INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2006 情財第 1056 号

暗号モジュール試験報告書作成支援ツール（CRYPTIPA）の開発　報告書

2007 年 5 月

独立行政法人 情報処理推進機構

目　次

1. はじめに

本報告書は、「暗号モジュール試験報告書作成支援ツール(CRYPTIPA)の改修」における開発成果をまとめたものであり、開発したソフトウェアの概要および詳細仕様を記述し、報告する。

1.1 開発の背景

電子政府の情報セキュリティを確保するためには、その基盤技術である暗号技術について、客観的な評価によって一定水準以上の安全性と信頼性を有するものを利用することが不可欠である。また、一定水準以上の安全性を確保するためには、暗号アルゴリズムの安全性確保だけでなく、暗号アルゴリズムをハードウェア、ファームウェア、またはソフトウェアに実装した暗号モジュールの安全性確保も必要である。

暗号モジュールの安全性確保については、米国が先行しており、暗号モジュールの評価基準および試験基準を用いた暗号モジュール認証制度が既に運用されている。また、その制度で用いられる試験基準は、試験機関が実際に試験を実施して得られた改善点等を反映するため、その都度更新が行われ、更に、運用ガイダンスも提供されている。

日本における暗号モジュール認証制度を立ち上げ、評価基準・試験基準の活用を本格化させるため、情報処理推進機構(以下、IPA と表記)が必要な準備を進めている。この作業の一環として、暗号モジュール試験基準のデータベースを構築し、基準策定の迅速化を図るとともに、将来的には、暗号モジュールの認証機関や試験機関、暗号製品ベンダ等が容易に利用できるデータベースとして、一昨年度「暗号モジュール試験基準データベースの開発」[1]を実施し、編集者／レビュー者ツール、管理者ツール、利用者ツールを開発し、データベースへの初期データとして基準情報の入力を行った。

暗号モジュール試験を実施するため、暗号モジュール試験報告書のフォーマット等の統一と作業の効率化を目的とし、昨年度「報告書作成支援ツール(以下、CRYPTIPA と表記)の開発」[2]を実施した。

そして、「安心」して利用できる IT 基盤の構築・維持のため、IPA は情報セキュリティ対策の強化、整備を進めており、2006 年 6 月から暗号モジュール試験及び認証制度(以下、JCMVP と表記)の試行運用を開始している。

1.2 開発の目的

本プロジェクトでは、2007 年 4 月からの JCMVP の正式運用に向けて、試験で活用される CRYPTIPA の改修を実施することを目的とする。改修は、昨年度開発された CRYPTIPA への機能追加と修正にて実施する。

1.3 開発の方針

開発ツールとして、Microsoft Access 2003 を使用し、プログラム言語として、Visual Basic を使用した。

また、開発に当たり、既に特許となっている技術を利用せずに開発を行い、ISO 9001 の社内品質管理システムに基づき作業を行った。

2. 開発の内容

2.1 全体の構成

報告書作成支援ツールは、試験機関において使用され、スタンドアロンマシン上で動作する。

まず、認証機関で基準データをインポートし、試験パラメータを設定した後に試験機関へ配布される。

メンテナンスツールは、認証機関において使用され、報告書作成支援ツールの試験パラメータを設定する。

試験機関では、試験対象となる暗号モジュールやベンダに関する情報を登録し、試験結果を入力して試験報告書を作成する。また、同じ製品のバージョンの異なる製品や同じベンダの類似製品に対する試験において過去の試験結果を活用できるようにする。また、認証機関では試験機関から提出された試験結果を報告書データとして受け取り、検証支援ツールへ読み込んで試験結果を確認する。**図１**にツールの利用イメージを示す。

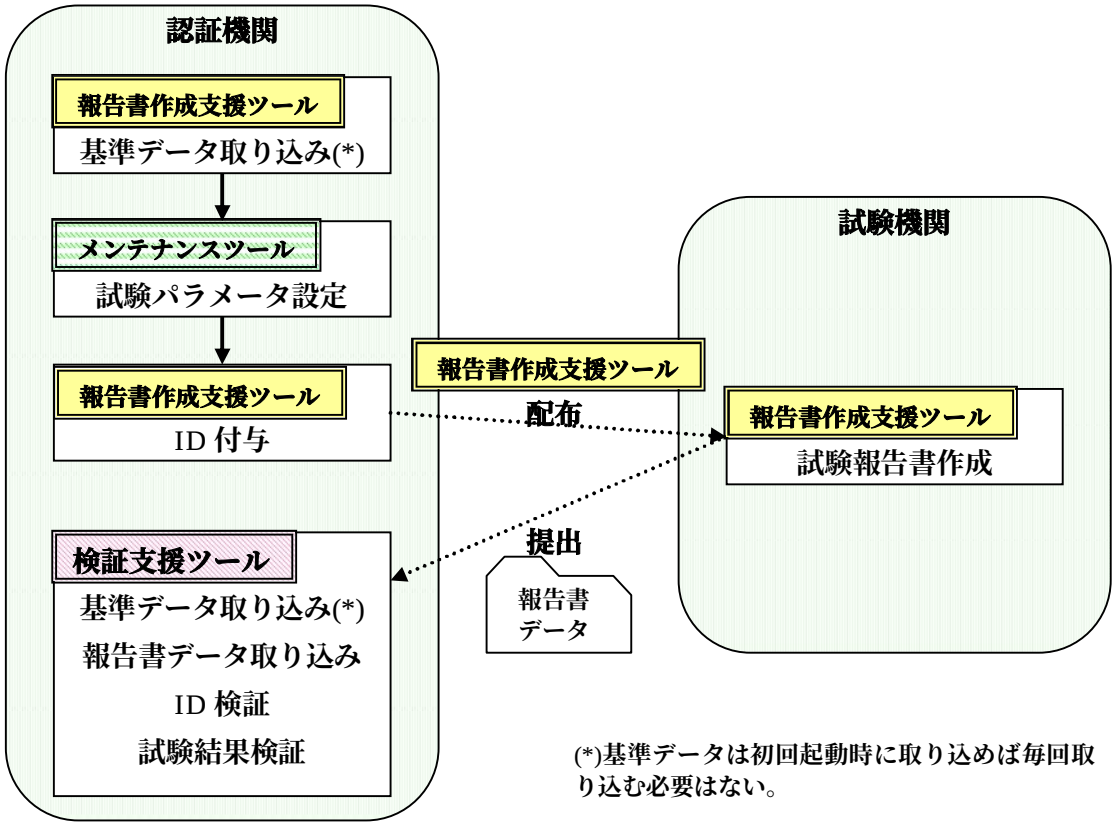

図 1　CRYPTIPA と検証支援ツールの利用イメージ

2.2 利用形態

各ツールの利用方法形態を整理したものを表１に示す。

表 1　各ツールの利用方法

利用場所	利用するツール	利用する機能
認証機関	報告書作成支援ツール （昨年度開発品に機能追加）	基準データの取り込み ID 付与
	メンテナンスツール （昨年度開発品）	試験パラメータの設定
	検証支援ツール （今年度新規開発）	ID の検証 試験結果の検証
試験機関	報告書作成支援ツール （昨年度開発品に機能追加）	基本情報入力、試験結果入力、 報告書作成、略号等の管理

2.3 用語の定義

データベース

2004 年度に開発した「暗号モジュール試験基準データベース」を表す。

基準情報

暗号モジュール試験基準の内容がデータベース内に格納された状態を表す。

基準データ

データベースに格納されている基準情報の特定のバージョンにおける基準情報をエクスポートした状態を表す。

物理形態

物理セキュリティに対する要求事項の規定における、暗号モジュールの物理的な形態に基づく分類で、シングルチップ暗号モジュール、マルチチップ組込型暗号モジュール、マルチチップスタンドアロン型暗号モジュールの 3 つが定義されている。

セキュリティレベル

暗号モジュールが提供するセキュリティを識別するための分類で、1～4 の 4 つのセキュリティレベルが定義され、数値が大きくなるほど要求事項が多くなり、セキュリティが強化される。

ＡＳ

評価基準で定められた暗号モジュールに対するセキュリティ要求事項を表す。

ＶＥ

AS に対応して試験基準で定められた暗号製品ベンダに課せられる要求事項を表す。

ＴＥ

AS に対応して試験基準で定められた試験機関に課せられる要求事項を表す。

ＩＧ

暗号モジュールの評価基準と評価認証制度の運用ガイダンスを表す。

アセスメント

試験に対する試験者の判断や見解を表す。

2.4 動作環境

開発するソフトウェアは、以下の環境で動作するものとする。

(a) ハードウェア

① CPU：クロック周波数 300 MHz 以上の Pentium 互換の CPU

② メモリ：128 MB 以上

③ ハードディスク：2.1 GB 以上

(b) ソフトウェア

① OS：Windows 2000 Professional SP4 又は Windows XP Professional SP2

② アプリケーション：Microsoft Access 2003

3. ソフトウェアの開発

本プロジェクトの開発作業項目として、次の 5 つが存在する。

A. データの入力
B. 試験報告書作成支援機能の強化
C. 完全性、不正使用の検出機能の追加
D. ユーザインタフェースの英語対応
E. マニュアルの作成

各作業項目の詳細を以下に述べる。

3.1 データ入力

データベースの機能を有効に活用できるよう、既に公開されている文書を利用して基準情報としてのデータを入力する。

① ISO/IEC 19790 への対応

ISO/IEC 19790 ベースの暗号モジュールセキュリティ試験要件を入力する。英文のみ。

② JIS 原案への対応

暗号モジュールセキュリティ試験要件の JIS 原案のデータを入力する。日本語のみ。

3.2 報告書作成支援機能の強化

(1) IPA が公開する「暗号モジュール試験及び認証制度の基本規程」及び JIS Q 17025 に則した暗号モジュール試験報告書を出力する。

・指定された規定や国内標準に基づき、CRYPTIPA の出力する項目や内容を修正する。
・試験機関で試験報告書を出力する場合、試験要件は出力せず、番号だけとする。
・暗号モジュール報告書を Adobe pdf 形式で出力できるように改良する。
・認証機関への提出用に報告書データのみをエクスポートできるようにする。

(2) 認証機関が試験報告書を検証する際に使用する「検証支援ツール」を作成する。

・検証支援ツールは、試験機関から提出された報告書データをインポートする。
・インポートした報告書データは、読み出し専用とする。
・検証支援ツールは、基準データもインポートし、画面で試験要件を参照しながら報告書の内容を検証できるようにする。
・認証機関で試験報告書を出力する場合、試験要件も出力できるようにする。

(3) 暗号モジュール認証書の雛形を出力する。

・CRYPTIPA の保持しているデータから暗号モジュール認証書に必要なデータを取り出し、エ

クスポートされる報告書データに含める。

・検証支援ツールは、報告書データをインポートし、指定されたフォーマットに基づき暗号モジュール認証書の雛形を出力する。

・後からの編集を容易にするため、Microsoft Word 形式で出力できるように改良する。

・認証書の基になるフォーマットを編集できるようにする。

3.3 CRYPTIPA の完全性、不正改造検出機能

(1) CRYPTIPA の完全性のチェック機能を実装する。

・プログラム部と基準データ部と報告書データ部のファイルを分離し、プログラム部と基準データ部を完全性チェックの対象とする。

・基準データ部は読み出し専用、報告書データ部は読み書き可能とする。

・ハッシュアルゴリズムとして SHA-1 を使用し、起動時にプログラム部と基準データ部のハッシュ値を算出する。

・あらかじめ格納されているハッシュ値と比較し、完全性をチェックする。

(2) CRYPTIPA の不正改造検出機能を実装する。

・プログラムの完全性チェックについては、(1)の機能を使用する。

・ハッシュ値が未格納の場合、算出結果を格納し、「格納済み」の状態に遷移する。

・ハッシュ値が「格納済み」の場合、格納されている値とプログラム起動時の算出値を比較し、完全性に問題があればプログラムを強制的に終了する。

・プログラム配布前に、あらかじめ「格納済み」の状態にすることにより、不正改造による使用の防止を実現する。

(3) CRYPTIPA の不正コピー検出機能を実装する。

・CRYPTIPA の配布時に、プログラム部のファイルに ID を付与できるようにする。

・CRYPTIPA に ID の確認用の画面を用意する。

・付与された ID も含めて完全性チェックを行い、ID の改変を検出し、改変による使用を防止する。

・試験報告書を出力する際、あらかじめ付与された ID を暗号化した形で報告書内に記載する。

・報告書データをエクスポートする際、あらかじめ付与された ID を暗号化した形で報告書データに含める。

・認証機関では、検証支援ツールによりあらかじめ付与した ID を暗号化した結果を取得できるようにする。

・試験報告書に記載されたり報告書データに含まれたりする暗号化された ID を検証することにより、不正コピーの検出を可能とする。

3.4 ユーザインタフェース

日本語及び英語のグラフィカルユーザインタフェースを提供する。

・日本語版と英語版の 2 種類の CRYPTIPA を用意する。

・機能は言語によらず同じ仕様とする。

3.5 マニュアルの作成

JCMVP において CRYPTIPA を使用するために必要なマニュアルを作成する。

・動作画面を取り込み、操作手順がわかりやすいマニュアルとする。

・英語のグラフィカルユーザインタフェースが提供されるため、英文のマニュアルも作成する。

4. 報告書作成支援ツール

4.1 メニュー構成

メインメニュー

試験機関情報	試験機関情報を登録、変更する。
ベンダ情報	ベンダ情報を登録、変更する。
モジュール情報	モジュール情報を登録、変更する。
├ レベル指定	セキュリティレベルを登録、変更する。
└ 再試験実施	試験状態をすべて未実施に設定する。
試験結果入力	試験項目を一覧表示する。
├ 指定された節を表示	指定した節の試験項目を表示する。
├ すべての節を表示	すべての節の試験項目を表示する。
├ モジュール情報	「モジュール情報」画面を表示する。
├ 文献情報	「文献情報」画面を表示する。
├ 略号定義	「略号定義」画面を表示する。
└ 報告書作成	「報告書作成」画面を表示する。
報告書作成	試験結果の表示と報告書の出力を行う。
├ プレビュー	試験結果の画面表示を行う。
├ 印刷	報告書の印刷出力を行う。
└ 出力	認証書発行または請求先情報を CSV で出力する。
ファイル、データ管理	
├ 新規作成	現在の報告書データを削除し、新規に作成する。
├ 名前を付けて保存	現在の報告書データをファイルに保存する。
├ 開く	以前の報告書データを読み込む。
├ エクスポート	Web 公開情報をエクスポートする。
├ バージョン情報	バージョン情報と ID を確認する。
└ データ削除	アセスメント、全試験結果、注釈、略語定義、非公開情報、文献情報、試験状態、モジュール情報を削除する。
終了	作業を終了する。

4.2 機能概要

① メインメニュー
メニューの選択、ツールの終了を行う。

② 試験機関情報
試験機関に関する情報として、名称、住所、試験担当者等を登録する。

③ ベンダ情報
ベンダに関する情報として、名称、住所、連絡先等を登録する。

④ モジュール情報
暗号モジュールに関する情報として、識別情報、名称、セキュリティレベル等を登録する。

⑤ 試験結果一覧
オプションの指定、入力対象となる節の選択、試験状態の表示を行う。

⑥ 試験結果入力
要求事項の表示、文章の入力、状態の管理を行う。

⑦ 報告書作成
試験結果の画面表示と報告書としての印刷出力を行う。

⑧ 試験結果入力
要求事項の表示、文章の入力、状態の管理を行う。

⑨ 略号定義
略号の定義を管理する。

⑩ 文献情報
報告書において参照される文献に関する情報を管理する。

⑪ ファイル管理
ファイルによるエクスポートとインポートを行う。

⑫ データ管理
試験結果から指定した項目に対応するデータを削除する。

4.3 機能仕様

試験機関における暗号モジュールの試験に対する試験報告書の作成を支援する。

・ツールの名称は「CRYPTIPA」とする。
・Microsoft Access を利用したアプリケーションとし、スタンドアロンでの利用を想定する。
・ツールは Access 形式のファイルとし、GUI の提供と試験結果のデータ保持を行う。
・試験済み製品の試験結果をエクスポートし、別製品の試験においてインポートして再利用可能とする。
・次のようなメニューを用意し、メニューごとに入出力のための操作画面を用意する。

①【メインメニュー】
メニューの選択、ツールの終了

②【試験機関情報】
試験機関に関する情報として、名称、住所、試験担当者等を登録する。

③【ベンダ情報】
ベンダに関する情報として、名称、住所、連絡先等を登録する。

④【モジュール情報】
暗号モジュールに関する情報として、識別情報、名称、セキュリティレベル等を登録する。
・節ごとにセキュリティレベルあるいは適用除外を指定可能とする。
・適用除外が指定可能な節については、メンテナンスツール(後述)で設定可能とする。
・物理形態(シングルチップ等)を指定する。
・モジュール区分(ハードウェア／ソフトウェア／ファームウェア)を指定する。

⑤【試験結果一覧】
オプションの指定、入力対象となる節の選択、試験状態の表示を行う。
・入力画面で表示する要求事項(VE／TE／両方)のオプションを選択する。
・入力対象となる試験項目(すべて／未完／不合格)のオプションを選択する。
・各節の試験状態(試験中／合格／不合格)を一覧表示する。

⑥【入力画面】
要求事項の表示、文章の入力、状態の管理を行う。
・要求事項を表示しながら、文章の入力や状態の変更を行えるようにする。
・節ごとに指定されたセキュリティレベルに該当する事項だけが入力対象となる。
・要求事項は AS と VE 及び／又は TE(前述のオプションに依存)が順番に表示される。
・アセスメント、注釈、非公開情報の文章を入力できる。

・試験状態として、未実施、合格、不合格、適用除外から 1 つを選択でき、それとは別に再試験済みをチェックできる。
・運用ガイダンスの G.8 で規定される再認証へ対応する。
・再認証における必須の要求事項については、メンテナンスツール(後述)で設定可能とする。
・必須の要求事項については、再試験開始時にすべて「未実施」状態に戻される。
・AS、VE、TE、IG、所見、注釈、非公開情報の 7 種を対象としてテキスト検索する。
・所見、注釈、非公開情報の 3 種については一括置換と逐次置換を可能とする。

⑦【報告書作成】
試験結果の画面表示と報告書としての印刷出力を行う。
・画面表示／印刷出力を選択可能とする。
・主要項目試験報告書として、主要項目に対する試験結果だけを表示する。
・主要項目の対象となる要求事項については、メンテナンスツール(後述)で設定可能とする。

試験結果に対する認証書及び請求書を発行する。
・認証書発行に必要となるモジュール情報とベンダ情報を CSV 形式でファイル出力する。
・請求書送付に必要となるベンダの請求先情報を CSV 形式でファイル出力する。

⑧【略号定義】
報告書で使用する略号の定義を管理する。
・各操作画面から登録されている定義を参照、検索、追加できるようにする。

⑨【文献情報】
試験で参照している文献に関する情報を管理する。
・各操作画面から登録されている情報を参照、検索、追加できるようにする。

⑩【ファイル管理】
ファイルによるエクスポートとインポートを行う。
・現在の支援ツールに格納されている試験結果をエクスポートする。
・認証製品の Web 公開用情報をエクスポートする。
・過去の試験結果を現在の支援ツールにインポートする。
・基準データとして配布されるファイルから基準情報をインポートする。
・バージョン情報と付与された ID を表示する。

⑪【データ管理】
試験結果から指定した項目に対応するデータを削除する。
・試験結果をエクスポートする前や過去の試験結果をインポートした際に使用される。

5. まとめ

昨年度開発された暗号モジュール試験報告書作成支援ツールの改修と検証支援ツールの作成を行った。また、最新のセキュリティ試験要件の内容をツールで活用できるようにデータ入力した。

暗号モジュール試験報告書作成支援ツールで改良された点は次の通りである。

・報告書の印刷や認証機関へ提出するための機能を強化した。
・ツールの完全性をチェックすることにより、不正な改変の検出機能を追加した。
・ツール毎に ID を付与することにより、不正使用の検出機能を追加した。
・英語版のユーザインタフェースとマニュアルも用意した。

検証支援ツールで提供される機能は次の通りである。

・報告書作成支援ツールに付与した ID を検証することにより、使用されたツールの正当性を確認できる。
・提出された報告書データを読み込み、試験結果を検証できる。
・試験要件を参照しながら作業できる。
・提出された報告書データに含まれる情報を基にして認証書を出力できる。

本改修により暗号モジュール試験及び認証制度の正式運用において、次のような効果が期待される。

・試験及び認証における試験結果の統一的な管理が図れる。
・試験機関及び認証機関における作業の効率化が期待される。

6. 参考文献

[1] 情報処理推進機構, 2004 情財第 651 号“暗号モジュール試験基準データベースの開発”, 2005
http://www.ipa.go.jp/security/fy16/development/crypt_db/index.html

[2] 情報処理推進機構, 2005 情財第 1099 号“暗号モジュール報告書作成支援ツールの開発”, 2006
http://www.ipa.go.jp/security/fy17/development/cryptipa/index.html