ITSC

暗号モジュール／暗号アルゴリズム試験

●CMVP/CAVP（米国・カナダ）及びJCMVP（日本）の暗号モジュール試験機関として暗号試験サービスを提供

暗号モジュール／暗号アルゴリズム試験制度

ITセキュリティセンターは米国NIST*とカナダCSE*が共同実施している「暗号モジュール／暗号アルゴリズム検証プログラム（CMVP/CAVP）」及び独立行政法人情報処理推進機構（IPA）が実施している「暗号モジュール試験及び認証制度（JCMVP）」の試験機関として認定されています。ITセキュリティセンターでは両制度で実施している暗号試験サービスおよびこれに係るコンサルティングサービスを実施しています。

NIST：National Institute of Standards and Technology　CSE：Communications Security Establishment

暗号試験の内容

対象となる暗号モジュール製品の例

スマートカード　USBトークン　PCIカード　ゲートウェイ　ソフトウエア暗号ライブラリ
ファイル暗号化ソフトウエア　その他暗号を使用しているハードウエアとソフトウエア

認証されたセキュリティ機能

セキュリティ機能は公開鍵、共通鍵、ハッシュ、メッセージ認証、乱数生成器、鍵確立手法からなっています。
CMVP/CAVPではFIPS PUB 140に基づきセキュリティ機能が認証されます。
JCMVPでは電子政府推奨暗号リストを中心にJIS X 19790に基づきセキュリティ機能が認定されます。

試験用提供物件（セキュリティレベルにより異なります）

暗号モジュール：
ハードウエア暗号モジュールの場合は物理的セキュリティに関する試験を実施します

セキュリティポリシ(SP：Security Policy)：
ブロック図及び必要に応じて暗号モジュールの写真を含む
《セキュリティポリシは暗号モジュール認証取得後に公開されます》

ベンダ証拠資料（Vendor Evidence）：
開発ドキュメント（設計書、回路図、ソースコード等）、利用者ドキュメント（マニュアル類）
状態遷移図及び状態遷移表（FSM：Finite State Model）

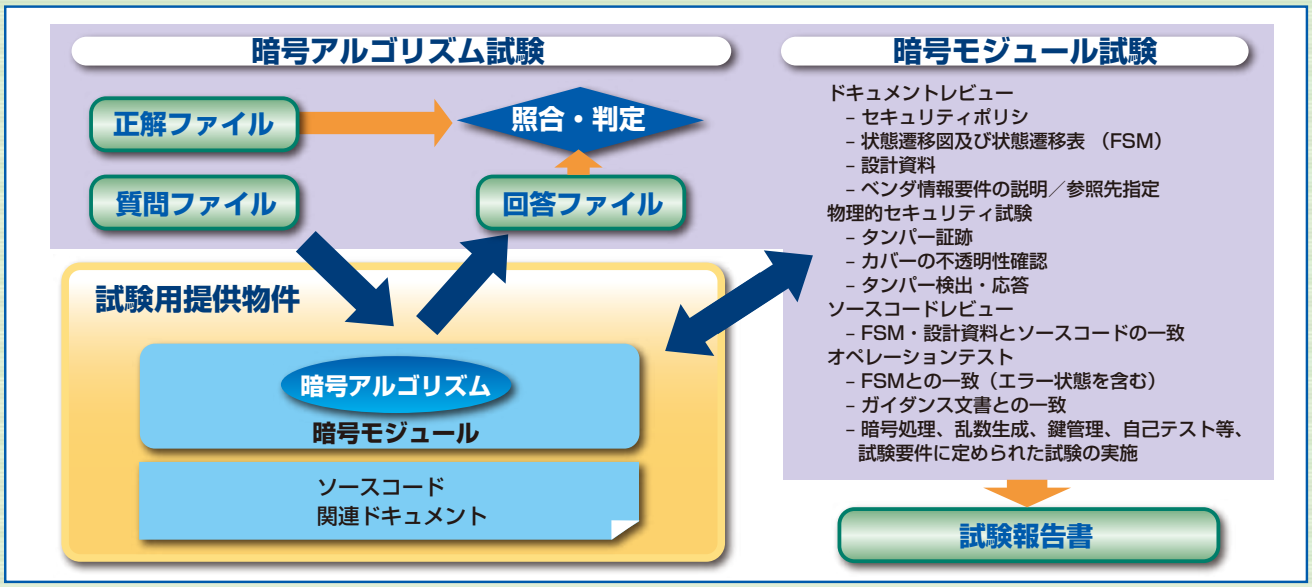
一般社団法人ITセキュリティセンター　URL：http://www.itsc.or.jp/

ITSC

暗号試験の手順

暗号モジュール試験／暗号アルゴリズム試験では以下のセキュリティ目標を確認します

- ●承認されたセキュリティ機能を使って正しく実装されている
- ●認可されていない操作や利用から暗号モジュールが保護されている
- ●暗号モジュールの内容の不当開示を防止している
- ●暗号モジュールと暗号アルゴリズムに対する認可されていない変更、代替、挿入、および削除を防止している
- ●暗号モジュールの動作状態を表示できる
- ●承認された動作モードで動作するときに、暗号モジュールが適切に実行される
- ●暗号モジュールの動作の誤りを検出して、誤りによる重要情報の危たい化を防止している



暗号試験のセキュリティ

セキュリティ要件	内　　容	セキュリティレベル			
		1	2	3	4
暗号モジュールの仕様	暗号モジュールの物理範囲、インタフェース等の仕様、セキュリティポリシ	●	●	●	●
暗号モジュールのポート及びインタフェース	入出力ポートの共有	●	●		
	入出力ポートの論理的/物理的分離			●	●
役割、サービス、及び認証	役割の選択	●			
	役割/IDベースのオペレータ認証		●		
	ID ベースのオペレータ認証			●	●
有限状態モデル	暗号モジュールの状態遷移	●	●	●	●
物理的セキュリティ	コーティング等の標準的保護	●	●	●	●
	タンパー証跡の提供		●	●	●
	タンパー検出と自己保護			●	●
	環境故障保護(EFP)/環境故障試験(EFT)				●
動作環境	単一オペレータモード、実行コードの保護、承認された完全性技術	●	●	●	●
	PP 準拠且つEAL2 のOSで動作、暗号プロセスの保護		●	●	●
	EAL3のOSで動作、暗号鍵、認証データ等の高信頼通信			●	●
	EAL4のOSで動作				●
暗号鍵管理	乱数生成及び鍵生成、鍵配送、鍵入出力、鍵のゼロ化等の鍵管理機構	●	●	●	●
	自動/手動による鍵確立	●	●		
	自動/知識分散による手動鍵確立			●	●
電磁妨害/電磁両立性(EMI/EMC)	商用向けEMI/EMC要求事項に適合	●	●		
	家庭向けEMI/EMC要求事項に適合			●	●
自己テスト	暗号モジュール起動時の自己テスト	●	●	●	●
設計保証(設計文書～ガイダンス文書)	設置手順、コンポーネント設計とセキュリティポリシの対応、ガイダンス	●	●	●	●
	ソースコード	●	●	●	●
	暗号モジュール配送時のセキュリティ維持手順、機能仕様		●	●	●
	高級言語による実装			●	●
	形式的モデル				●