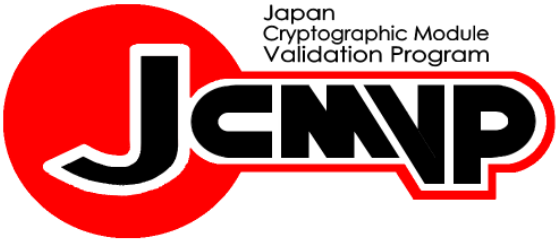
IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

暗号モジュール試験及び認証制度(JCMVP)



JCMVP
暗号アルゴリズム実装試験要件

ATR-01

Cryptographic Algorithm implementation Testing Requirements

平成 21 年１月８日

独立行政法人　情報処理推進機構

目次

JCMVP 暗号アルゴリズム実装試験要件

制定　平成 19 年 5 月 9 日　2007 情総第 22 号
最終改正　平成 21 年 1 月 21 日　2008 情総第 118 号　一部改正

1. 目的

本規程は、独立行政法人 情報処理推進機構 (以下「機構」という。) が、***暗号モジュール試験及び認証制度の基本規程*** (JCM-01) (以下「***制度基本規程***」という。) に基づいて、暗号モジュール認証機関 (以下「認証機関」という。) として実施する暗号モジュール試験及び認証制度 (JCMVP) (以下「本制度」という。) において、**暗号モジュール**に実装されているブロック暗号、ストリーム暗号、公開鍵暗号、メッセージ認証、ハッシュ関数、乱数生成器、鍵共有等の**承認されたセキュリティ機能**に対して、その入力値及び出力値の関係が所定の特性を示していることを確認するための**暗号アルゴリズム実装試験**の要件を定めるものである。

2. 用語

本規程で使用する用語は、***制度基本規程*** において使用する用語の例による。

3. 暗号アルゴリズム実装試験要件

機構は、**承認されたセキュリティ機能**を実装したものを検証するために、「暗号アルゴリズム実装試験ツール」を開発した。
暗号モジュール試験機関（以下、「試験機関」という。）は、**承認されたセキュリティ機能**に関する**暗号アルゴリズム実装試験**を「暗号アルゴリズム実装試験ツール」（以下、**JCATT**[Japan Cryptographic Algorithm implementation Testing Tool]という。)を用いて行うこととする。

JCATT の暗号アルゴリズム実装試験の対象となるのは、認証機関によって**承認されたセキュリティ機能**であり、それらは、***承認されたセキュリティ機能に関する仕様***(ASF-01)に規定されている。

JCATT の暗号アルゴリズム実装試験仕様は、以下の文書に、**承認されたセキュリティ機能**の種類別に規定されている。

＜公開鍵＞	暗号アルゴリズム実装試験仕様書 -公開鍵-	(ATR-01-A)
＜共通鍵＞	暗号アルゴリズム実装試験仕様書 -共通鍵-	(ATR-01-B)
＜ハッシュ＞	暗号アルゴリズム実装試験仕様書 -ハッシュ-	(ATR-01-C)
＜メッセージ認証＞	暗号アルゴリズム実装試験仕様書 -メッセージ認証-	(ATR-01-D)
＜乱数生成器＞	暗号アルゴリズム実装試験仕様書 -乱数生成器-	(ATR-01-E)
＜鍵確立手法＞	暗号アルゴリズム実装試験仕様書 -鍵確立手法-	(ATR-01-F)

附 則（平成 19 年５月９日 2007 情総第 22 号・全部改正）

この規程は、平成 19 年５月 15 日から施行する。

附　則（平成 19 年 10 月 29 日　2007 情総第 121 号・一部改正）

この規程は、平成 19 年 10 月 29 日から施行し、平成 19 年 10 月 26 日から適用する。

附　則（平成 21 年１月 21 日　2008 情総第 118 号・一部改正）

この規程は、平成 21 年１月８日から施行する。

改訂履歴

識別番号	ATR-01

改訂年月日	作成者・承認者	改訂内容
平成 18 年 10 月 16 日	上野・仲田	新規制定
平成 19 年５月９日	上野・仲田	全部改正
平成 19 年 10 月 29 日	櫻井・占部	一部改正
平成 21 年 1 月 21 日	井上・仲田	一部改正