JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

活動報告

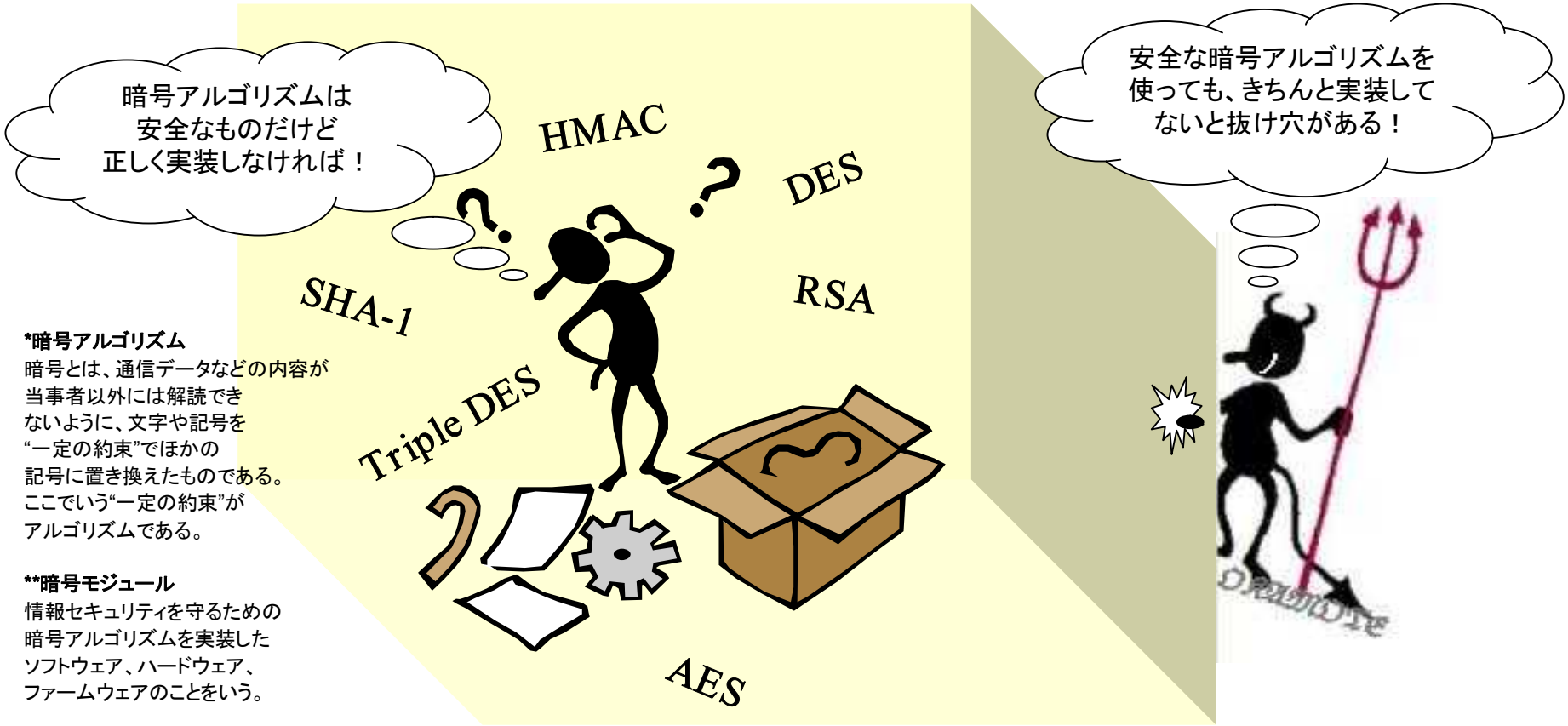
小川　博久

暗号モジュール評価基準WG

2005 年 6 月 13日

暗号モジュール評価の重要性

•情報の信頼性を確保するためには、暗号アルゴリズム*だけでなく、暗号モジュール**の安全性の確保が急務である



***暗号アルゴリズム**
暗号とは、通信データなどの内容が当事者以外には解読できないように、文字や記号を“一定の約束”でほかの記号に置き換えたものである。ここでいう“一定の約束”がアルゴリズムである。

****暗号モジュール**
情報セキュリティを守るための暗号アルゴリズムを実装したソフトウェア、ハードウェア、ファームウェアのことをいう。

暗号アルゴリズムの実装レベルでの評価の必要性が高まっている

暗号モジュール評価基準WG

暗号モジュールを第三者が評価する要件とスキームがあります。

- 要件：FIPS140-2
- スキーム：CMVP

利用者や、設計開発者など、暗号製品に関わる担当者の対応を考えると、これらを知る必要があるのではないか？

『暗号モジュール評価基準WG』では、これらの暗号の実装に伴う評価や要件について議論しています。

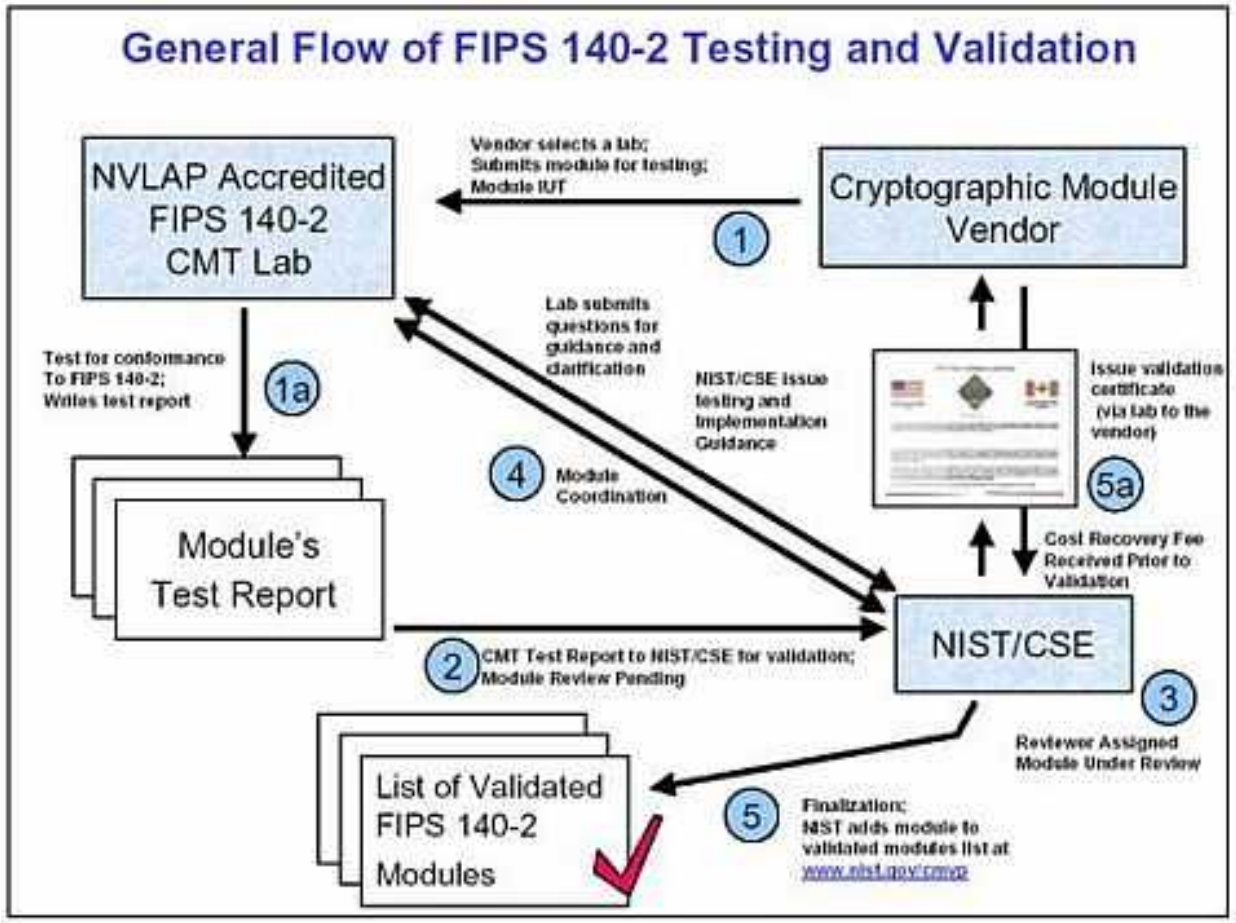
FIPS：Federal Information Processing Standard
FIPS 140-2：暗号モジュールのセキュリティ要件に関する規格
CMVP：Cryptographic Module Validation Program
CMT Lab.：Cryptographic Module Testing Laboratory
NIST：National Institute of Standards and Technology

FIPS140-2 の評価分野

【セキュリティ要件の評価分野 】		
1	**暗号モジュール仕様**	暗号モジュールの仕様、「FIPS 140-2」の適用範囲を規定
2	**暗号モジュールのポート･インタフェース**	情報の入出力に関する規定
3	**役割、サービス、及び認証**	ユーザーの役割や役割ごとに提供されるサービス、ユーザーの認証方法を規定
4	**有限状態モデル**	状態遷移の記載を規定
5	**物理セキュリティ**	表面処理やカバー等といった物理的しくみによるセキュリティ要件を規定
6	**動作環境**	暗号モジュールが動作する環境に関する規定
7	**暗号鍵管理**	鍵生成、鍵の入出力等を規定
8	**電磁妨害／電磁両立性(EMI/EMC)**	電磁波に対する要件を規定
9	**自己テスト**	暗号モジュールが正しく動作できることを確認するためのテストに関する規定
10	**設計保証**	ガイドライン等に関する規定
11	**その他の攻撃の対処**	「FIPS 140-2」では規定されていないその他の攻撃の対処方法の記載

各々の分野ごとに，4段階のセキュリティレベルを規定している.（ Level 1 ～ Level 4 ）
レベルの数値が高くなるほど要求されるセキュリティ要件は厳しくなる.

FIPS 140-2 テストと認定の概要



（NISTのWebサイトからの引用）
http://csrc.nist.gov/cryptval/140-1/140-2flow.pdf

WGの活動報告

『暗号モジュール評価基準カンファレンス』

■ 開会挨拶「情報セキュリティ大学院大学の紹介」
情報セキュリティ大学院大学学長 辻井 重男

■ 特別講演「FIPS 140-2 and the CMVP」
InfoGard Laboratories, Security Engineer, Travis Spann

■ 特別講演「我が国における暗号モジュール評価について」
山岸 篤弘 氏（独立行政法人 情報処理振興事業協会 セキュリティセンター）

■ ベンダーパネルディスカッション
- FIPS 140-2認定取得について
WGメンバー 中川路 哲男 氏（三菱電機）
- FIPS 140-2認定作業について
WGメンバー 萩原 雄一 氏（シーフォーテクノロジー）

■ 公開WG（＋WGの紹介）

日時：2004年12月14日（火）
場所：情報セキュリティ大学院大学
主催：NPO 日本ネットワークセキュリティ協会
情報セキュリティ大学院大学
中央大学21世紀COEプログラム
後援：InfoGard Laboratories, Inc.

ベンダーは・・・

- どの要件を対応したらいいのだろうか？
  - FIPS 140-2
  - FIPS 140-3
  - ISO IEC 19790
- スキームを整備している国が少ない。

ユーザーは・・・

- ベンダーに聞いてみることからはじめる
  - 暗号アルゴリズムは何を使っているのか？
  - その暗号アルゴリズムが確実に実装されていると、誰か（第三者）に評価されたのか？

暗号モジュール実装の確実性

電子政府系 暗号調達では、調達した暗号の実装が正しいことを
厳密に確認する技術方法として下記が例示されています。

i. テストベクトルの利用

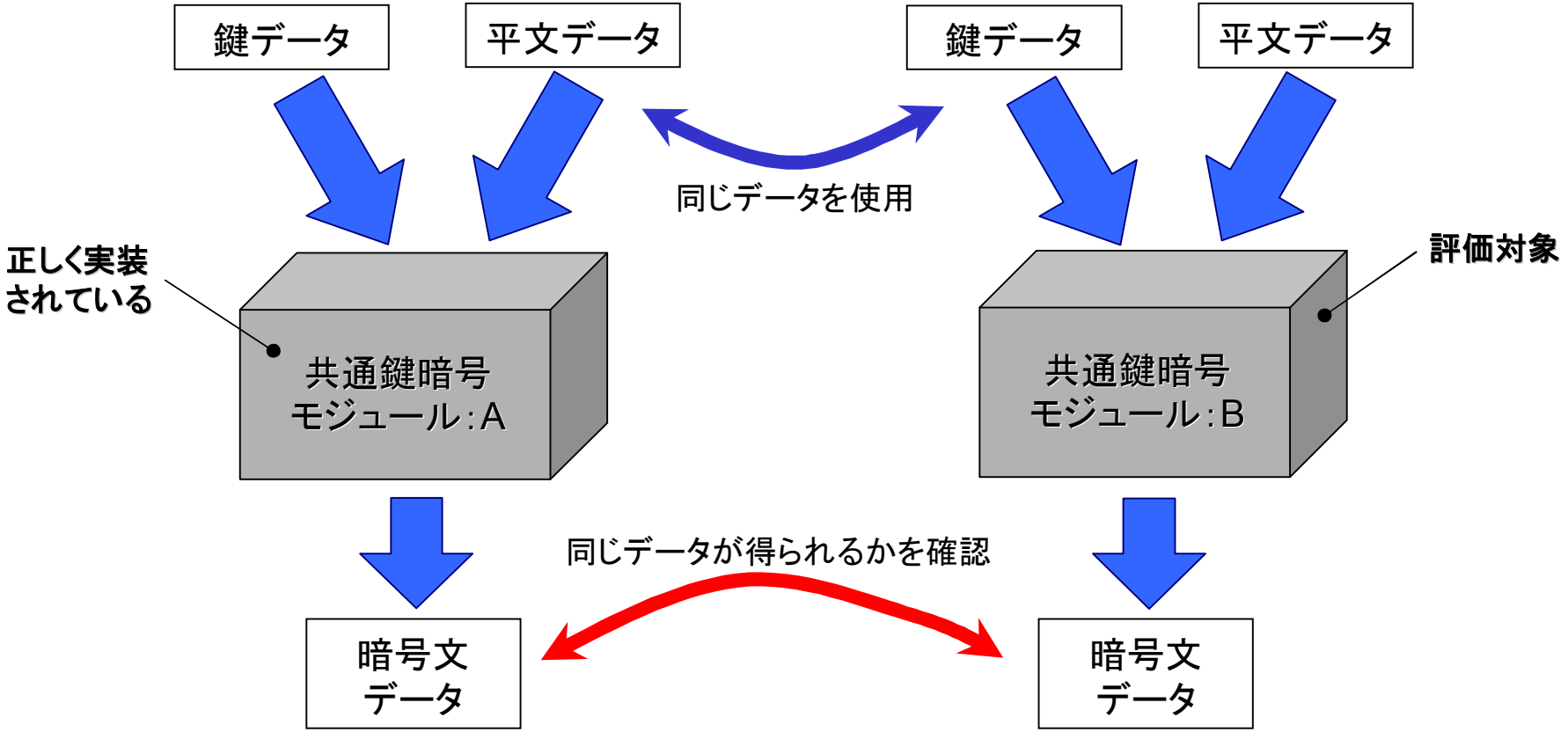
ii. 別の暗号製品・システムとの対向通信

iii. 第三者機関による評価

参照:「暗号調達のためのガイドブック」
暗号技術検討会，暗号調達ガイドブック作成ワーキンググループ，平成15年3月
http://www.meti.go.jp/policy/netsecurity/downloadfiles/Guidebook.pdf

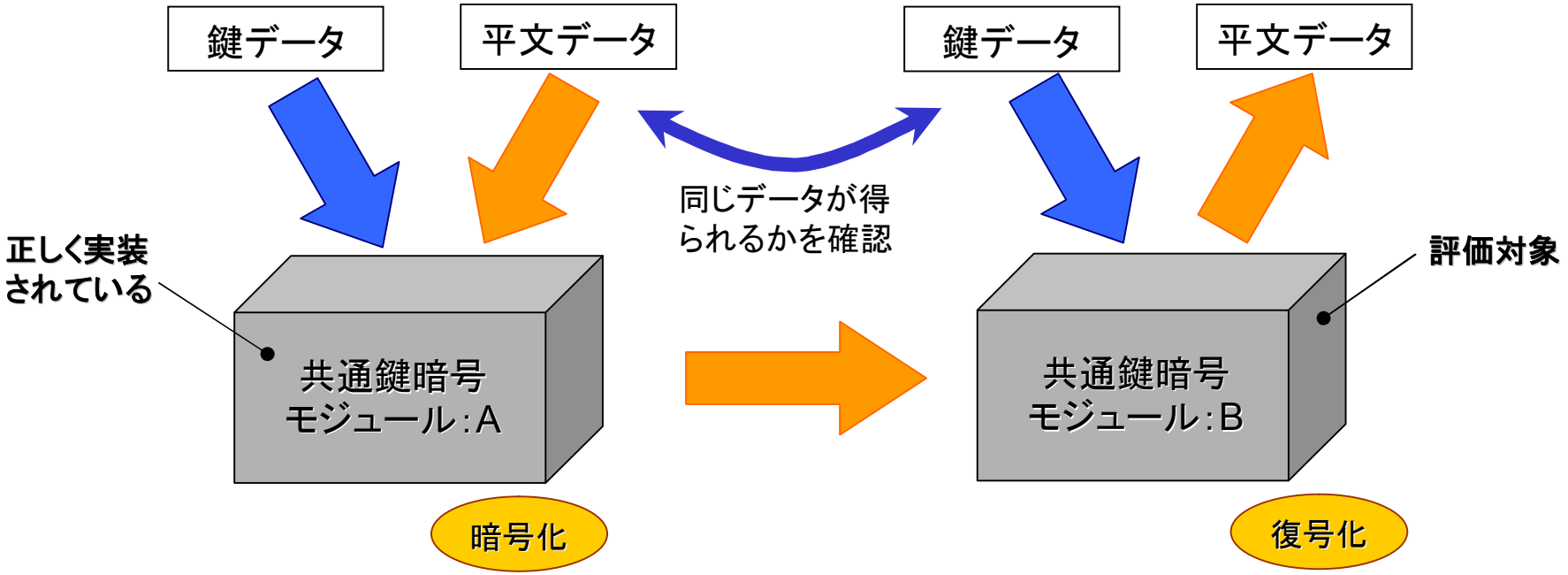
i. テストベクトルを利用したテスト

正しく実装された暗号モジュールと，評価対象の暗号モジュールから得られたデータを比較し，実装の正しさを確認する方法



ii. 別の暗号製品・システムとの対向通信

正しく実装された暗号製品と、評価対象の暗号製品とを通信させ、評価対象の暗号モジュールの実装が正しいとする方法



iii. 第三者機関による評価

第三者機関に各種のテストを行わせ、暗号の実装が正しいことを確認させる方法である。
米国ではNISTがFIPS 140-2 に基づいて、暗号製品の安全性の認定を行っているが、国内においては公的に承認されている評価機関はまだ存在しないので、
暗号の専門家に評価を依頼する等の方策が必要である。

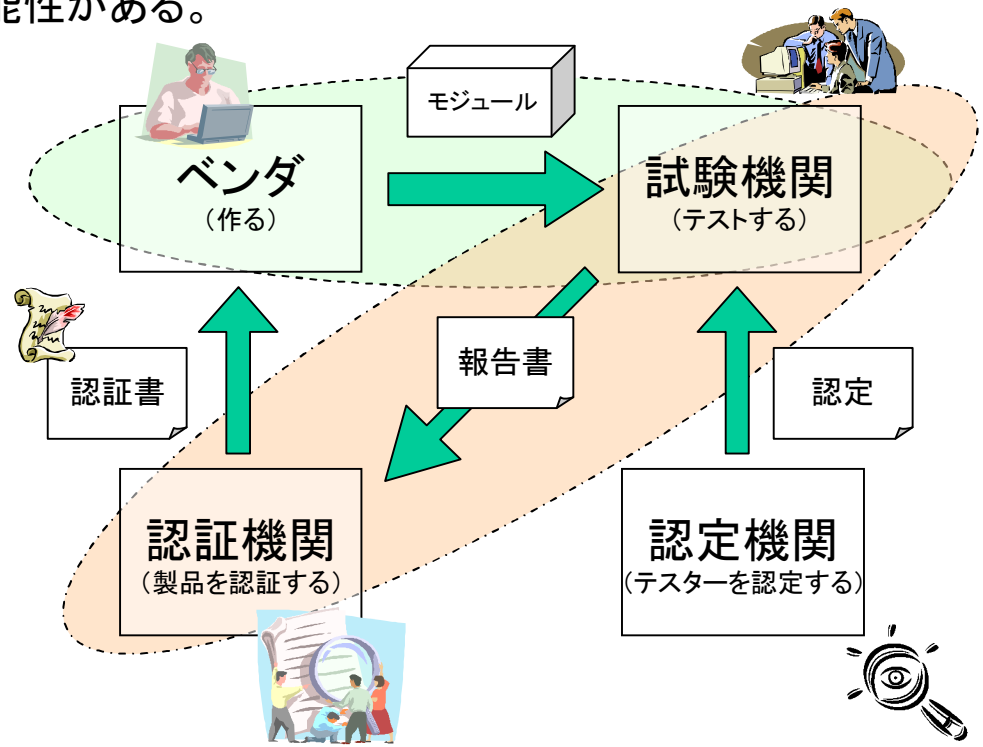
わが国における検討(移行措置案)

(1)自己評価方式

- ベンダにとっては自主的な品質管理制度との親和性が高く、導入しやすい。
- ベンダ間で評価レベルに差が生じる可能性がある。
- 評価結果の中立性が確保できない。

(2)認証機関併設方式

- 中立な評価が期待できる。
- 競争原理が働かないため、評価コスト高止まりする可能性がある。



山岸 , 網島 , 近藤 , 大熊 , 西原(独立行政法人情報処理推進機構セキュリティセンター暗号グループ), "わが国における暗号モジュール評価制度について" , SCIS2005 , 2B4-1,p829-834, Jan,2005.

移行措置案に対して

- 自己評価方式は、厳密な意味で第三者評価になるのだろうか？
- 認証取得を促す動機付けが欲しい。
- 試験人員、認証人員が極端に不足していることが予想されるので、大学の研究機関などでの人材育成も重要。
- 移行措置案1，2に拘らず、現状運用されているFIPS140-2と同等レベルの報告書であれば（海外の試験機関の報告書も含め）、認証機関はすべて受付けていいのではないか？
  - 中立的な評価を期待できる。
  - 適正な金額で認定を受けることが期待できる。
  - 国際的な親和性，協調性を期待できる。

参照文献

- NITS Cryptographic Module Validation Program
  http://csrc.nist.gov/cryptval/
  http://csrc.nist.gov/cryptval/140-1/140-2flow.pdf

- 2003年度暗号モジュール委員会活動について
  http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030801_modplan.html

- CRYPTREC Report 2003
  http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20040310_report01.html

- CRYPTREC Report 2004
  http://www.ipa.go.jp/security/enc/CRYPTREC/fy16/cryptrec20050421_report01.html

- 「暗号調達のためのガイドブック」
  http://www.meti.go.jp/policy/netsecurity/downloadfiles/Guidebook.pdf

- 『暗号モジュール評価の基礎知識』（アットマーク・アイティ社　連載記事）
  - 第1回　暗号モジュールの安全性について考える
    http://www.atmarkit.co.jp/fsecurity/rensai/fips01/fips01.html
  - 第2回　各国で採用されるFIPS 140-2の重要性
    http://www.atmarkit.co.jp/fsecurity/rensai/fips02/fips01.html
  - 最終回　FIPS 140-2認定がもたらすユーザーへの恩恵
    http://www.atmarkit.co.jp/fsecurity/rensai/fips03/fips01.html