2010 情財第 538 号

# 企業・個人の情報セキュリティ対策事業

# 暗号アルゴリズム実装試験ツールの機能追加

# JCATT ファイルフォーマット仕様書

# GCM/GMAC

2012 年 5 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.
- ASCII 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 GCM/GMAC

GCM(Galois/Counter Mode)/GMAC 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.

各表におけるブロック暗号の識別子は次表の通り.

表 1: ブロック暗号識別子

| ブロック暗号識別子 | 対応するブロック番号 |
|---|---|
| M_BlockCipher_AES | AES |
| M_BlockCipher_CAMELLIA | Camellia |
| M_BlockCipher_CIPHERUNICORN_A | CIPHERUNICORN-A |
| M_BlockCipher_HIEROCRYPT_3 | Hierocrypt-3 |
| M_BlockCipher_SC2000 | SC2000 |

## 2.1 パラメータファイル (*.par)

表 2: GCM/GMAC パラメータファイル

| 機能 | タグ | 内容 |
|---|---|---|
| (共通) | [Algorithm Name] | GCM/GMAC |
| 暗号化 | [Function Name] | Encryption |
| | [Block Cipher] | GCM/GMAC 内部で使用するブロック暗号識別子 |
| | [Bitlength of Key] | 鍵のビット長. 128 または 192 または 256 [10 進数表記] |
| | [Min BitLength of IV] | IV のビット長の最小値 [10 進数表記] |
| | [Max BitLength of IV] | IV のビット長の最大値 [10 進数表記] |
| | [IV Generation] | IV 生成. 外部 (External) あるいは内部 (Internal) |
| | [Min BitLength of Plaintext] | 平文のビット長の最小値 [10 進数表記] |
| | [Max BitLength of Plaintext] | 平文のビット長の最大値 [10 進数表記] |
| | [Min BitLength of AAD] | AAD のビット長の最小値 [10 進数表記] |
| | [Max BitLength of AAD] | AAD のビット長の最大値 [10 進数表記] |
| | [Bitlength of Tag] | Tag のビット長. 128, 120, 112, 104, 96, 64, 32 のいずれかひとつを設定する. [10 進数表記] |
| | [Number of Plaintexts] | 平文の個数 [10 進数表記] |
| 復号 | [Function Name] | Decryption |
| | [Block Cipher] | GCM/GMAC 内部で使用するブロック暗号識別子 |
| | [Bitlength of Key] | 鍵のビット長. 128 または 192 または 256 [10 進表記] |
| | [Min BitLength of IV] | IV のビット長の最小値 [10 進数表記] |
| | [Max BitLength of IV] | IV のビット長の最大値 [10 進数表記] |
| | [Min BitLength of Ciphertext] | 暗号文のビット長の最小値 [10 進数表記] |
| | [Max BitLength of Ciphertext] | 暗号文のビット長の最大値 [10 進数表記] |
| | [Min BitLength of AAD] | AAD のビット長の最小値 [10 進数表記] |
| | [Max BitLength of AAD] | AAD のビット長の最大値 [10 進数表記] |
| | [Bitlength of Tag] | Tag のビット長. 128, 120, 112, 104, 96, 64, 32 のいずれかひとつを設定する. [10 進数表記] |
| | [Number of Ciphertexts] | 暗号文の個数 [10 進数表記] |
| | [Rate of Fail Data] | 改ざんデータの割合 (%) |

## 2.2 リクエストファイル (*.req)

表 3: GCM/GMAC リクエストファイル

| 機能 | タグ | 内容 |
|---|---|---|
| (共通) | [Algorithm Name] | GCM/GMAC |
| 暗号化 | [Function Name] | Encryption |
| | [Block Cipher] | GCM/GMAC 内部で使用するブロック暗号識別子 |
| | [Bitlength of Key] | 鍵のビット長. 128 または 192 または 256 [10 進表記] |
| | [Min BitLength of IV] | IV のビット長の最小値 [10 進数表記] |
| | [Max BitLength of IV] | IV のビット長の最大値 [10 進数表記] |
| | [IV Generation] | IV 生成. 外部 (External) あるいは内部 (Internal) |
| | [Min BitLength of Plaintext] | 平文のビット長の最小値 [10 進数表記] |
| | [Max BitLength of Plaintext] | 平文のビット長の最大値 [10 進数表記] |
| | [Min BitLength of AAD] | AAD のビット長の最小値 [10 進数表記] |
| | [Max BitLength of AAD] | AAD のビット長の最大値 [10 進数表記] |
| | [Bitlength of Tag] | Tag のビット長. 128, 120, 112, 104, 96, 64, 32 のいずれかひとつを設定する. [10 進表記] |
| | [Number of Plaintexts] | 平文の個数 [10 進数表記] |
| | [Key][1] | 鍵 [16 進表記] |
| | [IV][1] | IV[16 進表記]. IV が内部生成の場合，空行 |
| | [Plaintext][1] | 平文 [16 進表記] |
| | [AAD][1] | AAD[16 進表記] |
| | [Ciphertext][1] | 暗号文 [空行] |
| | [Tag][1] | Tag[空行] |
| 復号 | [Function Name] | Decryption |
| | [Block Cipher] | GCM/GMAC 内部で使用するブロック暗号識別子 |
| | [Bitlength of Key] | 鍵のビット長. 128 または 192 または 256 [10 進表記] |
| | [Min BitLength of IV] | IV のビット長の最小値 [10 進数表記] |
| | [Max BitLength of IV] | IV のビット長の最大値 [10 進数表記] |
| | [Min BitLength of Ciphertext] | 暗号文のビット長の最小値 [10 進数表記] |
| | [Max BitLength of Ciphertext] | 暗号文のビット長の最大値 [10 進数表記] |
| | [Min BitLength of AAD] | AAD のビット長の最小値 [10 進数表記] |
| | [Max BitLength of AAD] | AAD のビット長の最大値 [10 進数表記] |
| | [Bitlength of Tag] | Tag のビット長. 128, 120, 112, 104, 96, 64, 32 のいずれかひとつを設定する.[10 進表記] |
| | [Number of Ciphertexts] | 暗号文の個数 [10 進数表記] |
| | [Key][2] | 鍵 [16 進表記] |
| | [IV][2] | IV[16 進表記] |
| | [Ciphertext][2] | 暗号文 [16 進表記] |
| | [AAD][2] | AAD[16 進表記] |
| | [Plaintext][2] | 平文 [空行] |
| | [Tag][2] | Tag[16 進表記] |

**注**

1. [Number of Plaintexts] 個の鍵 [Key] と IV[IV] と平文 [Plaintext] と AAD[AAD] と空行の暗号文 [Ciphertext] と空行の Tag[Tag] を以下のようにデータを記述する.

   [Key]
   . . . ♯ 1 つ目の鍵を記述する.

   [IV]
   . . . ♯ 1 つ目の IV を記述する. IV が内部生成の場合, 何も記述しない空行を表示

   [Plaintext]
   . . . ♯ 1 つ目の平文を記述する.

   [AAD]
   . . . ♯ 1 つ目の AAD を記述する.

   [Ciphertext]
   . . . ♯ [何も記述しない空行を表示]

   [Tag]
   . . . ♯ [何も記述しない空行を表示]

   [Key]
   . . . ♯ 2 つ目の鍵を記述する.

   [IV]
   . . . ♯ 2 つ目の IV を記述する. IV が内部生成の場合, 何も記述しない空行を表示

   [Plaintext]
   . . . ♯ 2 つ目の平文を記述する.

   [AAD]
   . . . ♯ 2 つ目の AAD を記述する.

   [Ciphertext]
   . . . ♯ [何も記述しない空行を表示]

   [Tag]
   . . . ♯ [何も記述しない空行を表示]

2. [Number of Ciphertexts] 個の鍵 [Key] と IV[IV] と暗号文 [Ciphertext] と AAD[AAD] と空行の平文 [Plaintext] と Tag[Tag] を以下のようにデータを記述する.

   [Key]
   . . . ♯ 1 つ目の鍵を記述する.

   [IV]
   . . . ♯ 1 つ目の IV を記述する.

   [Ciphertext]
   . . . ♯ 1 つ目の暗号文を記述する.

   [AAD]
   . . . ♯ 1 つ目の AAD を記述する.

   [Plaintext]
   . . . ♯ [何も記述しない空行を表示]

   [Tag]
   . . . ♯ 1 つ目の Tag を記述する.

[Key]
. . . ♯ 2 つ目の鍵を記述する.

[IV]
. . . ♯ 2 つ目の IV を記述する.

[Ciphertext]
. . . ♯ 2 つ目の暗号文を記述する.

[AAD]
. . . ♯ 2 つ目の AAD を記述する.

[Plaintext]
. . . ♯ [何も記述しない空行を表示]

[Tag]
. . . ♯ 2 つ目の Tag を記述する.

### 2.3 Facts ファイル (*.fax)

表 4: GCM/GMAC Facts ファイル

| 機能 | タグ | 内容 |
|---|---|---|
| (共通) | [Algorithm Name] | GCM/GMAC |
| 暗号化 | [Function Name] | Encryption |
| | [Block Cipher] | GCM/GMAC 内部で使用するブロック暗号識別子 |
| | [Bitlength of Key] | 鍵のビット長. 128 または 192 または 256 [10 進表記] |
| | [Min BitLength of IV] | IV のビット長の最小値 [10 進数表記] |
| | [Max BitLength of IV] | IV のビット長の最大値 [10 進数表記] |
| | [IV Generation] | IV 生成. 外部 (External) あるいは内部 (Internal) |
| | [Min BitLength of Plaintext] | 平文のビット長の最小値 [10 進数表記] |
| | [Max BitLength of Plaintext] | 平文のビット長の最大値 [10 進数表記] |
| | [Min BitLength of AAD] | AAD のビット長の最小値 [10 進数表記] |
| | [Max BitLength of AAD] | AAD のビット長の最大値 [10 進数表記] |
| | [Bitlength of Tag] | Tag のビット長. 128, 120, 112, 104, 96, 64, 32 のいずれかひとつを設定する.[10 進表記] |
| | [Number of Plaintexts] | 平文の個数 [10 進数表記] |
| | [Key][1] | 鍵 [16 進表記] |
| | [IV][1] | IV[16 進表記]. IV が内部生成の場合，空行 |
| | [Plaintext][1] | 平文 [16 進表記] |
| | [AAD][1] | AAD[16 進表記] |
| | [Ciphertext][1] | 暗号文 [16 進表記]. IV が外部生成の場合のみ. GMAC の試験の場合は本内容は使用しない. |
| | [Tag][1] | Tag[16 進表記]. IV が外部生成の場合のみ. |

次のページに続く

表 5: GCM/GMAC Facts ファイル (続き)

| 機能 | タグ | 内容 |
|---|---|---|
| 復号 | [Function Name] | Decryption |
| | [Block Cipher] | GCM/GMAC 内部で使用するブロック暗号識別子 |
| | [Bitlength of Key] | 鍵のビット長. 128 または 192 または 256 [10 進表記] |
| | [Min BitLength of IV] | IV のビット長の最小値 [10 進数表記] |
| | [Max BitLength of IV] | IV のビット長の最大値 [10 進数表記] |
| | [Min BitLength of Ciphertext] | 暗号文のビット長の最小値 [10 進数表記] |
| | [Max BitLength of Ciphertext] | 暗号文のビット長の最大値 [10 進数表記] |
| | [Min BitLength of AAD] | AAD のビット長の最小値 [10 進数表記] |
| | [Max BitLength of AAD] | AAD のビット長の最大値 [10 進数表記] |
| | [Bitlength of Tag] | Tag のビット長. 128, 120, 112, 104, 96, 64, 32 のいずれかひとつを設定する.[10 進表記] |
| | [Number of Ciphertexts] | 暗号文の個数 [10 進数表記] |
| | [Key][2] | 鍵 [16 進表記] |
| | [IV][2] | IV[16 進表記] |
| | [Ciphertext][2] | 暗号文 [16 進表記] |
| | [AAD][2] | AAD[16 進表記] |
| | [Plaintext][2] | 平文 [16 進表記]. 復号に失敗した場合は, [Plaintext] データの該当行に INVALID と記載 |
| | [Tag][2] | Tag[16 進表記] |

**注**

1. [Number of Plaintexts] 個の鍵 [Key] と IV[IV] と平文 [Plaintext] と AAD[AAD] と暗号文 [Ciphertext] と Tag[Tag] を以下のようにデータを記述する.

   [Key]
   ... ♯ 1 つ目の鍵を記述する.

   [IV]
   ... ♯ 1 つ目の IV を記述する. IV が内部生成の場合, 何も記述しない空行を表示

   [Plaintext]
   ... ♯ 1 つ目の平文を記述する.

   [AAD]
   ... ♯ 1 つ目の AAD を記述する.

   [Ciphertext]
   ... ♯ 1 つ目の暗号文を記述する.

   [Tag]
   ... ♯ 1 つ目の Tag を記述する.

   [Key]
   ... ♯ 2 つ目の鍵を記述する.

   [IV]
   ... ♯ 2 つ目の IV を記述する. IV が内部生成の場合, 何も記述しない空行を表示

   [Plaintext]
   ... ♯ 2 つ目の平文を記述する.

[AAD]
. . . ♯ 2 つ目の AAD を記述する.

[Ciphertext]
. . . ♯ 2 つ目の暗号文を記述する.

[Tag]
. . . ♯ 2 つ目の Tag を記述する.

2. [Number of Ciphertexts] 個の鍵 [Key] と IV[IV] と暗号文 [Ciphertext] と AAD[AAD] と平文 [Plaintext] と Tag[Tag] を以下のようにデータを記述する.

   [Key]
   . . . ♯ 1 つ目の鍵を記述する.

   [IV]
   . . . ♯ 1 つ目の IV を記述する.

   [Ciphertext]
   . . . ♯ 1 つ目の暗号文を記述する.

   [AAD]
   . . . ♯ 1 つ目の AAD を記述する.

   [Plaintext]
   . . . ♯ 1 つ目の平文を記述する.

   [Tag]
   . . . ♯ 1 つ目の Tag を記述する.

   [Key]
   . . . ♯ 2 つ目の鍵を記述する.

   [IV]
   . . . ♯ 2 つ目の IV を記述する.

   [Ciphertext]
   . . . ♯ 2 つ目の暗号文を記述する.

   [AAD]
   . . . ♯ 2 つ目の AAD を記述する.

   [Plaintext]
   . . . ♯ 2 つ目の平文を記述する.

   [Tag]
   . . . ♯ 2 つ目の Tag を記述する.

## 2.4 レスポンスファイル (*.rsp)

表 6: GCM/GMAC レスポンスファイル

| 機能 | タグ | 内容 |
|---|---|---|
| (共通) | [Algorithm Name] | GCM/GMAC |
| 暗号化 | [Function Name] | Encryption |
| | [Block Cipher] | GCM/GMAC 内部で使用するブロック暗号識別子 |
| | [Bitlength of Key] | 鍵のビット長. 128 または 192 または 256 [10 進表記] |
| | [Min BitLength of IV] | IV のビット長の最小値 [10 進数表記] |
| | [Max BitLength of IV] | IV のビット長の最大値 [10 進数表記] |
| | [IV Generation] | IV 生成. 外部 (External) あるいは内部 (Internal) |
| | [Min BitLength of Plaintext] | 平文のビット長の最小値 [10 進数表記] |
| | [Max BitLength of Plaintext] | 平文のビット長の最大値 [10 進数表記] |
| | [Min BitLength of AAD] | AAD のビット長の最小値 [10 進数表記] |
| | [Max BitLength of AAD] | AAD のビット長の最大値 [10 進数表記] |
| | [Bitlength of Tag] | Tag のビット長. 128, 120, 112, 104, 96, 64, 32 のいずれかひとつを設定する。[10 進表記] |
| | [Number of Plaintexts] | 平文の個数 [10 進数表記] |
| | [Key][1] | 鍵 [16 進表記] |
| | [IV][1] | IV[16 進表記].IV が内部生成の場合は【出力】 |
| | [Plaintext][1] | 平文 [16 進表記] |
| | [AAD][1] | AAD[16 進表記] |
| | [Ciphertext][1] | 【出力】暗号文 [16 進表記]. GMAC の試験の場合は空行とする. |
| | [Tag][1] | 【出力】Tag[16 進表記]. |

次のページに続く

表 7: GCM/GMAC レスポンスファイル (続き)

| 機能 | タグ | 内容 |
|---|---|---|
| 復号 | [Function Name] | Decryption |
| | [Block Cipher] | GCM/GMAC 内部で使用するブロック暗号識別子 |
| | [Bitlength of Key] | 鍵のビット長. 128 または 192 または 256 [10 進表記] |
| | [Min BitLength of IV] | IV のビット長の最小値 [10 進数表記] |
| | [Max BitLength of IV] | IV のビット長の最大値 [10 進数表記] |
| | [Min BitLength of Ciphertext] | 暗号文のビット長の最小値 [10 進数表記] |
| | [Max BitLength of Ciphertext] | 暗号文のビット長の最大値 [10 進数表記] |
| | [Min BitLength of AAD] | AAD のビット長の最小値 [10 進数表記] |
| | [Max BitLength of AAD] | AAD のビット長の最大値 [10 進数表記] |
| | [Bitlength of Tag] | Tag のビット長. 128, 120, 112, 104, 96, 64, 32 のいずれかひとつを設定する.[10 進表記] |
| | [Number of Ciphertexts] | 暗号文の個数 [10 進数表記] |
| | [Key][2] | 鍵 [16 進表記] |
| | [IV][2] | IV[16 進表記] |
| | [Ciphertext][2] | 暗号文 [16 進表記] |
| | [AAD][2] | AAD[16 進表記] |
| | [Plaintext][2] | 【出力】平文 [16 進表記]. 復号に失敗した場合は, [Plaintext] データの該当行に INVALID と記載 |
| | [Tag][2] | Tag[16 進表記] |

**注**

1. [Number of Plaintexts] 個の鍵 [Key] と IV[IV] と平文 [Plaintext] と AAD[AAD] と【出力】暗号文 [Ciphertext] と【出力】Tag[Tag] を以下のようにデータを記述する.

   [Key]
   . . . ♯ 1 つ目の鍵を記述する.

   [IV]
   . . . ♯ 1 つ目の IV を記述する.

   [Plaintext]
   . . . ♯ 1 つ目の平文を記述する.

   [AAD]
   . . . ♯ 1 つ目の AAD を記述する.

   [Ciphertext]
   . . . ♯ 1 つ目の【出力】暗号文を記述する. GMAC の試験の場合は空行とする.

   [Tag]
   . . . ♯ 1 つ目の【出力】Tag を記述する.

   [Key]
   . . . ♯ 2 つ目の鍵を記述する.

   [IV]
   . . . ♯ 2 つ目の IV を記述する.

[Plaintext]
. . . ♯ 2 つ目の平文を記述する.

[AAD]
. . . ♯ 2 つ目の AAD を記述する.

[Ciphertext]
. . . ♯ 2 つ目の【出力】暗号文を記述する. GMAC の試験の場合は空行とする.

[Tag]
. . . ♯ 2 つ目の【出力】Tag を記述する.

2. [Number of Ciphertexts] 個の鍵 [Key] と IV[IV] と暗号文 [Ciphertext] と AAD[AAD] と【出力】平文 [Plaintext] と Tag[Tag] を以下のようにデータを記述する.

[Key]
. . . ♯ 1 つ目の鍵を記述する.

[IV]
. . . ♯ 1 つ目の IV を記述する.

[Ciphertext]
. . . ♯ 1 つ目の暗号文を記述する.

[AAD]
. . . ♯ 1 つ目の AAD を記述する.

[Plaintext]
. . . ♯ 1 つ目の【出力】平文を記述する.

[Tag]
. . . ♯ 1 つ目の Tag を記述する.

[Key]
. . . ♯ 2 つ目の鍵を記述する.

[IV]
. . . ♯ 2 つ目の IV を記述する.

[Ciphertext]
. . . ♯ 2 つ目の暗号文を記述する.

[AAD]
. . . ♯ 2 つ目の AAD を記述する.

[Plaintext]
. . . ♯ 2 つ目の【出力】平文を記述する.

[Tag]
. . . ♯ 2 つ目の Tag を記述する.

## 2.5 結果ファイル (*.out)

表 8: GCM/GMAC 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．