暗号モジュール試験及び認証制度

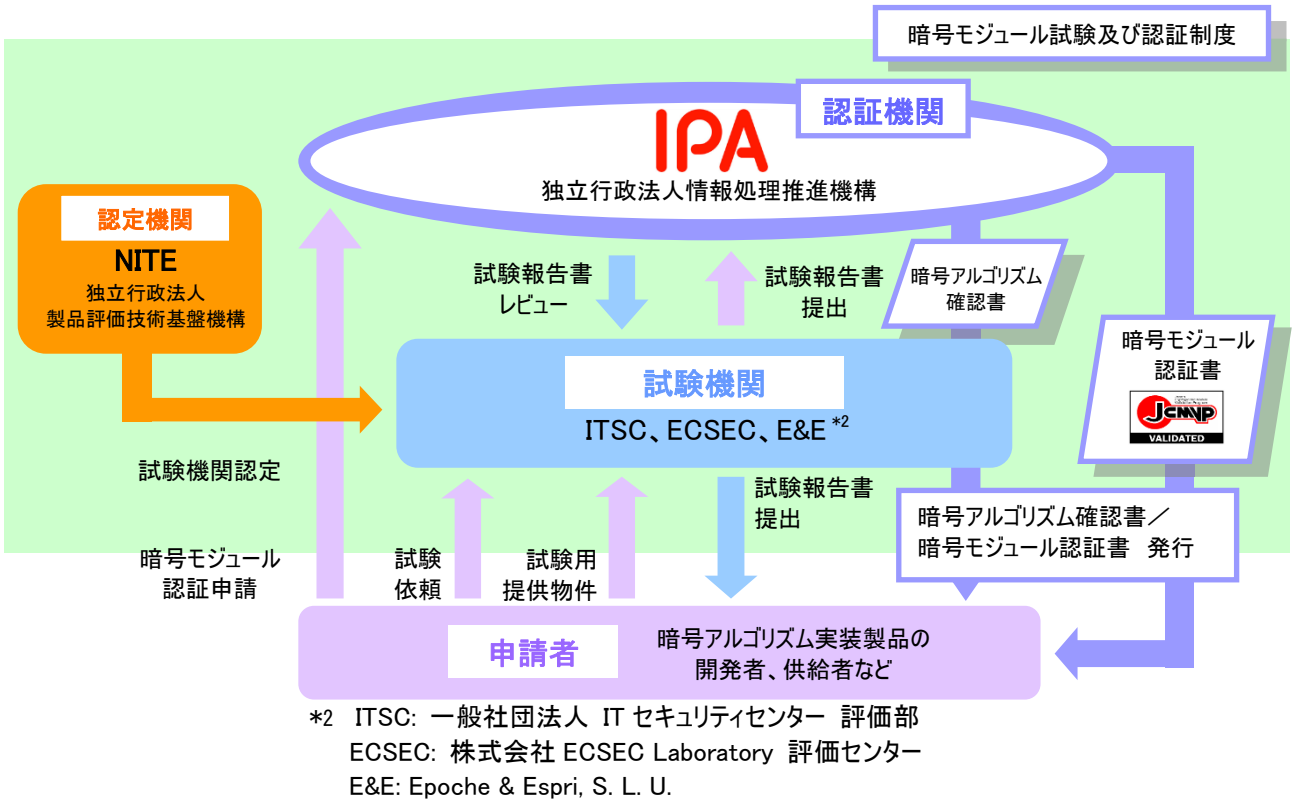
暗号モジュール試験及び認証制度（JCMVP： Japan Cryptographic Module Validation Program）とは、暗号モジュールに暗号アルゴリズムが適切に実装され、その鍵やパスワードといった重要情報が攻撃者から保護されるとともに、許可された者がいつでもその機能を確実に利用できることを、暗号モジュールのユーザが客観的に把握できるように設けられた第三者適合性評価制度です。

本制度が承認した暗号アルゴリズムを実装している暗号モジュール製品を対象に、暗号モジュールのセキュリティに関する国際規格 ISO/IEC 19790*1 の一致規格 JIS X 19790 に基づく試験・認証を実施します。

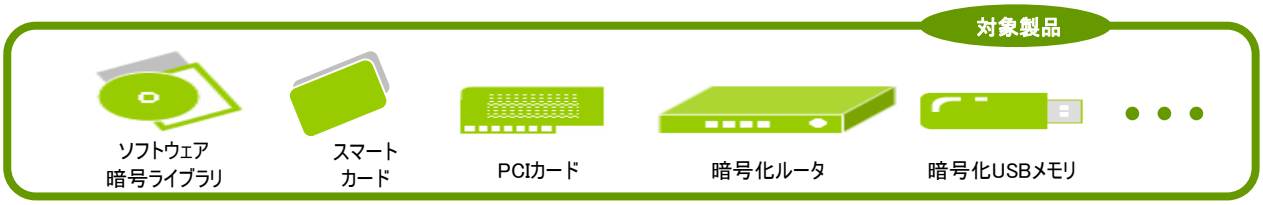
本制度は、製品認証制度の 1 つとして、独立行政法人情報処理推進機構（IPA）により運営されるものです。JCMVP は、IPA の登録商標です。

＊1　ISO/IEC 19790：米国及びカナダが運営する暗号モジュール試験及び認証制度（CMVP：Cryptographic Module Validation Program）で採用されている FIPS 140-2 を基に作成された暗号モジュールのセキュリティを確保するための要求事項を定めた国際規格。ここで、FIPS とは、米国連邦政府情報処理規格（Federal Information Processing Standards）のことです。

暗号モジュール試験及び認証制度の仕組み



＊2　ITSC：一般社団法人 IT セキュリティセンター 評価部
ECSEC：株式会社 ECSEC Laboratory 評価センター
E&E：Epoche & Espri, S. L. U.



独立行政法人**情報処理推進機構**

(2017.05.01)

暗号モジュール試験及び認証の手順

暗号モジュール試験の内容は、暗号アルゴリズム実装試験とその他の試験に大別されます。

暗号アルゴリズム実装試験では、暗号アルゴリズム実装試験ツール JCATT*3 を用いて、暗号アルゴリズムが適切に実装されていることを確認します。

その手順は、次の通りです。

（1） 暗号アルゴリズム実装試験ツールで作成した質問ファイルに含まれる値を、暗号アルゴリズムの実装に入力し、処理結果を回答ファイルに出力します。

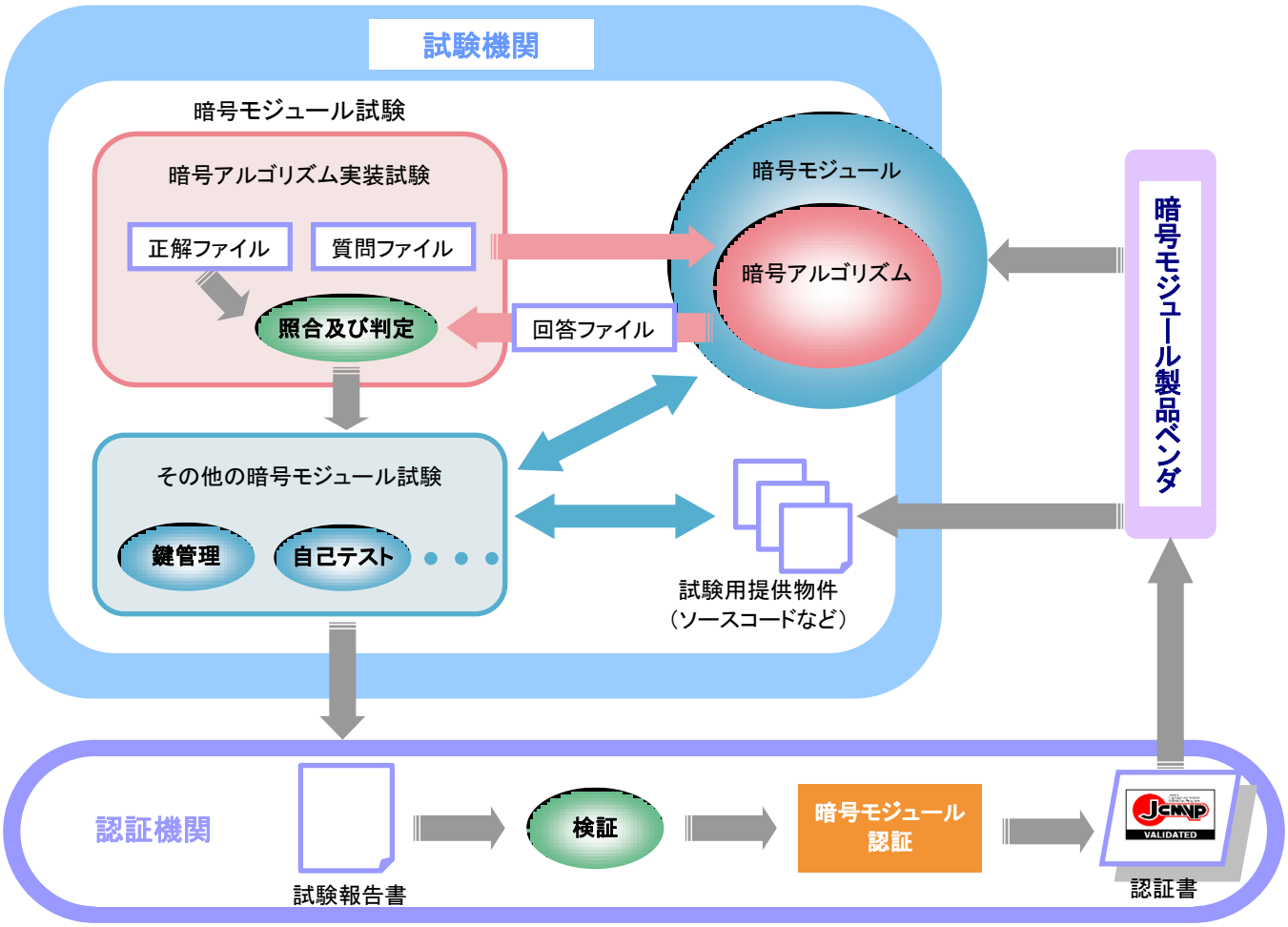
（2） 暗号アルゴリズム実装試験ツールにより、その回答ファイルとあらかじめ正しい出力結果を書き込んでおいた正解ファイルを照合して結果を判定します。

本制度では、CRYPTREC*4 が作成した電子政府推奨暗号リストに記載された暗号アルゴリズムを含む本制度で承認されたセキュリティ機能（次頁参照）に対して、暗号アルゴリズム実装試験を実施します。

その他の暗号モジュール試験では、暗号モジュールのセキュリティ要求事項（暗号鍵管理、自己テストなど）を満足していることを試験します。

暗号モジュール試験の結果は試験報告書にまとめられ、認証機関に提出されます。認証機関での検証の結果、適正であると確認されると、その暗号モジュールに対して暗号モジュール認証書が授与されます。

また、暗号アルゴリズム実装試験のみを独立して実施し、合格した実装に対して暗号アルゴリズム確認書が発行される「暗号アルゴリズム確認制度」を 2009 年 1 月より運用しております。



＊3 JCATT: Japan Cryptographic Algorithm implementation Testing Tool, JCMVP で開発した暗号アルゴリズム実装試験ツール

＊4 CRYPTREC: Cryptography Research and Evaluation Committees
電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討する。経済産業省及び総務省が共同で開催する暗号技術検討会と、独立行政法人情報処理推進機構及び国立研究開発法人情報通信研究機構が共同で開催する暗号技術評価委員会及び暗号技術活用委員会で構成。
CRYPTREC URL: http://www.cryptrec.go.jp/

本制度の対象とする暗号アルゴリズム

本制度では、「承認されたセキュリティ機能」を実装した暗号モジュールに対して、暗号モジュール認証を実施しています。

承認されたセキュリティ機能		
技術分類		暗号名称
公開鍵暗号	署名	**DSA, ECDSA, RSASSA-PKCS1-v1_5, RSASSA-PSS**
	守秘	RSA-OAEP
	鍵確立	**DH, ECDH, MQV, ECMQV, NIST SP800-56B**
共通鍵暗号	64 ビットブロック暗号	**3-key Triple DES**
	128 ビットブロック暗号	**AES,** Camellia
	ブロック暗号利用モード	**ECB, CBC, CFB, OFB, CTR, XTS**
	ストリーム暗号	KCipher-2
その他	ハッシュ関数	**SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256**
	メッセージ認証	**CCM, CMAC, GCM/GMAC, HMAC (HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-SHA-512/224, HMAC-SHA-512/256)**
	擬似乱数生成系	**NIST SP800-90A (Hash_DRBG, HMAC_DRBG, CTR_DRBG)**

注 1: CMVP で承認されたセキュリティ機能は太字で表示。
注 2: 2014 年 4 月に、安全性の高いアルゴリズム及び鍵長への移行を実施しました。詳しくは
https://www.ipa.go.jp/security/jcmvp/algorithm.html をご覧ください。

一方、「暗号アルゴリズム確認制度」では、「承認されたセキュリティ機能」に加えて、「暗号アルゴリズム確認対象非承認セキュリティ機能」に対しても暗号アルゴリズム確認を実施しています。

暗号アルゴリズム確認対象非承認セキュリティ機能		
技術分類		暗号名称
公開鍵暗号	鍵確立	PSEC-KEM
共通鍵暗号	64 ビットブロック暗号	CIPHERUNICORN-E, Hierocrypt-L1, MISTY1
	128 ビットブロック暗号	CIPHERUNICORN-A, CLEFIA, Hierocrypt-3, SC2000
	ストリーム暗号	Enocoro128-v2, MUGI, MULTI-S01
その他	メッセージ認証	PC-MAC-AES

「暗号アルゴリズム確認対象非承認セキュリティ機能」は、CRYPTREC が発行する推奨候補暗号リストに対応するもので、このリストに掲載されている暗号アルゴリズムが適切に実装されていることを確認可能です。

これらの暗号アルゴリズムは、暗号モジュール認証においては承認されていないセキュリティ機能として扱われます。したがって、「暗号アルゴリズム確認対象非承認セキュリティ機能」は、「承認されたセキュリティ機能」と異なり、機密性や完全性などのセキュリティを担うものとして、本制度の対象とする暗号モジュールの中で使用することはできません。

暗号モジュールのセキュリティレベル

暗号モジュール試験及び認証制度では、それぞれの暗号モジュールが取扱うデータの重要度や利用環境が多様であることにかんがみ、暗号モジュールのセキュリティ確保のための機能等に対する要求事項（セキュリティ要求事項）を 4 つのレベルで設定しています。

セキュリティレベル	各セキュリティレベルの概要
1	市販品として求められる基本的なセキュリティ要求事項を満たすレベル。セキュリティ確保のための物理的なメカニズムは要求されないレベル。
2	セキュリティレベル 1 に加え、タンパー証跡（暗号モジュールを開封した跡が残るようなシールなど）に関する要求事項を加えたレベル。また、管理者、ユーザといった役割ベースの認証機能を必須とする。
3	セキュリティレベル 2 に加え、タンパー検出・応答（暗号モジュールを開封したことを検出しデータ消去などの応答をする）に関する要求事項を加えたレベル。ID ベースの認証機能を必須とする。また、重要情報の入出力に関する要求事項が追加されている。
4	セキュリティレベル 3 に加え、いかなる物理的な攻撃に対してもタンパー検出・応答をするように完全に暗号モジュール部分を被覆保護する物理的メカニズムを加えたレベル。さらに、正常に動作する電圧・温度の範囲を超えた環境条件・変動に関する要求事項も追加されている。

暗号モジュール認証に関わる申請料金

認証機関への申請に際して、次表の申請料金が必要になります。

暗号モジュール認証申請等の種類		認証申請等の料金(税込) *5、*8、*9
暗号モジュール認証申請	セキュリティレベル 1 の場合	270,000 円
	セキュリティレベル 2 の場合	385,700 円
	セキュリティレベル 3 の場合	540,000 円
	セキュリティレベル 4 の場合	756,000 円
再認証 *6 保証継続 *7	セキュリティレベル 1 の場合	81,300 円
	セキュリティレベル 2 の場合	115,700 円
	セキュリティレベル 3 の場合	162,000 円
	セキュリティレベル 4 の場合	226,800 円
暗号アルゴリズム確認申請		21,600 円
英文暗号アルゴリズム確認書発行申請 英文暗号モジュール認証書発行申請 英文暗号モジュール認証報告書発行申請		3,800 円/枚
各種認証書、認証報告書再発行申請		3,800 円/枚

＊5: 上記申請手数料は、申請 1 件あたりの料金です。
＊6: 上記再認証申請手数料は、認証済み暗号モジュールを設計変更する場合に、そのセキュリティ要求事項に関する修正が全体の 30%以下の場合の料金です。
＊7: 上記保証継続申請手数料は、修正が暗号モジュールセキュリティ要件に関連した事項に影響を与えない場合の料金です。
＊8: 申請手数料は、申請の取下げがされても返金しません。
＊9: 暗号モジュール認証の場合において、旅費等の必要経費が生じたときは、暗号モジュール認証申請等の料金の他に別途当該必要経費を請求することがあります。
注: 試験実施に際しては別途試験費用が必要となります。試験費用は、セキュリティレベルなどの諸条件によって異なります。

問い合わせ先

独立行政法人情報処理推進機構
技術本部　セキュリティセンター
情報セキュリティ認証室（JCMVP 担当）

〒113-6591　東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコート　センターオフィス 16 階
TEL: 03-5978-7545　　FAX: 03-5978-7548
E-mail:　jcmvp-info@ipa.go.jp
■　JCMVP ホームページ
URL:　https://www.ipa.go.jp/security/jcmvp/