 識別子)	文字列
		PRFInputWithCounter	counter を含めた PRF の入力とするかどうか (counter を含める:True,counter を含めない:False)	文字列
		CTRLOCATION	(counter の挿入位置)BEFORE_FIXED	文字列
		RLEN	(counter i のビット長)	10 進
		LdivisibleBy8	8 の倍数の L のサポートの有無 (有:True, 無:False)	文字列
		BitLengthOfKeyForKSltB	HMAC を使った PRF 選択時, B 未満の HMAC 鍵のビット長	10 進
		BitLengthOfKeyForKSeqB	HMAC を使った PRF 選択時, B に等しい HMAC 鍵のビット長	10 進
		BitLengthOfKeyForKSgtB	HMAC を使った PRF 選択時, B より大きい HMAC 鍵のビット長	10 進
		BitLengthOfIVForIVLeneq0	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) = 0$ なる IV を IUT がサポートする場合, 0. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.	10 進
		BitLengthOfIVForIVLenlth	KDF in Feedback Mode の選択時, $0 < \mathbf{len}(IV) < h$ なる IV を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.	10 進
		BitLengthOfIVForIVLeneqh	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) = h$ なる IV を IUT がサポートする場合, そのビット長. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.	10 進
		BitLengthOfIVForIVLength	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) > h$ なる IV を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.	10 進
		MinLDivisibleByH	h で割り切れる L の, IUT がサポートする範囲の最小値	10 進
		MaxLDivisibleByH	h で割り切れる L の, IUT がサポートする範囲の最大値	10 進
		MinLDivisibleBy8	(h で割り切れない)8 の倍数の L の, IUT がサポートする範囲の最小値	10 進
		MaxLDivisibleBy8	(h で割り切れない)8 の倍数の L の, IUT がサポートする範囲の最大値	10 進
		NumberOfTestSubsets	試験の部分集合の数	10 進
		NumberOfTrialsForEachTestSubset	試験の各部分集合の中で, 導出する keying material の数	10 進

2.1.2 リクエストファイル (*.req)

表4: NIST SP800-108 に記載された鍵導出関数 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 ―鍵確立手法― 上の表記との対応	値の表記	例示
鍵導出関数	ヘッダ	AlgorithmName	KDF_in_NIST_SP800_108		文字列	[AlgorithmName = KDF_in_NIST_SP800_108]
		KDFMode	鍵導出関数識別子		文字列	[KDFMode = KDFinCounterMode]
		PRF	PRF 識別子		文字列	[PRF = HMAC_SHA512]
		PRFInputWithCounter	(counter を含めた PRF の入力とするかどうか)(counter を含める:True,counter を含めない:False)		文字列	[PRFInputWithCounter = True]
		CTRLOCATION	(counter の挿入位置)BEFORE_FIXED		文字列	[CTRLOCATION = BEFORE_FIXED]
		RLEN	counter i のビット長		10 進表記	[RLEN = 32]
		LdivisibleBy8	8 の倍数の L のサポートの有無 (有:True, 無:False)		文字列	[LdivisibleBy8 = True]
		BitLengthOfKeyForKSltB	HMAC を使った PRF 選択時, B 未満の HMAC 鍵のビット長. CMAC を使った PRF 選択時, タグは省略.		10 進表記	[BitLengthOfKeyForKSltB = 256]
		BitLengthOfKeyForKSeqB	HMAC を使った PRF 選択時, B に等しい HMAC 鍵のビット長. CMAC を使った PRF 選択時, タグは省略.		10 進表記	[BitLengthOfKeyForKSeqB = 1024]
		BitLengthOfKeyForKSgtB	HMAC を使った PRF 選択時, B より大きい HMAC 鍵のビット長. CMAC を使った PRF 選択時, タグは省略.		10 進表記	[BitLengthOfKeyForKSgtB = 2048]
		BitLengthOfIVForIVLeneq0	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) = 0$ なる IV を IUT がサポートする場合, 0. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.		10 進表記	[BitLengthOfIVForIVLeneq0 = 0]
		BitLengthOfIVForIVLenlth	KDF in Feedback Mode の選択時, $0 < \mathbf{len}(IV) < h$ なる IV を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.		10 進表記	[BitLengthBitLengthOfIVForIVLenlth = 256]
		BitLengthOfIVForIVLeneqh	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) = h$ なる IV を IUT がサポートする場合, そのビット長. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.		10 進表記	[BitLengthOfIVForIVLeneqh = 512]
		BitLengthOfIVForIVLength	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) > h$ なる IV を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.		10 進表記	[BitLengthOfIVForIVLength = 768]
		MinLDivisibleByH	h で割り切れる L の, IUT がサポートする範囲の最小値		10 進表記	[MinLDivisibleByH = 512]
		MaxLDivisibleByH	h で割り切れる L の, IUT がサポートする範囲の最大値		10 進表記	[MaxLDivisibleByH = 2048]
		MinLDivisibleBy8	(h で割り切れない)8 の倍数の L の, IUT がサポートする範囲の最小値		10 進表記	[MinLDivisibleBy8 = 112]
		MaxLDivisibleBy8	(h で割り切れない)8 の倍数の L の, IUT がサポートする範囲の最大値		10 進表記	[MaxLDivisibleBy8 = 1280]
		NumberOfTestSubsets	試験の部分集合の数		10 進表記	[NumberOfTestSubsets = 12]
		NumberOfTrialsForEachTestSubset	試験の各部分集合の中で, 導出する keying material の数		10 進表記	[NumberOfTrialsForEachTestSubset = 10]
	試験部分集合 *1 *2 *3	COUNT	0 以上 NumberOfTrialsForEachTestSubset 未満の整数		10 進表記	COUNT = 0
		L	導出する keying material (K_0) のビット長 (L)	L	10 進表記	L = 512
		KI	鍵導出鍵 (K_I)	K_I	16 進表記	KI = 2f9a ... 3664
		IVlen	(KDF in Feedback Mode の選択時,) IV のビット長	$\mathbf{len}(IV)$	10 進表記	IVlen = 256
		IV	(KDF in Feedback Mode の選択時,) IV	IV	16 進表記	IV = 1cf7 ... 778d
		FixedInputDataByteLen	$FixedInput$ のバイト長		10 進表記	FixedInputDataByteLen = ?
		FixedInputData	$FixedInput$	$FixedInput$	16 進表記	FixedInputData = ?
		KO	keying material (K_0)	K_0	16 進表記	KO = ?

*1 KDF in Counter Mode 及び KDF in Double-Pipeline Iteration Mode の場合, PRF(HMAC 又は CMAC) の選択及び IUT がサポートする L 値の範囲の組みあわせに対応して, 最大 12 個の部分集合を記載する. KDF in Feedback Mode の場合, PRF(HMAC 又は CMAC) の選択, IUT がサポートする L 値の範囲, IUT がサポートする IV の長さの組みあわせに対応して, 最大 48 個の部分集合を記載する.

*2 KDF in Counter Mode 及び KDF in Double-Pipeline Iteration Mode の場合, NumberOfTrialsForEachTestSubset 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.
L = 512                                    ♯ i = 0 に対応する L を記述する.
KI = e571 ... 519f                         ♯ i = 0 に対応する鍵導出鍵を記述する.
FixedInputDataByteLen = ?                  ♯ i = 0 に対応する FixedInput のバイト長のプレースホルダ.
FixedInputData = ?                         ♯ i = 0 に対応する FixedInput のプレースホルダ.
KO = ?                                     ♯ i = 0 に対応する keying material K0 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.
L = 512                                    ♯ i = 1 に対応する L を記述する.
KI = 9f15 ... 4d17                         ♯ i = 1 に対応する鍵導出鍵を記述する.
FixedInputDataByteLen = ?                  ♯ i = 1 に対応する FixedInput のバイト長のプレースホルダ.
FixedInputData = ?                         ♯ i = 1 に対応する FixedInput のプレースホルダ.
KO = ?                                     ♯ i = 1 に対応する keying material K0 のプレースホルダ.
⋮
COUNT = ⟨NumberOfTrialsForEachTestSubset − 1⟩   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ のデータの組について記述する.
L = 512                                    ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する L を記述する.
KI = dc6f ... c8f2                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する鍵導出鍵を記述する.
FixedInputDataByteLen = ?                  ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する FixedInput のバイト長のプレースホルダ.
FixedInputData = ?                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する FixedInput のプレースホルダ.
KO = ?                                     ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する keying material K0 のプレースホルダ.
```

*3 KDF in Feedback Mode の場合, NumberOfTrialsForEachTestSubset 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.
L = 512                                    ♯ i = 0 に対応する L を記述する.
KI = e571 ... 519f                         ♯ i = 0 に対応する鍵導出鍵を記述する.
IVlen = 256                                ♯ i = 0 に対応する IV のビット長を記述する.
IV = 1cf7 ... 778d                         ♯ i = 0 に対応する IV を記述する.
FixedInputDataByteLen = ?                  ♯ i = 0 に対応する FixedInput のバイト長のプレースホルダ.
FixedInputData = ?                         ♯ i = 0 に対応する FixedInput のプレースホルダ.
KO = ?                                     ♯ i = 0 に対応する keying material K0 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.
L = 512                                    ♯ i = 1 に対応する L を記述する.
KI = 9f15 ... 4d17                         ♯ i = 1 に対応する鍵導出鍵を記述する.
IVlen = 256                                ♯ i = 1 に対応する IV のビット長を記述する.
IV = 1cf7 ... 778d                         ♯ i = 1 に対応する IV を記述する.
FixedInputDataByteLen = ?                  ♯ i = 1 に対応する FixedInput のバイト長のプレースホルダ.
FixedInputData = ?                         ♯ i = 1 に対応する FixedInput のプレースホルダ.
KO = ?                                     ♯ i = 1 に対応する keying material K0 のプレースホルダ.
⋮
COUNT = ⟨NumberOfTrialsForEachTestSubset − 1⟩   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ のデータの組について記述する.
L = 512                                    ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する L を記述する.
KI = dc6f ... c8f2                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する鍵導出鍵を記述する.
IVlen = 256                                ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する IV のビット長を記述する.
IV = 1cf7 ... 778d                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する IV を記述する.
FixedInputDataByteLen = ?                  ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する FixedInput のバイト長のプレースホルダ.
FixedInputData = ?                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する FixedInput のプレースホルダ.
KO = ?                                     ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する keying material K0 のプレースホルダ.
```

2.1.3 Facts ファイル (*.fax)

表5: NIST SP800-108 に記載された鍵導出関数 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 ―鍵確立手法― 上の表記との対応	値の表記	例示
鍵導出関数	ヘッダ	AlgorithmName	KDF_in_NIST_SP800_108		文字列	[AlgorithmName = KDF_in_NIST_SP800_108]
		KDFMode	鍵導出関数識別子		文字列	[KDFMode = KDFinCounterMode]
		PRF	PRF 識別子		文字列	[PRF = HMAC_SHA512]
		PRFInputWithCounter	(counter を含めた PRF の入力とするかどうか)(counter を含める:True,counter を含めない:False)		文字列	[PRFInputWithCounter = True]
		CTRLOCATION	(counter の挿入位置)BEFORE_FIXED		文字列	[CTRLOCATION = BEFORE_FIXED]
		RLEN	counter i のビット長		10 進表記	[RLEN = 32]
		LdivisibleBy8	8 の倍数の L のサポートの有無 (有:True, 無:False)		文字列	[LdivisibleBy8 = True]
		BitLengthOfKeyForKSltB	HMAC を使った PRF 選択時, B 未満の HMAC 鍵のビット長. CMAC を使った PRF 選択時, タグは省略.		10 進表記	[BitLengthOfKeyForKSltB = 256]
		BitLengthOfKeyForKSeqB	HMAC を使った PRF 選択時, B に等しい HMAC 鍵のビット長. CMAC を使った PRF 選択時, タグは省略.		10 進表記	[BitLengthOfKeyForKSeqB = 1024]
		BitLengthOfKeyForKSgtB	HMAC を使った PRF 選択時, B より大きい HMAC 鍵のビット長. CMAC を使った PRF 選択時, タグは省略.		10 進表記	[BitLengthOfKeyForKSgtB = 2048]
		BitLengthOfIVForIVLeneq0	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) = 0$ なる IV を IUT がサポートする場合, 0. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.		10 進表記	[BitLengthOfIVForIVLeneq0 = 0]
		BitLengthOfIVForIVLenlth	KDF in Feedback Mode の選択時, $0 < \mathbf{len}(IV) < h$ なる IV を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.		10 進表記	[BitLengthBitLengthOfIVForIVLenlth = 256]
		BitLengthOfIVForIVLeneqh	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) = h$ なる IV を IUT がサポートする場合, そのビット長. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.		10 進表記	[BitLengthOfIVForIVLeneqh = 512]
		BitLengthOfIVForIVLength	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) > h$ なる IV を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.		10 進表記	[BitLengthOfIVForIVLength = 768]
		MinLDivisibleByH	h で割り切れる L の, IUT がサポートする範囲の最小値		10 進表記	[MinLDivisibleByH = 512]
		MaxLDivisibleByH	h で割り切れる L の, IUT がサポートする範囲の最大値		10 進表記	[MaxLDivisibleByH = 2048]
		MinLDivisibleBy8	(h で割り切れない)8 の倍数の L の, IUT がサポートする範囲の最小値		10 進表記	[MinLDivisibleBy8 = 112]
		MaxLDivisibleBy8	(h で割り切れない)8 の倍数の L の, IUT がサポートする範囲の最大値		10 進表記	[MaxLDivisibleBy8 = 1280]
		NumberOfTestSubsets	試験の部分集合の数		10 進表記	[NumberOfTestSubsets = 12]
		NumberOfTrialsForEachTestSubset	試験の各部分集合の中で, 導出する keying material の数		10 進表記	[NumberOfTrialsForEachTestSubset = 10]
	試験部分集合 *1 *2 *3	COUNT	0 以上 NumberOfTrialsForEachTestSubset 未満の整数		10 進表記	COUNT = 0
		L	導出する keying material (K_0) のビット長 (L)	L	10 進表記	L = 512
		KI	鍵導出鍵 (K_I)	K_I	16 進表記	KI = 2f9a ... 3664
		IVlen	(KDF in Feedback Mode の選択時,) IV のビット長	$\mathbf{len}(IV)$	10 進表記	IVlen = 256
		IV	(KDF in Feedback Mode の選択時,) IV	IV	16 進表記	IV = 1cf7 ... 778d

*1 KDF in Counter Mode 及び KDF in Double-Pipeline Iteration Mode の場合, PRF(HMAC 又は CMAC) の選択及び IUT がサポートする L 値の範囲の組みあわせに対応して, 最大 12 個の部分集合を記載する. KDF in Feedback Mode の場合, PRF(HMAC 又は CMAC) の選択, IUT がサポートする L 値の範囲, IUT がサポートする IV の長さの組みあわせに対応して, 最大 48 個の部分集合を記載する.

*2 KDF in Counter Mode 及び KDF in Double-Pipeline Iteration Mode の場合, NumberOfTrialsForEachTestSubset 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.
L = 512                                    ♯ i = 0 に対応する L を記述する.
KI = e571 ... 519f                         ♯ i = 0 に対応する鍵導出鍵を記述する.

COUNT = 1                                  ♯ i = 1 のデータの組について記述する.
L = 512                                    ♯ i = 1 に対応する L を記述する.
KI = 9f15 ... 4d17                         ♯ i = 1 に対応する鍵導出鍵を記述する.
⋮
COUNT = ⟨NumberOfTrialsForEachTestSubset − 1⟩   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ のデータの組について記述する.
L = 512                                    ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する L を記述する.
KI = dc6f ... c8f2                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する鍵導出鍵を記述する.
```

*3 KDF in Feedback Mode の場合, NumberOfTrialsForEachTestSubset 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.
L = 512                                    ♯ i = 0 に対応する L を記述する.
KI = e571 ... 519f                         ♯ i = 0 に対応する鍵導出鍵を記述する.
IVlen = 256                                ♯ i = 0 に対応する IV のビット長を記述する.
IV = 1cf7 ... 778d                         ♯ i = 0 に対応する IV を記述する.

COUNT = 1                                  ♯ i = 1 のデータの組について記述する.
L = 512                                    ♯ i = 1 に対応する L を記述する.
KI = 9f15 ... 4d17                         ♯ i = 1 に対応する鍵導出鍵を記述する.
IVlen = 256                                ♯ i = 1 に対応する IV のビット長を記述する.
IV = 1cf7 ... 778d                         ♯ i = 1 に対応する IV を記述する.
⋮
COUNT = ⟨NumberOfTrialsForEachTestSubset − 1⟩   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ のデータの組について記述する.
L = 512                                    ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する L を記述する.
KI = dc6f ... c8f2                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する鍵導出鍵を記述する.
IVlen = 256                                ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する IV のビット長を記述する.
IV = 1cf7 ... 778d                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する IV を記述する.
```

2.1.4 レスポンスファイル (*.rsp)

表6: NIST SP800-108 に記載された鍵導出関数 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 ―鍵確立手法― 上の表記との対応	値の表記	例示
鍵導出関数	ヘッダ	AlgorithmName	KDF_in_NIST_SP800_108		文字列	[AlgorithmName = KDF_in_NIST_SP800_108]
		KDFMode	鍵導出関数識別子		文字列	[KDFMode = KDFinCounterMode]
		PRF	PRF 識別子		文字列	[PRF = HMAC_SHA512]
		PRFInputWithCounter	(counter を含めた PRF の入力とするかどうか)(counter を含める:True,counter を含めない:False)		文字列	[PRFInputWithCounter = True]
		CTRLOCATION	(counter の挿入位置)BEFORE_FIXED		文字列	[CTRLOCATION = BEFORE_FIXED]
		RLEN	counter i のビット長		10 進表記	[RLEN = 32]
		LdivisibleBy8	8 の倍数の L のサポートの有無 (有:True, 無:False)		文字列	[LdivisibleBy8 = True]
		BitLengthOfKeyForKSltB	HMAC を使った PRF 選択時, B 未満の HMAC 鍵のビット長. CMAC を使った PRF 選択時, タグは省略.		10 進表記	[BitLengthOfKeyForKSltB = 256]
		BitLengthOfKeyForKSeqB	HMAC を使った PRF 選択時, B に等しい HMAC 鍵のビット長. CMAC を使った PRF 選択時, タグは省略.		10 進表記	[BitLengthOfKeyForKSeqB = 1024]
		BitLengthOfKeyForKSgtB	HMAC を使った PRF 選択時, B より大きい HMAC 鍵のビット長. CMAC を使った PRF 選択時, タグは省略.		10 進表記	[BitLengthOfKeyForKSgtB = 2048]
		BitLengthOfIVForIVLeneq0	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) = 0$ なる IV を IUT がサポートする場合, 0. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.		10 進表記	[BitLengthOfIVForIVLeneq0 = 0]
		BitLengthOfIVForIVLenlth	KDF in Feedback Mode の選択時, $0 < \mathbf{len}(IV) < h$ なる IV を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.		10 進表記	[BitLengthBitLengthOfIVForIVLenlth = 256]
		BitLengthOfIVForIVLeneqh	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) = h$ なる IV を IUT がサポートする場合, そのビット長. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.		10 進表記	[BitLengthOfIVForIVLeneqh = 512]
		BitLengthOfIVForIVLength	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) > h$ なる IV を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.		10 進表記	[BitLengthOfIVForIVLength = 768]
		MinLDivisibleByH	h で割り切れる L の, IUT がサポートする範囲の最小値		10 進表記	[MinLDivisibleByH = 512]
		MaxLDivisibleByH	h で割り切れる L の, IUT がサポートする範囲の最大値		10 進表記	[MaxLDivisibleByH = 2048]
		MinLDivisibleBy8	(h で割り切れない)8 の倍数の L の, IUT がサポートする範囲の最小値		10 進表記	[MinLDivisibleBy8 = 112]
		MaxLDivisibleBy8	(h で割り切れない)8 の倍数の L の, IUT がサポートする範囲の最大値		10 進表記	[MaxLDivisibleBy8 = 1280]
		NumberOfTestSubsets	試験の部分集合の数		10 進表記	[NumberOfTestSubsets = 12]
		NumberOfTrialsForEachTestSubset	試験の各部分集合の中で, 導出する keying material の数		10 進表記	[NumberOfTrialsForEachTestSubset = 10]
	試験部分集合 *1 *2 *3	COUNT	0 以上 NumberOfTrialsForEachTestSubset 未満の整数		10 進表記	COUNT = 0
		L	導出する keying material (K_0) のビット長 (L)	L	10 進表記	L = 512
		KI	鍵導出鍵 (K_I)	K_I	16 進表記	KI = 2f9a ... 3664
		IVlen	(KDF in Feedback Mode の選択時,) IV のビット長	$\mathbf{len}(IV)$	10 進表記	IVlen = 256
		IV	(KDF in Feedback Mode の選択時,) IV	IV	16 進表記	IV = 1cf7 ... 778d
		FixedInputDataByteLen	【出力】$FixedInput$ のバイト長		10 進表記	FixedInputDataByteLen = 55
		FixedInputData	【出力】$FixedInput$	$FixedInput$	16 進表記	FixedInputData = 0c51 ... 0200
		KO	【出力】keying material (K_0)	K_0	16 進表記	KO = fe6b ... 6681

*1 KDF in Counter Mode 及び KDF in Double-Pipeline Iteration Mode の場合, PRF(HMAC 又は CMAC) の選択及び IUT がサポートする L 値の範囲の組みあわせに対応して, 最大 12 個の部分集合を記載する. KDF in Feedback Mode の場合, PRF(HMAC 又は CMAC) の選択, IUT がサポートする L 値の範囲, IUT がサポートする IV の長さの組みあわせに対応して, 最大 48 個の部分集合を記載する.

*2 KDF in Counter Mode 及び KDF in Double-Pipeline Iteration Mode の場合, NumberOfTrialsForEachTestSubset 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.
L = 512                                    ♯ i = 0 に対応する L を記述する.
KI = e571 ... 519f                         ♯ i = 0 に対応する鍵導出鍵を記述する.
FixedInputDataByteLen = 55                 ♯ i = 0 に対応する, ベンダーが指定した FixedInput のバイト長を記述する.
FixedInputData = 0c51 ... 0200             ♯ i = 0 に対応する, ベンダーが指定した FixedInput の値を記述する.
KO = fe6b ... 6681                         ♯ i = 0 に対応して, IUT が導出した keying material K0 の期待値.

COUNT = 1                                  ♯ i = 1 のデータの組について記述する.
L = 512                                    ♯ i = 1 に対応する L を記述する.
KI = 9f15 ... 4d17                         ♯ i = 1 に対応する鍵導出鍵を記述する.
FixedInputDataByteLen = 55                 ♯ i = 1 に対応する, ベンダーが指定した FixedInput のバイト長を記述する.
FixedInputData = 0c51 ... 0200             ♯ i = 1 に対応する, ベンダーが指定した FixedInput の値を記述する.
KO = fe6b ... 6681                         ♯ i = 1 に対応して, IUT が導出した keying material K0.
⋮
COUNT = ⟨NumberOfTrialsForEachTestSubset − 1⟩   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ のデータの組について記述する.
L = 512                                    ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する L を記述する.
KI = dc6f ... c8f2                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する鍵導出鍵を記述する.
FixedInputDataByteLen = 55                 ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する, ベンダーが指定した FixedInput のバイト長を記述する.
FixedInputData = 0c51 ... 0200             ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する, ベンダーが指定した FixedInput の値を記述する.
KO = fe6b ... 6681                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応して, IUT が導出した keying material K0.
```

*3 KDF in Feedback Mode の場合, NumberOfTrialsForEachTestSubset 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.
L = 512                                    ♯ i = 0 に対応する L を記述する.
KI = e571 ... 519f                         ♯ i = 0 に対応する鍵導出鍵を記述する.
IVlen = 256                                ♯ i = 0 に対応する IV のビット長を記述する.
IV = 1cf7 ... 778d                         ♯ i = 0 に対応する IV を記述する.
FixedInputDataByteLen = 55                 ♯ i = 0 に対応する, ベンダーが指定した FixedInput のバイト長を記述する.
FixedInputData = 0c51 ... 0200             ♯ i = 0 に対応する, ベンダーが指定した FixedInput の値を記述する.
KO = fe6b ... 6681                         ♯ i = 0 に対応して, IUT が導出した keying material K0.

COUNT = 1                                  ♯ i = 1 のデータの組について記述する.
L = 512                                    ♯ i = 1 に対応する L を記述する.
KI = 9f15 ... 4d17                         ♯ i = 1 に対応する鍵導出鍵を記述する.
IVlen = 256                                ♯ i = 1 に対応する IV のビット長を記述する.
IV = 1cf7 ... 778d                         ♯ i = 1 に対応する IV を記述する.
FixedInputDataByteLen = 55                 ♯ i = 1 に対応する, ベンダーが指定した FixedInput のバイト長を記述する.
FixedInputData = 0c51 ... 0200             ♯ i = 1 に対応する, ベンダーが指定した FixedInput の値を記述する.
KO = fe6b ... 6681                         ♯ i = 1 に対応して, IUT が導出した keying material K0.
⋮
COUNT = ⟨NumberOfTrialsForEachTestSubset − 1⟩   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ のデータの組について記述する.
L = 512                                    ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する L を記述する.
KI = dc6f ... c8f2                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する鍵導出鍵を記述する.
IVlen = 256                                ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する IV のビット長を記述する.
IV = 1cf7 ... 778d                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する IV を記述する.
FixedInputDataByteLen = 55                 ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する, ベンダーが指定した FixedInput のバイト長を記述する.
FixedInputData = 0c51 ... 0200             ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する, ベンダーが指定した FixedInput の値を記述する.
KO = fe6b ... 6681                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応して, IUT が導出した keying material K0.
```

2.1.5 結果ファイル (*.out)

表7: NIST SP800-108 に記載された鍵導出関数 結果ファイル

機能	分類	タグ	内容	値の表記	例示
鍵導出関数	ヘッダ	AlgorithmName	KDF_in_NIST_SP800_108	文字列	[AlgorithmName = KDF_in_NIST_SP800_108]
		KDFMode	鍵導出関数識別子	文字列	[KDFMode = KDFinCounterMode]
		PRF	PRF 識別子	文字列	[PRF = HMAC_SHA512]
		PRFInputWithCounter	(counter を含めた PRF の入力とするかどうか)(counter を含める:True,counter を含めない:False)	文字列	[PRFInputWithCounter = True]
		CTRLOCATION	(counter の挿入位置)BEFORE_FIXED	文字列	[CTRLOCATION = BEFORE_FIXED]
		RLEN	counter i のビット長	10 進表記	[RLEN = 32]
		LdivisibleBy8	8 の倍数の L のサポートの有無 (有:True, 無:False)	文字列	[LdivisibleBy8 = True]
		BitLengthOfKeyForKSltB	HMAC を使った PRF 選択時, B 未満の HMAC 鍵のビット長. CMAC を使った PRF 選択時, タグは省略.	10 進表記	[BitLengthOfKeyForKSltB = 256]
		BitLengthOfKeyForKSeqB	HMAC を使った PRF 選択時, B に等しい HMAC 鍵のビット長. CMAC を使った PRF 選択時, タグは省略.	10 進表記	[BitLengthOfKeyForKSeqB = 1024]
		BitLengthOfKeyForKSgtB	HMAC を使った PRF 選択時, B より大きい HMAC 鍵のビット長. CMAC を使った PRF 選択時, タグは省略.	10 進表記	[BitLengthOfKeyForKSgtB = 2048]
		BitLengthOfIVForIVLeneq0	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) = 0$ なる IV を IUT がサポートする場合, 0. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.	10 進表記	[BitLengthOfIVForIVLeneq0 = 0]
		BitLengthOfIVForIVLenlth	KDF in Feedback Mode の選択時, $0 < \mathbf{len}(IV) < h$ なる IV を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.	10 進表記	[BitLengthBitLengthOfIVForIVLenlth = 256]
		BitLengthOfIVForIVLeneqh	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) = h$ なる IV を IUT がサポートする場合, そのビット長. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.	10 進表記	[BitLengthOfIVForIVLeneqh = 512]
		BitLengthOfIVForIVLength	KDF in Feedback Mode の選択時, $\mathbf{len}(IV) > h$ なる IV を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, -1. KDF in Counter Mode 又は KDF in Double-Pipeline Iteration Mode 選択時, タグは省略.	10 進表記	[BitLengthOfIVForIVLength = 768]
		MinLDivisibleByH	h で割り切れる L の, IUT がサポートする範囲の最小値	10 進表記	[MinLDivisibleByH = 512]
		MaxLDivisibleByH	h で割り切れる L の, IUT がサポートする範囲の最大値	10 進表記	[MaxLDivisibleByH = 2048]
		MinLDivisibleBy8	(h で割り切れない)8 の倍数の L の, IUT がサポートする範囲の最小値	10 進表記	[MinLDivisibleBy8 = 112]
		MaxLDivisibleBy8	(h で割り切れない)8 の倍数の L の, IUT がサポートする範囲の最大値	10 進表記	[MaxLDivisibleBy8 = 1280]
		NumberOfTestSubsets	試験の部分集合の数	10 進表記	[NumberOfTestSubsets = 12]
		NumberOfTrialsForEachTestSubset	試験の各部分集合の中で, 導出する keying material の数	10 進表記	[NumberOfTrialsForEachTestSubset = 10]
		〈 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．