

電子政府情報セキュリティ技術開発事業
暗号モジュール評価に関する国内ニーズ調査
報告書



平成 15 年 2 月 28 日

情報処理振興事業協会
セキュリティセンター

目次

1. 調査目的・調査方法.....	1
1.1 調査の背景・目的.....	1
1.2 調査方法.....	3
2. 暗号モジュール評価の現状整理.....	6
2.1 暗号関連製品市場の現状.....	6
2.2 第三者評価の実施および認証取得に関する現状.....	16
2.3 自己評価の実施に関する実態.....	20
3. 暗号モジュール製品の市場動向.....	23
3.1 暗号モジュール製品を含む暗号関連製品市場の動向.....	23
3.2 今後5年間において国内暗号市場に影響を与える技術的・制度的要因.....	25
3.3 今後5年間を見据えた国内市場の暗号関連製品数の予測.....	27
4. 暗号モジュール評価・認証制度のニーズ分析.....	32
4.1 評価・認証制度に関する暗号関連製品供給サイドの関心、ニーズ.....	32
4.2 評価・認証制度に関する暗号関連製品需要サイドの関心、ニーズ.....	37
4.3 評価・認証制度に関する制度運営サイドの見解と意向.....	40
4.4 評価・認証制度の需要規模予測.....	46
5. 提言.....	55
5.1 提言の概要.....	55
5.2 ニーズの顕在化および掘り起こしに必要と考えられる施策の提言.....	56
5.3 国内暗号モジュール評価・認証制度の姿.....	57

1. 調査目的・調査方法

1.1 調査の背景・目的

(1) 背景

情報システムやそれを構成する機器・ソフトウェアの国際的なセキュリティ評価基準としては ISO/IEC 15408 があるが、電子政府システムのセキュリティを十分に確保するためには、加えて、暗号アルゴリズムの実装レベルでのセキュリティ評価基準が必要である。

海外では既に米国 NIST とカナダ CSE が共同で暗号モジュール評価・認証制度 (CMVP) を運用しており、暗号アルゴリズムの実装レベルでのセキュリティ評価基準が制定されている。また、2003 年 2 月には、ISO/IEC JCT1/SC27 において暗号モジュールのセキュリティ要件の国際標準化に向けた検討の提案が受理され、委員会に諮るワーキングドラフト作成の段階 (規格化に至る 6 段階の 2 段階目) に移行した。

わが国においても、こうした国際標準化の流れを意識しながら、国内における暗号モジュール評価・認証制度の整備に向けた検討を行う必要がある。

(2) 目的

海外では既に米国 NIST とカナダ CSE が共同で暗号モジュール評価・認証制度 (CMVP) を運用しており、暗号アルゴリズムの実装レベルでのセキュリティ評価基準が制定されている。また、ISO/IEC JCT1/SC27 では、暗号モジュールのセキュリティ要件を国際標準化する取り組みが進行している。

わが国においても、国際標準化の流れを意識しながら、国内における暗号モジュール評価・認証制度の整備に向けた検討を行う必要がある。

情報処理振興事業協会において暗号モジュール評価・認証制度の整備を検討するにあたり、暗号モジュールベンダーを対象とした市場規模と評価機関設置に関する費用対効果を十分に把握するため、暗号モジュール評価に関する国内ニーズ調査を実施した。

(3) 本調査における暗号モジュールの定義

本調査では、他のハードウェアやシステムへの組み込みを想定した暗号機能を実現するための暗号ライブラリ、ハードウェアを「暗号モジュール」と定義し調査を実施した。なお、ここでいう暗号機能とは、暗号化/復号、鍵の生成、鍵の保管、乱数生成、ハッシング、デジタル署名、電子証明書等を指す。

この定義の下での暗号モジュールの例として、

- 暗号化 / 復号の機能を持つ LSI (スマートカードを含む)
- 暗号機能を持つ PCI ボード

- 開発者向け SDK**等の暗号処理ソフトの開発ツールキット
- 電子署名機能を付加するためのプラグインソフト(文書作成ソフト用)

などを想定している。

また、本調査では、暗号機能を備えたソフトウェア、ハードウェアあるいはそれらを組み合わせたシステムを包括して「暗号関連製品」と呼んでいる。この定義における「暗号関連製品」には、暗号モジュールが含まれる。(図 1.1)

暗号関連製品の例としては、前述の暗号モジュールに該当するものの他、

- データ暗号化や DHCP/DNS の機能が組みこまれたファイアウォール製品
- ハードディスクのデータ暗号機能等をもつ情報漏洩対策ソフトウェア製品
- 公開鍵基盤(PKI)を用いた決済機能をもつ電子決済システム
- 暗号化通信機能を含むサーバー向けセキュリティソリューション
- 鍵発行・管理機能を含む PKI ソリューション

などを想定している。

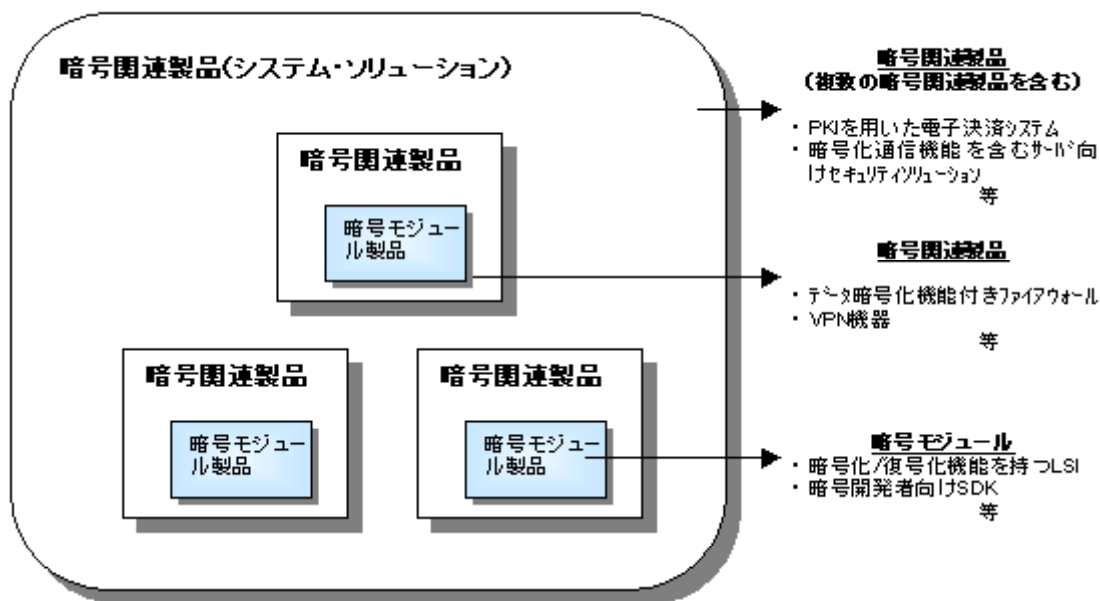


図 1.1 暗号モジュール製品の定義

** Software Developer Kit(ソフトウェア開発キット): アプリケーションの実装、コンパイル、テスト等、ソフトウェア開発に必要な統合環境を提供するソフトウェアのこと。テスト用のアプリケーション、例となるソフトウェアが含まれる場合もある

1.2 調査方法

(1) 調査の全体像

本調査では、暗号関連製品販売窓口に対するアンケート調査と4つの対象に対するインタビュー調査を実施した。

調査の流れとしては、まず、アンケート調査を通じて「暗号モジュール製品の自己評価の実態」(図1.2中の[B])および「暗号モジュール評価・認証制度の潜在的対象製品の動向」(図1.2中の[C])を整理した。

アンケート調査を通じて整理した事項のうち、「暗号モジュール評価認証制度の潜在的対象製品の動向」については、暗号モジュール製品窓口とCRYPTREC 評価委員会メンバーに対するインタビュー調査によって事実の掘り下げを行った。また、インタビュー調査によって、「暗号モジュール製品制度の評価・認証制度に関する意向」(図1.2中の[D])を整理した。

なお、本調査は、暗号モジュール製品を含む暗号関連製品のリストの作成と並行して実施した。図1.2に示すとおり、アンケート調査については、「国内で入手可能な暗号関連製品リスト」の作成のための情報収集を兼ねている。

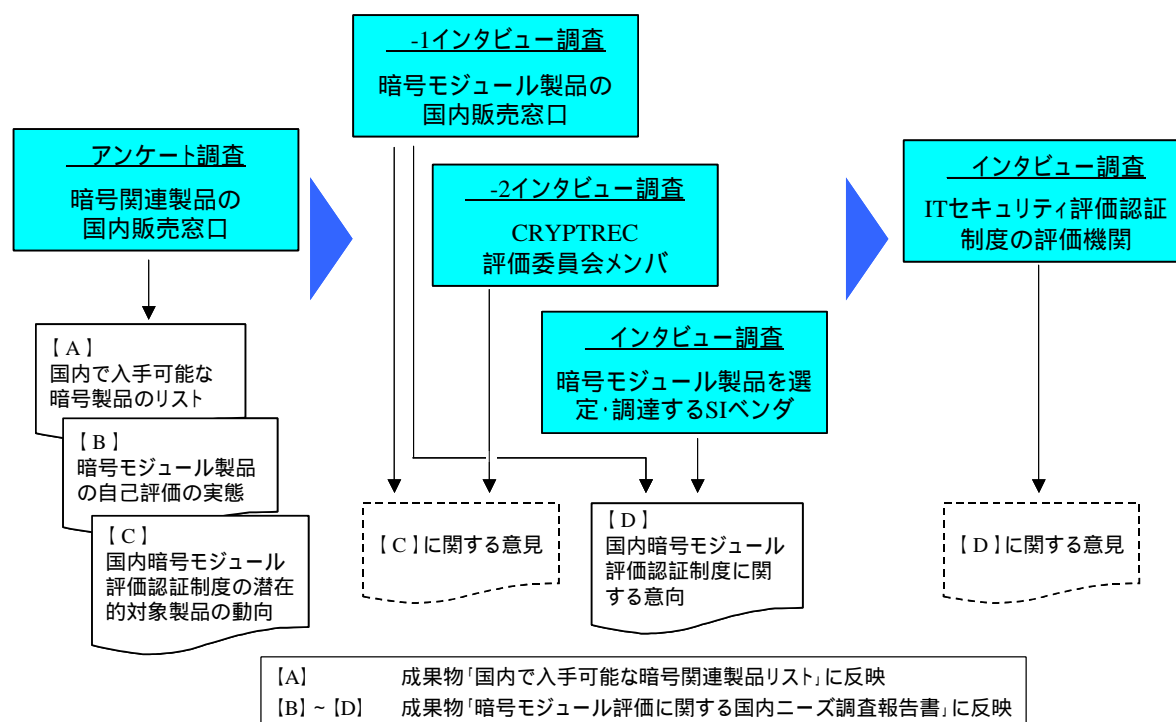


図 1.2 作業の全体像

(2) アンケート調査

国内で入手可能な暗号関連製品の情報の入手、および国内販売窓口の暗号関連製品の取扱状況と今後の意向の確認を目的として、暗号関連製品の国内販売窓口向けにアンケート調査を実施した。このアンケート調査の対象・調査方法は以下のとおりである。

【調査対象】

- 以下のソースをもとにリストアップした暗号モジュール製品およびそれ以外の暗号関連製品の販売窓口 180 社
 - 情報処理振興事業協会 Web サイトに掲載されている「国内で入手可能な暗号関連製品リスト」(平成 11 年 10 月作成)
 - IT 専門誌(「日経コミュニケーション」、「日経ネットワーク」、「ネットワークマガジン」、「セキュリティマガジン」、「日経インターネットソリューション」)
 - IT 関連情報 Web サイト(「日経IT Pro」、「ZD Net エンタープライズ」)
 - 各種検索エンジンを使った Web サイトの検索結果

【調査方法】

- リストアップした販売窓口に対して以下の調査票を郵送にて送付、郵送にて回収(なお、送付に先立ち、販売窓口に対して電話にて調査協力の承諾を得た)
 - 「暗号モジュール製品についての調査票」 ~ 該当製品ごとに 1 部送付
 - 「暗号モジュール製品以外の暗号関連製品についての調査票」 ~ 該当製品ごとに 1 部送付
 - 「暗号モジュール製品の販売窓口としての調査票」 ~ 該当製品を取り扱う販売窓口に 1 部送付
 - 「暗号モジュール製品以外の暗号関連製品の販売窓口としての調査票」 ~ 該当製品を取り扱う販売窓口に 1 部送付

なお、次の点を次章以降および付録 1 のアンケート調査結果を見る上で注意されたい。このアンケート調査の送付に当たってリストアップした販売窓口は、国内で暗号関連製品を取り扱っている販売窓口の大半をカバーしたと考えているが、必ずしもすべての販売窓口を網羅しているわけではない。また、製品についても、国内で入手可能な製品の大半をカバーしたと考えているが、必ずしもすべての製品をカバーしているわけではない。

また、本報告書の中でのアンケート調査結果の図表では、有効回答のみを集計したものである。そのため無効回答があった場合、図表中の回答数の合計(N 数)と対象回答者数は一致しない。

(3) インタビュー調査

暗号モジュール評価・認証制度に対する認識・意向および暗号関連製品の市場動向の認識など、アンケート調査では明らかにしきれない点を掘り下げることが目的として、暗号関連製品の販売窓口に対してインタビュー調査を実施した。なお、インタビュー先の選定において、暗号関連製品販売窓口を以下の 3 つのカテゴリに分け、それぞれのカテゴリごとに複数件のインタビューを実施するよう配慮した。

【暗号関連製品販売窓口の調査対象】

- 暗号モジュールの自己評価を実施している暗号モジュール製品販売窓口 2 件実施

- 暗号モジュールの自己評価を実施していない暗号モジュール製品販売窓口 2 件実施
- 暗号モジュール製品以外の暗号関連製品販売窓口である SI 事業者 3 件実施

暗号関連製品販売窓口に対する調査の結果から得られた今後の市場動向に関する情報の確認および今後の市場動向に影響しうる要因についての示唆を得るため、CRYPTREC 評価委員会のメンバーに対するインタビュー調査を行った。

さらに、暗号モジュール評価・認証制度の下で製品の評価を実施する評価機関から見た制度に関する意向を想定するために、既存の類縁制度の下で製品の評価を行っている機関にインタビュー調査を行った。

【暗号関連製品販売窓口以外の調査対象】

- CRYPTREC 評価委員会メンバー 1 件実施
- IT セキュリティ製品評価・認証制度の評価機関 2 件実施
(認定評価機関、ST の評価を実施できる評価者がいる機関の双方を含む)

2. 暗号モジュール評価の現状整理

2.1 暗号関連製品市場の現状

本節では、国内の暗号関連製品の販売窓口 127 社から回収した暗号モジュール 61 製品、暗号モジュール以外の暗号関連製品 188 製品についてのアンケート調査の結果をもとに、国内の暗号関連製品市場の現状を整理する。

(1) 形態別・用途別の製品数

アンケート調査では、61 種類の暗号モジュール製品について回答があった。形態に関する質問について回答のあった 59 製品では、ライブラリの形態をもつ暗号モジュールが 33 製品と最も多い。それ以外の形態については、ハードウェアであるものが 15 製品、ライブラリに該当しないソフトウェアが 11 製品となっている。なお、ファームウェアが他に比べて極端に少ないが、これは製品として外販市場には出てきにくい製品であるため、本調査の対象に入るものがあまりなかったためと考えられる。

(図 2.1)

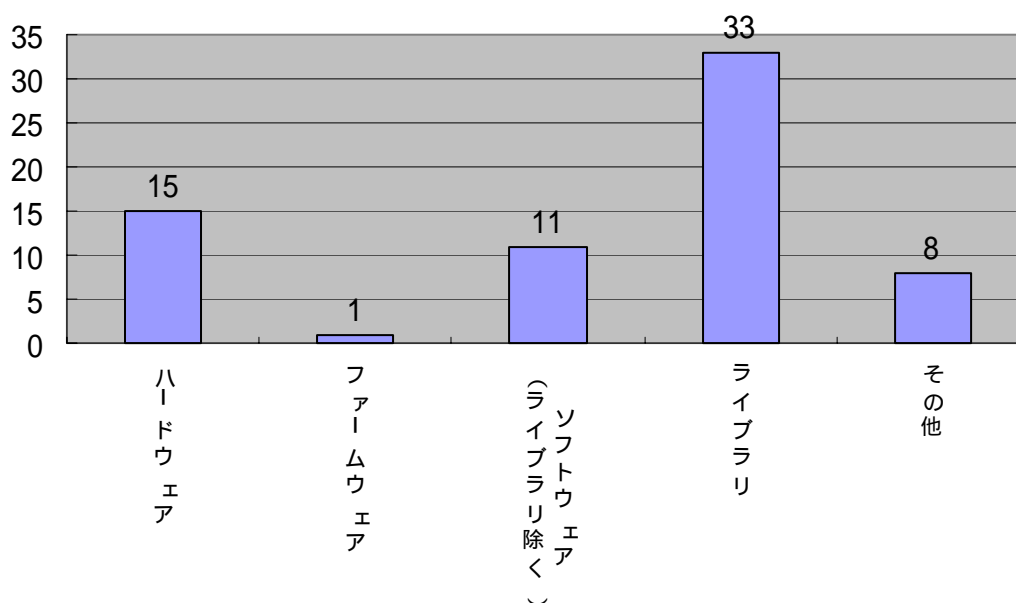


図 2.1 形態別製品数[暗号モジュール製品] (複数選択、単位:製品、N=59)

回答があったモジュール製品の用途を見ると、大分類単位では「暗号化製品」と「認証関連製品」が多い。「暗号関連製品」の中では、特に「データ/ファイル暗号化、暗号化装置等」が 30 製品と小分類では最も多い。また、「認証関連製品」の中では、「PKI 関連製品」が多い。

一方、「VPN 関連製品」、「電子商取引関連製品」は他に比べて製品数が少ない。こうした少ない製品は、製品のカテゴリとして未確立で参入が少ないあるいは既に特定の製品がデファクトスタンダード化している状態にあると考えられる。(図 2.2)

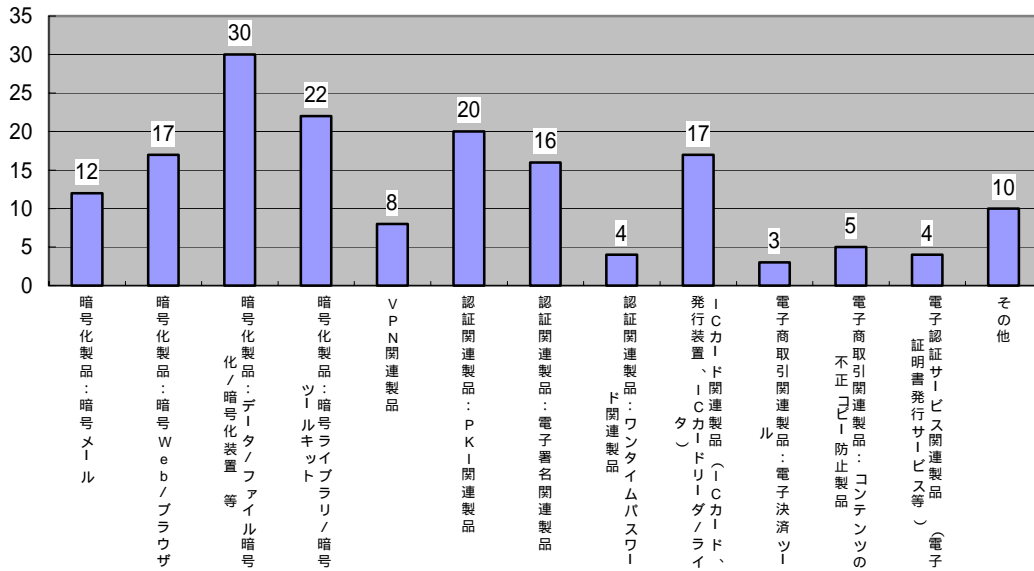


図 2.2 用途別製品数[暗号モジュール製品]（複数選択、単位：製品、N=58）

暗号モジュール製品以外の暗号関連製品については、188 製品について回答があった。これらの製品の形態は、ソフトウェアであるものが 90 製品、ハードウェアであるものが 72 製品である。なお、23 製品が該当している「その他」のうち、18 製品は ASP サービスである。

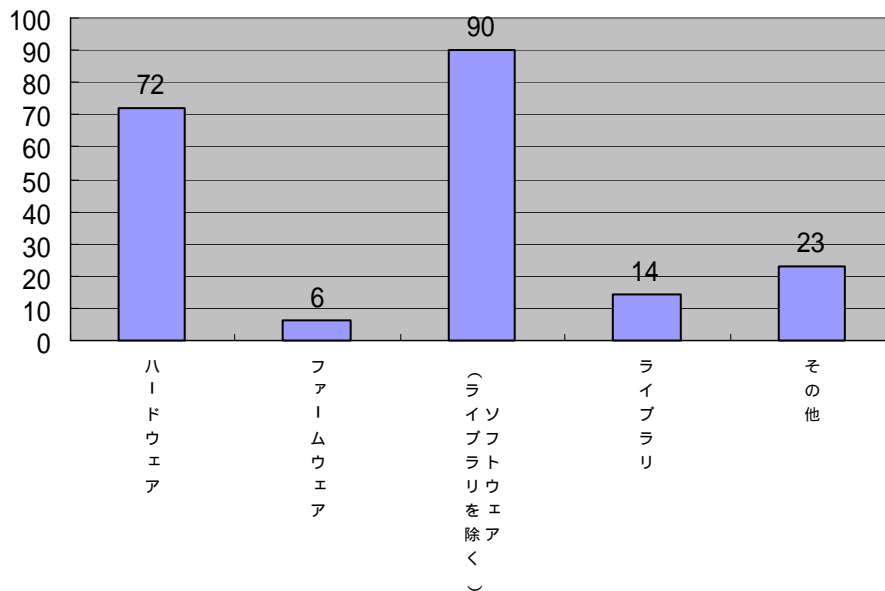


図 2.3 形態別製品数[暗号モジュール製品以外]（複数選択、単位：製品、N=188）

回答があった暗号モジュール製品以外の暗号関連製品の用途について見ると、大分類で見た「暗号化製品」、「認証関連製品」が多い点は暗号モジュール製品の傾向と類似している。しかし、暗号モジュール製品では少なかった「VPN 関連製品」が小分類単位では最も多くなっている。(図 2.4)

暗号モジュール製品では種類が少なかった「VPN 関連製品」が、暗号モジュール以外の暗号関連製品では多数の種類があるということは、このカテゴリの製品の中心が、暗号機能以外を含んだ製品であることを意味している。

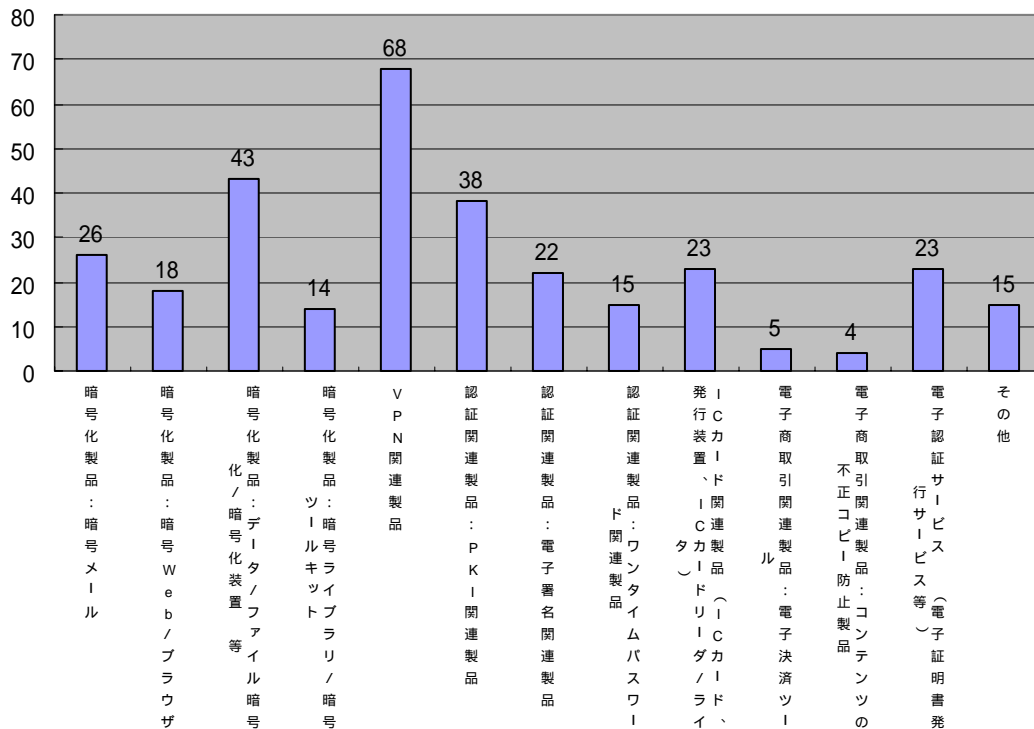


図 2.4 用途別製品数[暗号モジュール製品以外]（複数選択、単位：製品、N=174）

(2) 製品に採用されている暗号仕様

a. 暗号モジュール製品

暗号モジュール製品について見ると、公開鍵暗号方式に対応している製品が多い。公開鍵暗号方式のうち署名に用いられるものの中では、RSASSA-PKCS1-v1_5に対応している製品が多く、DSAがそれに次ぐ。また、鍵共有に用いられるものの中では、RSAES-PKCS-v1_5に対応する製品の数とDHに対応する製品の数が拮抗している。(図 2.5)

共通鍵暗号方式への暗号モジュール製品の対応状況では、64 ビットブロック暗号である 3-key Triple DES に対応している製品数が最も多く、128 ビットブロック暗号である AES およびストリーム暗号である 128-bitRC4 がそれに続いている。なお、「電子政府推奨暗号リスト案」には掲載されていない共通鍵暗号方式(選択肢「共通鍵暗号 - その他」)に対応している暗号モジュール製品が多い。ただし、これらの製品の中には「電子政府推奨暗号リスト案」に掲載されている暗号仕様に対応しているものもある。

また、ハッシュ関数では SHA-1 の対応製品数が最も多く、SHA-256、SHA-384、SHA-512 がそれに続く。

b. 暗号モジュール製品以外の暗号関連製品

暗号関連製品について見ると、暗号モジュール製品よりも特定の暗号仕様への集中がはっきりしている。特に、多くの製品に対応しているのは、共通鍵暗号方式では 3-key Triple DES、AES である。また、署名に使われる公開鍵暗号方式では RSASSA-PKCS1-v1_5、鍵共有に使われる公開鍵暗号方式では DH、ハッシュ関数では SHA-1 に対応する製品がそれぞれ区分の中で目立って多くなっている。(図 2.6)

なお、暗号モジュール製品以外の暗号関連製品でも、「電子政府推奨暗号リスト案」には掲載されていない共通鍵暗号方式(選択肢「共通鍵暗号 - その他」)に対応している製品が多く、こうした製品は、回答があった製品のほぼ半数に達している。なお、「電子政府推奨暗号リスト案」に掲載されていない暗号仕様にのみ対応している製品は 50 製品であった。

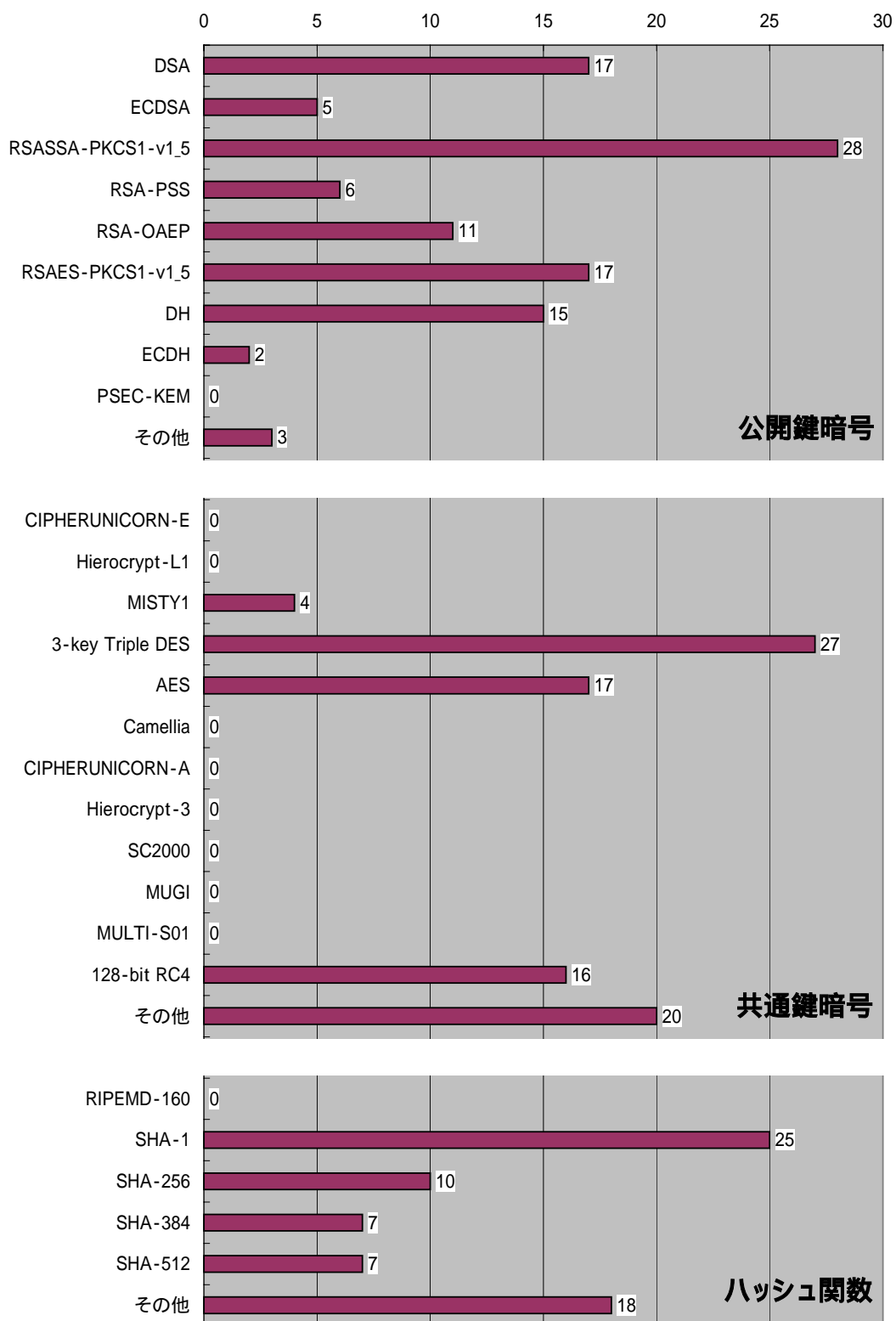


図 2.5 対応している暗号仕様[暗号モジュール製品] (複数選択、単位:製品、N=43)

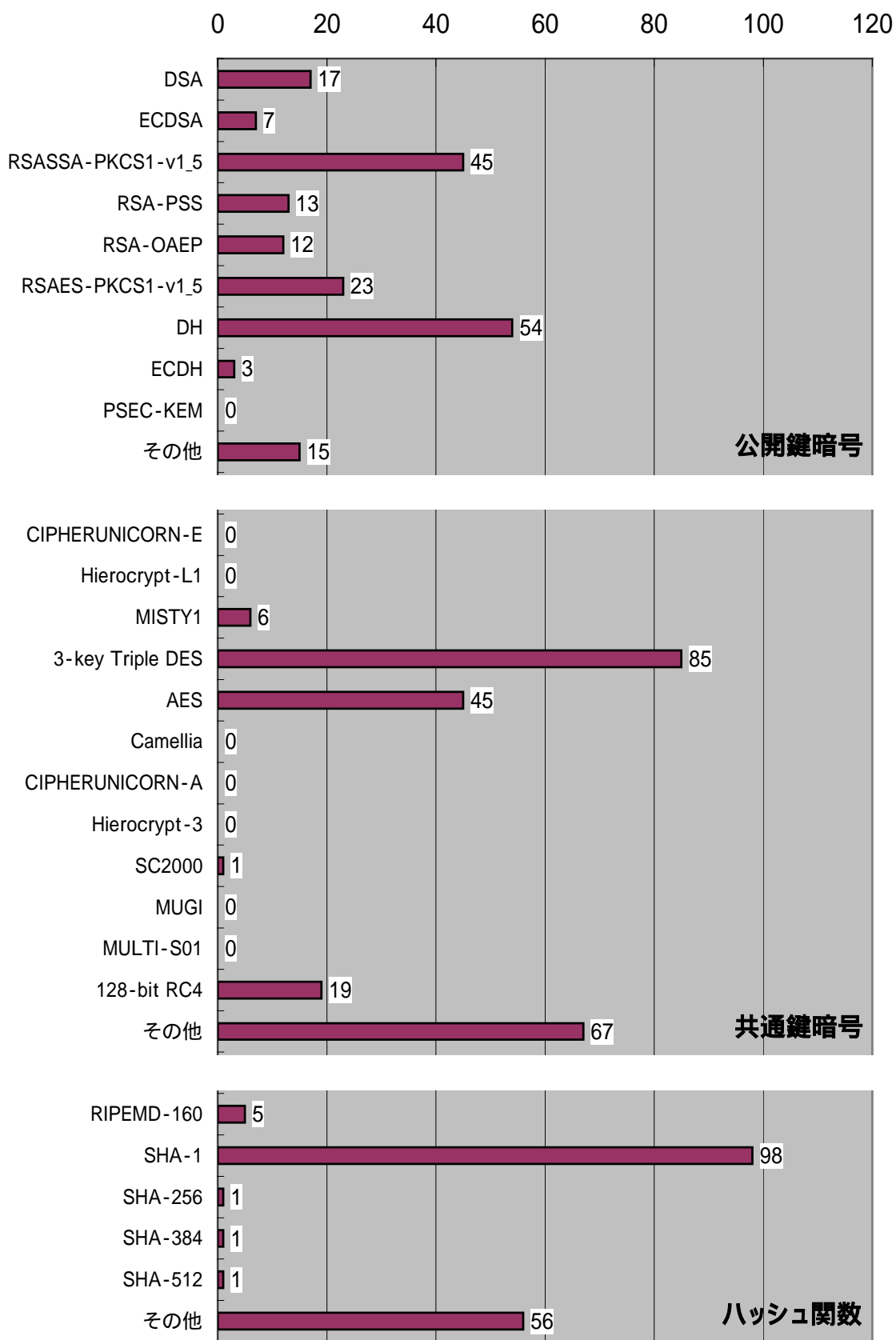


図 2.6 対応している暗号仕様[暗号モジュール製品以外] (複数選択、単位:製品、N=161)

(3) 製品に採用されている乱数生成器・素数検定法・インタフェースプロトコル

a. 乱数生成器

独自と回答したものを除くと、10 種の乱数生成器が暗号モジュール製品に採用されているが、目立って多い方式はない。暗号関連製品においては、4 製品に採用されている SPRINGS が最も多く採用されている乱数生成器であるが、この 4 製品とも韓国のセキュリティベンダにより提供されている。

表 2.1 使用している乱数生成器[暗号モジュール製品](複数選択、単位:製品、N=17)

乱数生成器(暗号モジュール製品)	製品数
Blum Blum Shub	1
ClutterBox	1
EntropyPoller	1
FIPS 186-1 準拠	2
FIPS 186-2	1
IC チップ機能及びドライバソフトウェア	2
IntelChipset	1
MT19937	1
ハッシュベースの擬似乱数生成	2
擬似乱数生成器	1
独自	4

表 2.2 使用している乱数生成器[暗号モジュール製品以外](複数選択、単位:製品、N=24)

乱数生成器(モジュール関連製品)	製品数
Blum Blum Shub	1
Java Security API	1
Mersenne Twister	2
PRNG based on SHA-1	3
Quasar	1
Security Control Device	1
SPRINGS(Future Systems 社製)	4
X.509V3	1
XRNG based on SHA-1	2
ソフトによる擬似乱数	1
独自	7

b. 素数検定法

素数検定法についてみると、ラビン法が暗号モジュール製品では 17 製品中 10 製品、暗号モジュール製品以外の暗号関連製品では 11 製品中 9 製品を占めておりどちらも過半を占めている。

表 2.3 使用している素数検定法[暗号モジュール製品](複数選択、単位:製品、N=17)

素数検定法	製品数
Fermat's Test	1
IEEE P1363	1
Lucasx Lehmer Test	2
Pocklington 法	2
ラビン法	10
独自	1

表 2.4 使用している素数検定法[暗号モジュール製品以外](複数選択、単位:製品、N=11)

素数検定法	製品数
Pocklington 法	1
ラビン法	9
確定方式	1
独自	1

c. インタフェース/プロトコル

暗号モジュール製品について見ると、これについて回答のあった 31 製品で使用されているインタフェース/プロトコルは 30 種類を超える。その中で最も使用されているプロトコルである X.509 は、19 製品で使用されている。(表 2.5)

また、暗号モジュール製品以外の暗号関連製品では、これについて回答のあった 64 製品で 20 種類を超えるインタフェース/プロトコルが使用されている。その中で多く使用されているインタフェース/プロトコルは、X.509、PKCS#7、PKCS#11、PKCS#12 及び IPSEC であり、それぞれ 18~26 製品で使用されている。(表 2.6)

表 2.5 使用しているインタフェースプロトコル[暗号モジュール製品]

(複数選択、単位:製品、N=31)

インタフェース / プロトコル(暗号モジュール製品)	製品数
CMP	2
CRL	1
CRLv1	1
CRLv2	1
CRS	2
Crypto-API	5
Encryption	1
IEEE802.15.3	1
IPSec	5
ISDN(E - DSS,ITU-T)	1
ISO14443・15693	1
JCE	2
CRMF	1
OCSP	6
OpenSSL	2
PKCS#1	4
PKCS#10	5
PKCS#11	14
PKCS#12	7
PKCS#5	3
PKCS#7	6
PKCS#8	5
PKCS#9	1
S/MIME	2
SCEP	1
secsh	1
SERIAL(X-21、V-24、V-35)	1
SSL3.0/TLS1.0	1
SSL3.0/TLS2.0	2
SSL1.0	1
SSL2.0	3
SSL3.0	4
TLS1.0	3
X.509	19
XML Digital Signature	4

表 2.6 使用しているインタフェースプロトコル[暗号モジュール製品以外]

(複数選択、単位:製品、N=64)

インターフェイス/プロトコル名(モジュール関連製品)	製品数
CSP	1
CryptoAPI	2
DPTP	1
IPSec	18
PKCS#7	16
PKCS#10	7
PKCS#11	26
PKCS#12	19
PKIX-CMP	2
S/MIME	4
SSL	1
SSL3.0	9
SSL3.0/TLS1.0	8
RFC-2314	2
RFC-2315	2
RFC-2459	2
RFC-2510	2
RFC-2511	4
RFC-2560	2
RFC-2587	2
RFC-2630	2
RFC-3161	2
RFC-3280	2
RFC-3281	2
X.509	26
セキヤシールド	1

2.2 第三者評価の実施および認証取得に関する現状

本節では、アンケート調査結果に基づき、暗号モジュール製品及び暗号モジュール製品以外の暗号関連製品における第三者評価の実施および認証取得に関する現状を整理する。

(1) 暗号モジュール評価認証取得状況

回答があった暗号モジュール製品 58 製品のうち、FIPS140 の認定を受けている製品は 7 製品である(図 2.7)。また、暗号関連製品 138 製品のうち、FIPS140 の認定を取得している製品は 28 製品である(図 2.8)。

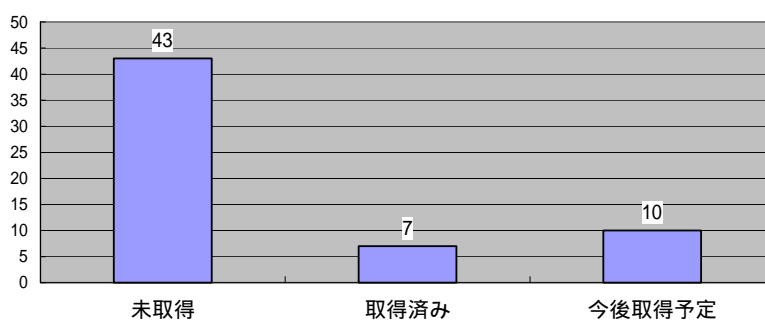


図 2.7 暗号モジュール評価・認証取得状況[暗号モジュール製品]

(複数選択、単位:製品、N=58)

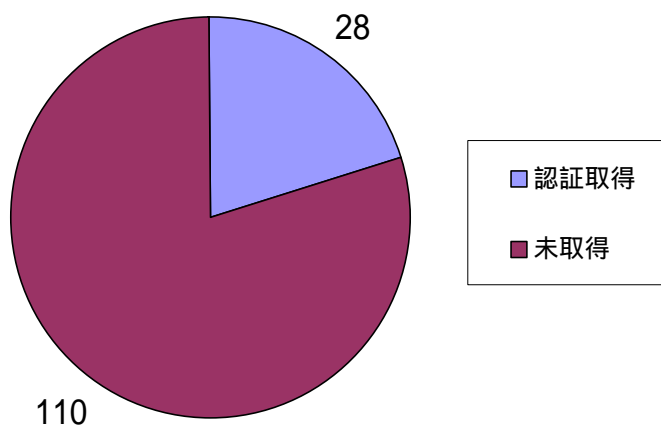


図 2.8 暗号モジュール評価・認証取得状況[暗号モジュール製品以外]

(単一選択、単位:製品、N=138)

(2)暗号モジュール評価認証の取得予定

有効な回答があった暗号モジュール製品 58 製品のうち、10 製品が FIPS140 の認証取得の予定があると回答している。ただし、そのうちの 2 製品は既に FIPS140 を取得している製品であり、仕様変更などに伴い改めて取得するものと考えられる。従って、取得予定のある 10 製品のうち、新たに認証を受けようとしている製品は 8 製品ということになる。(表 2.7)

また、暗号モジュール製品以外の暗号関連製品においては、17 製品が FIPS140 の認証取得を予定している。なお、そのうち 5 製品はすでに FIPS140 を取得している製品であり、これも仕様変更などに伴い改めて取得するものと考えられる。(図 2.9)

表 2.7 FIPS140 取得状況および予定 [暗号モジュール製品]

(一部複数選択、単位:製品、N=58)

回答番号	暗号モジュール製品の FIPS140 認定取得状況	製品数	認証の種類別	製品数	レベル	製品数
1	未取得	43				
2	取得済み	7	FIPS140-1	5	1	2
					2	1
					3	2
					4	0
			FIPS140-2	1	1	0
					2	0
					3	1
回答なし	1					
3	今後取得予定	10	FIPS140-1	1	1	0
					2	0
					3	1
					4	0
			FIPS140-2	5	1	3
					2	0
					3	2
					4	0
			不明	1		
			回答なし	3		

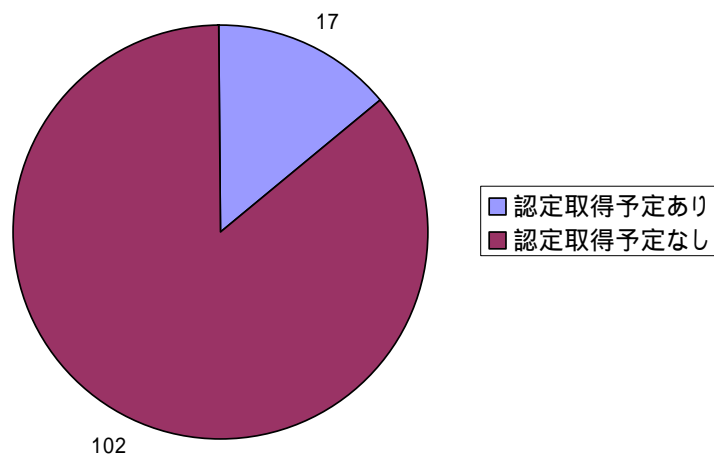


図 2.9 FIPS140 取得状況および予定 [暗号モジュール製品以外]
(単一選択、単位:製品、N=119)

(3)暗号モジュール評価認証取得製品の組み込み状況および組み込み予定

暗号モジュール製品以外の暗号関連製品のうち、暗号機能を実現する部分を暗号モジュール製品として物理的に分離可能なものは 39 製品である。その 37 製品のうち、FIPS140 認定の暗号モジュール製品を組み込んだ製品は 10 製品あった(表 2.8)。また、今後、FIPS140 の認定を取得した暗号モジュールを組み込んでいく予定があると回答のあった製品は 3 製品であった(表 2.9)。

表 2.8 認証取得暗号モジュールの組み込み状況(自由記述、単位:製品、N=10)

開発元	製品に組み込まれているFIPS140認定暗号モジュール製品の名称	製品数	認証の種別
Datakey.Inc	Datakey CIP	2	FIPS140-1 レベル2
F-Secure Corporation	F-Secure Cryptographic Service Provider	3	FIPS140-1 レベル1
nCipher	nForce	2	FIPS140-1 レベル3
S (セコ-インスマツ株式会社)	s-Keyper	2	FIPS140-1 レベル4
SafeNet Inc.	SoftRemote	1	FIPS140-1
SafeNet Inc.	CGX	2	FIPS140-2 レベル3

表 2.9 認証取得暗号モジュールの組み込み予定(単一選択、単位:製品、N=8)

FIPS140認定を受けた暗号モジュール製品を組み込む予定があるか	製品数	認証の種別	製品数
はい	3	FIPS140-1 レベル2	1
		FIPS140-1 レベル3	2
		FIPS140-2	0
いいえ	5		

(4) IT セキュリティ製品評価・認証取得状況

暗号モジュール製品では、FIPS140 以外のセキュリティ認証の取得はほとんど行われていない。一方、暗号モジュール製品以外の暗号関連製品では、31 製品が CC (ISO/ISE15408、JISX5070) の認証を取得している。また、CC 以外で多くの製品が取得している認証としては、26 製品が取得している ICESA がある。(表 2.10、表 2.11)

表 2.10 評価・認証取得状況[暗号モジュール製品](複数選択、単位:製品 N=5)

暗号モジュール製品において Fips140以外で取得した標準化規格	製品数
ITSEC	1
TCSEC	0
CC (ISO/ISE 15408/JIS X 5070)	3
その他	2

暗号モジュール製品において CCを取得した製品の認証レベル	製品数
EAL1	0
EAL2	0
EAL3	0
EAL4	1
EAL5	1
EAL6	0
EAL7	0

表 2.11 評価・認証取得状況[暗号モジュール製品以外](複数選択、単位:製品 N=62)

暗号関連製品において Fips140以外で取得した標準化規格	製品数
ITSEC	48
TCSEC	3
CC (ISO/ISE 15408/JIS X 5070)	31
その他	34

暗号関連製品において CCを取得した製品の認証レベル	製品数
EAL1	0
EAL2	8
EAL3	2
EAL4	14
EAL5	0
EAL6	0
EAL7	0
回答なし	7

2.3 自己評価の実施に関する実態

本節では、アンケート調査結果に基づき、暗号モジュール製品における製品の自己評価(自己検証)の実施に関する現状を整理する。なお、定量的な集計に十分な有効回答数が得られなかったため、一部の設問は定性的な整理を行っている。

(1) 暗号モジュール製品の自己評価の実施状況

開発元企業が販売窓口となっている延べ 33 製品の暗号モジュール製品の約半数にあたる延べ 17 製品が自己検証試験をおこなっている。(図 2.10)

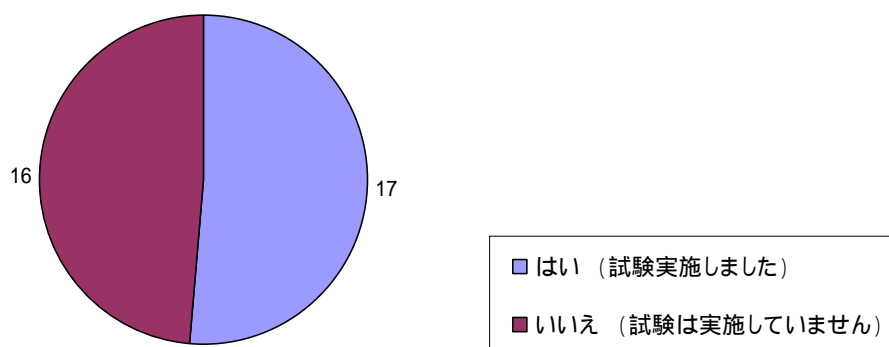


図 2.10 暗号モジュール自己評価(自己検証)の実施状況[開発元 = 販売窓口]
(単位:延べ製品 N=33)

また、販売窓口が開発元ではない(すなわち、販売窓口と開発元が異なる)延べ 21 製品においても、約半数にあたる延べ 10 製品が自己検証の実施や外部へ検証試験の実施委託を行っている。

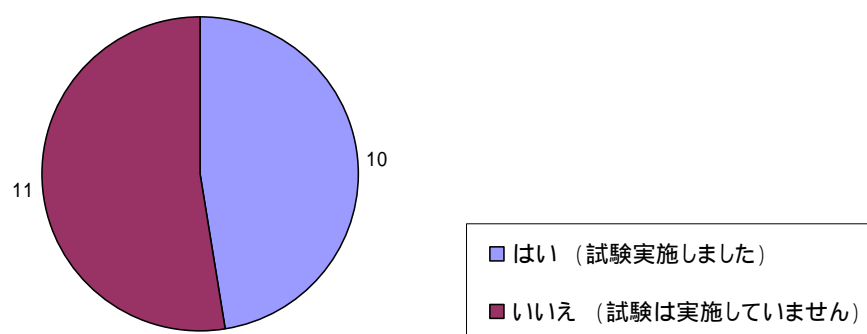


図 2.11 暗号モジュール自己評価(自己検証)の実施状況[開発元 ≠ 販売窓口]
(単位:延べ製品、N=21)

また、暗号モジュール製品の検証をおこなっている企業についての評価の目的は、無回答の1製品を除きすべて、「品質保証としての要件充足」および「カタログ等に機能・性能を表示するための機能検証」である。(図 2.12)

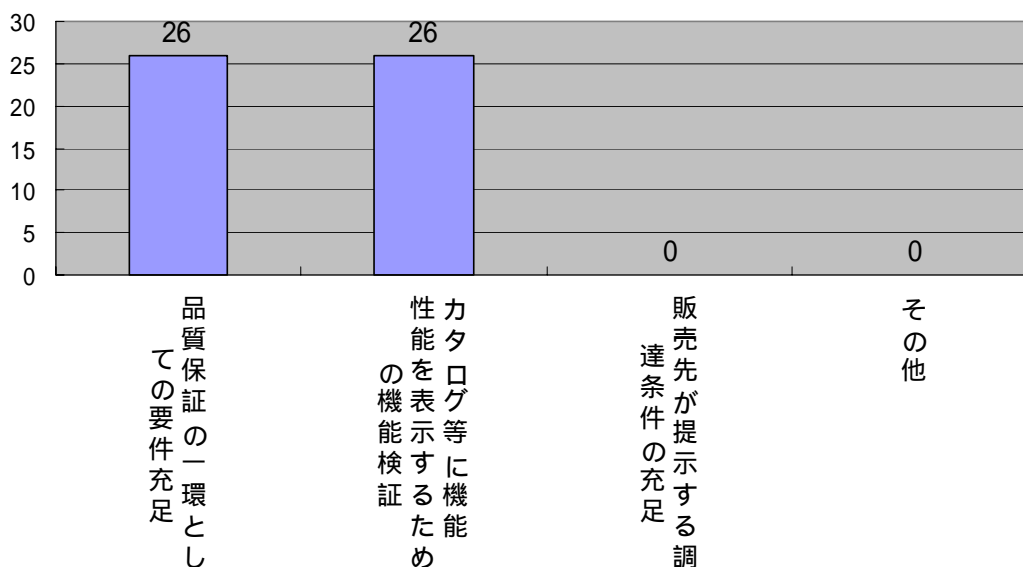


図 2.12 自己評価(自己検証)の実施理由(複数選択、単位:延べ製品、N=27)

(2) 暗号モジュール製品の自己評価の実施における体制、基準、期間・費用

暗号モジュールの検証試験の実施体制としては、検証を実施している 27 製品のうち 2 社を除きすべての企業が自社で検証試験を行っている。(表 2.12)

表 2.12 自己評価(自己検証)の実施体制 (単位:延べ製品 N=27)

検証実験の実地体制について	製品数
自社内の体制で実施	25
自社が外部の企業・機関に全てを委託して実施	0
自社が外部の企業・機関に一部を委託して実施	1
回答なし	1

また、検証試験において FIPS140 等に準拠した検証試験を行っているのは 3 製品 (FIPS140-1 レベル 3) である (表 2.13)。その他の多くは自社基準で検証試験を行っており、その対象を FIPS140 の要求条件の分類に当てはめて整理すると、「自己検査」が 11 製品、「インタフェース」が 9 製品と、これら 2 つの項目が約半数にのぼっている。

表 2.13 自己評価の基準（複数選択、単位：延べ製品、N=27）

検証の基準	製品数
FIPS140-1 レベル1	0
FIPS140-1 レベル2	0
FIPS140-1 レベル3	2
FIPS140-1 レベル4	0
FIPS140-2 レベル1	0
FIPS140-2 レベル2	0
FIPS140-2 レベル3	0
FIPS140-2 レベル4	0
Common Criteria(CC) EAL1	0
Common Criteria(CC) EAL2	0
Common Criteria(CC) EAL3	0
Common Criteria(CC) EAL4	0
Common Criteria(CC) EAL5	0
Common Criteria(CC) EAL6	0
Common Criteria(CC) EAL7	0
その他の公開されている基準	
FIPS 140-1 (statistical random number generator test)	1
IETF	2
NISTSP800-22	1
自社基準	11

自己評価に要した期間、費用、稼働工数については、回答が得られた企業が少なかったため、同行を定性的に見ることとする。

- 自己評価に要した期間について、アンケート調査での回答は最長が 6 ヶ月、最短が 0.5 ヶ月であった。なお、6 ヶ月と回答している製品は延べ 3 製品である。
- 自己評価に要した費用について、アンケート調査での回答は最高が 7,200 千円、最低が 800 千円であった。
- 自己評価に要した稼働工数について、アンケート調査での回答は最高 3 人月、最低が 1 人月であった。

3. 暗号モジュール製品の市場動向

3.1 暗号モジュール製品を含む暗号関連製品市場の動向

(1) 販売窓口の製品取扱に関する状況

暗号モジュール製品の販売窓口に対して、現在取り扱っている暗号モジュール製品の数についてアンケート調査で尋ねた。該当する設問に回答があった26社¹の取扱製品の合計は60製品であり、現在の1社当りの平均取扱製品は2.31製品である。26社のうち、14社は取扱製品が1つだけであり、取扱製品が3種類以下の販売窓口だと20社以上と大半を占める。このように、数多くの種類の暗号モジュール製品を取り扱う販売窓口は少なく、取り扱う製品を絞り込んでいる。(表3.1)

そのような中、10種類以上の製品を扱う販売窓口は海外の大手セキュリティベンダーの日本法人であるRSAセキュリティ(株)のみであった。この販売窓口は、国内で暗号機能を実装するためのライブラリ製品を中心に12種類の製品を販売している。日本国内に出自を持つ販売窓口の中で最も多くの種類を販売しているのは、三菱電機インフォメーションシステムズ(株)と半導体製造機器を販売している(株)ダイヘンであり、それぞれ6製品を販売している。前者は大手電機メーカーであるこの会社の親会社が開発した暗号アルゴリズムを搭載したライブラリ製品を中心とした製品を販売している。また、後者はLSIに組み込んで暗号機能を実現するIP(設計資産)を6種類販売している。

表3.1 販売窓口ごとの暗号モジュール製品の平均取扱製品数(現状)

平均取扱製品数
2.31

国内の販売窓口が扱う製品の開発元は、全体では販売窓口とほぼ同数の25社に渡る。名前が挙がっているそれぞれの開発元について見ると、1社が複数の製品の開発元として登場するケースは比較的少なく、複数の製品の開発元として登場しているのは25社のうち7社に留まる。また、複数の販売代理店等を通じて販売している開発元は、国内のベンチャー系企業1社だけである。これは、ネットワーク機器等の暗号関連製品とは異なり、暗号モジュール製品は開発した企業が自ら販売する、あるいは特定の販売窓口のみを通じて販売するという形態が中心になっていることを窺わせる。

(2) 海外企業が開発した製品の進出状況

a. 現在の状況

アンケートで回答のあった61製品について、開発元企業が日本企業であるか海外の企業であるかによって分類し集計を行った。それぞれの販売数量を網羅的に把握できていないため国内製品・

¹ 当該設問に回答がなかった暗号モジュール製品販売窓口が2社あった。

海外製品それぞれのマーケットシェアは明らかではないが、製品の種類だけで見ると、海外製品は日本市場の中で一定以上の存在感を持っていると見ることができる。

ハードウェア、ファームウェア、ソフトウェア、ライブラリの製品区分別に国内製品と海外製品の割合を見ると、どの区分においても海外製品の種類が国内製品の種類とほぼ同数である。ただし、国内製品は海外製品に比べてソフトウェアとハードウェアをパッケージ化した製品が多く、それらの製品が複数の区分でカウントされている。そのため、純粋なソフトウェア製品やハードウェア製品で比較をした場合、海外製品の数の方が多くなる。

多くの海外製品が国内市場に進出する理由としては、国内で開発された製品の競争力が脆弱であるか、カバーしきれない領域があるといったことが考えられる。仮に、国内製品がカバーしきれない領域があることが理由であるとしても、海外製品がこれほど多くの種類あるということは、国内で開発された製品がカバーしていない領域はある程度の規模を有するマーケットであると想像できる。

インタビューにおいても、日本製品を取り扱う販売窓口からは、海外製品を強く意識している意見が聞かれた。また、反対に、海外製品を取り扱う販売窓口では、国内製品を競合として見なす意識はそれほど高くない。例えば、海外の大手セキュリティベンダーは、日本市場のソフトウェア・ライブラリ製品の分野で既に高いシェアを獲得しており、競合として意識しているのはフリーウェアやオープンソースだけとのことであった。また、別の海外のハードウェア製品を取り扱っている販売窓口でも、日本製品で競合製品として意識しているものはなく、競合となりうるのは他の海外製品であるという意見であった。

こうした結果を見る限り、現状では、国内の市場において海外の企業で開発された暗号モジュール製品が概して優勢であることが窺える。製品の分野によっては、種類としては日本企業で開発された暗号モジュール製品が多くあるものの、販売面では海外の製品に苦戦を強いられているというようなケースもあると想像できる。

b. 今後の動向

暗号モジュールの種類において、少なくとも既存の暗号モジュール製品の分野では、海外の企業が開発した製品が日本国内の市場をリードしていくことになると考えられる。ビジネスとしての成否を考えると、既にワールドワイドに展開している海外製品と直接競合する分野で新たな暗号モジュールの開発に取り組む動きが、日本企業の間にはあまり期待できない。その理由としては、暗号関連製品全般に、市場での認知度やブランド力が利用者側の製品選定の基準となる傾向があることが挙げられる。既にデファクトスタンダードとなる海外製品が現れてきている現状を考えると、今後、既存の暗号モジュール製品市場で国内製品の種類が大きく増えていくことは考えにくい。

そのため、今後、日本企業で開発される製品と海外の企業で開発された製品の市場での形勢が変わるとするならば、現状、完全に確立していない分野での日本企業が開発する製品が優位に立つ場合であろう。日本企業が未開拓の分野において暗号モジュール製品を開発し、その分野で優位性を築けば、現在の海外の製品が優勢な暗号モジュール市場の状況が変わる可能性はある。

3.2 今後5年間に於いて国内暗号市場に影響を与える技術的・制度的要因

(1) 暗号モジュールが対応する暗号アルゴリズムに影響する要因

2000年に、電子政府のセキュリティ確保のための暗号技術の評価検討を行う組織としてCRYPTRECが設立され、これまでに開発元などから応募のあった暗号アルゴリズムの評価を行ってきた。そして、2002年にはその評価結果を元に「電子政府推奨暗号リスト案」を公表している。

今後5年間を見通した暗号モジュール製品が対応する暗号アルゴリズムの増減について、暗号モジュール製品の販売窓口に対するアンケート調査で尋ねた。さらに、CRYPTRECによる暗号アルゴリズム評価や暗号アルゴリズムの標準化などのインパクトについても質問した。

まず、販売窓口の今後5年間に取扱製品が対応する暗号アルゴリズムの数に関する予想は、「対応するアルゴリズムが増える傾向にある」が過半を占め、次いで「現状とほぼ変わらない」が3割を超える。反対に、「減る傾向にある」と予想している販売窓口は1社だけである。(図3.1)

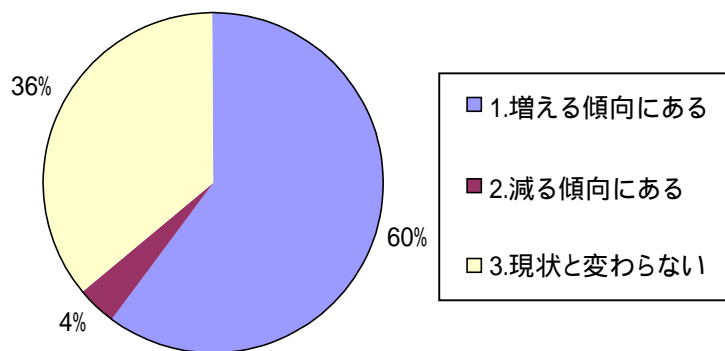


図3.1 今後5年間の暗号モジュール製品の対応暗号アルゴリズム数に関する想定(N=25)

「増える傾向にある」と回答した販売窓口に対して対応する暗号アルゴリズムが増えるという予想の理由を尋ねたところ、「政府調達要件や規格・標準に適合するアルゴリズムに新たに対応するから」と回答した販売窓口が6割を占め、「政府調達要件や規格・標準に関係なく新たなアルゴリズムに対応する」と回答した販売窓口を上回った(図3.2)。また、「現状とほぼ変わらない」と回答した販売窓口では、「政府調達要件や規格・標準に適合するアルゴリズムに入れ替える」と回答した販売窓口が6割以上を占め、「アルゴリズムの入れ替えはなく現状のまま推移する」と回答した販売窓口を上回っている(図3.3)。

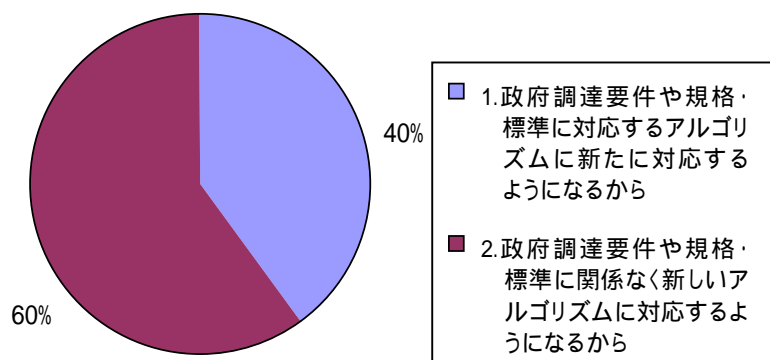


図 3.2 増える傾向にあると回答した理由 (N=15)

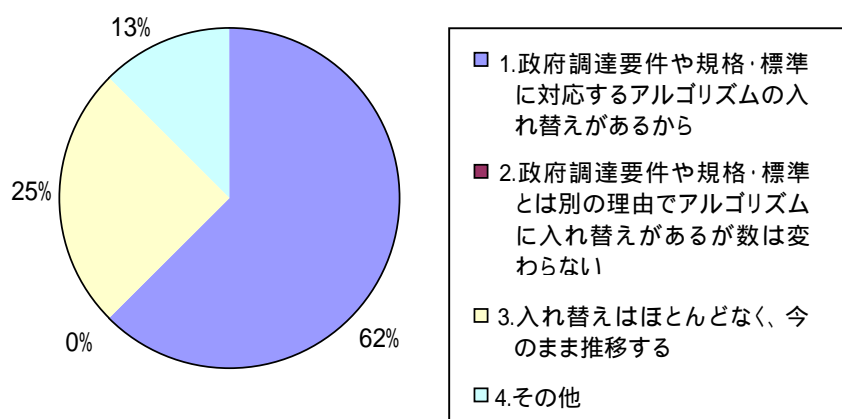


図 3.3 変わらないと回答した理由 (N=9)

なお、有識者や販売窓口に対するインタビューでは、「電子政府推奨暗号リスト」の作成などの政府調達の動向が市場全体における暗号モジュール製品の種類の増減に直接的な影響を及ぼすとする意見はなかった。今後 5 年間で、市場の構造を変えるような新しいアルゴリズムの登場の可能性も定かではなく、いわゆる「ネットワークの経済性」²を意識したデファクトスタンダードへの収斂、開発費用低減を意識した無償アルゴリズムの採用増加の方が、トレンドに影響するという指摘があった。

こうしたことをまとめると、今後 5 年間を見通した場合、電子政府推奨暗号リストやその他の基準・標準を受けて、暗号モジュールに採用される暗号アルゴリズムの追加や入れ替えが行われることが予想できる。また同時に、これらとは関係のない理由による暗号アルゴリズムの追加が行われうるが、

² ネットワークへの参加者が増えることにより、ネットワーク参加者の費用低減や便益の向上が図られること。ここでは、より多くの相手との相互運用性が保証された方式を選択して、複数の方式を併用することによる負担の発生を回避すること。

それは新しいアルゴリズムの登場に起因するものではなく、その製品が対応していない既存アルゴリズムの追加が中心になると考えられる。

(2) 暗号アルゴリズム以外の部分に影響を与える要因

アルゴリズムではなく、純粋に暗号モジュールの製品数を増やしうる技術的要因として、暗号モジュールを搭載するプラットフォームの多様化を考えることができる。インタビューでは、情報家電や IC カード等への組み込みを想定した暗号化チップ等の分野において日本企業が強みを発揮する可能性があるという指摘があった。今後、ユビキタス化の進展にともない、こうした分野での暗号モジュールの需要が高まることが予想されている。

今後、新たなプラットフォームへの暗号モジュール搭載によって登場しうる製品の一例として、IC カードが多機能になることに関連した暗号化チップ、リーダ・ライタ等の周辺機器等の暗号モジュール製品などを挙げることができる。ただし、こうした暗号モジュールを搭載するプラットフォームの広がり、一般に広く行き渡る安価な製品に向かっていくものであるため、暗号モジュール自体の単価は現状の暗号モジュール製品よりもかなり低くなっていくと考えられる。

3.3 今後 5 年間を見据えた国内市場の暗号関連製品数の予測

(1) 販売窓口における暗号モジュール製品の取扱の動向

a. 市場全体における暗号モジュール製品の種類

今後想定される暗号の利用範囲の拡大に伴って、データ暗号化、メール・通信の暗号化といったアプリケーションレベルでの暗号関連製品が大きく増えていくことが予想される。しかし、暗号化・複合等の基盤部分を実装した暗号モジュール製品の種類は複数の製品間で共通化でき、また製品の開発コスト低減のためにはそうすることが好まれることから、暗号関連製品ほどには増加しないと考えられる。

b. 販売窓口の取扱製品数に関する意向

暗号モジュール製品の販売窓口を対象にしたアンケート調査では、5 年後(2007 年度)までに取り扱う暗号モジュール製品の種類を増やすと想定している企業がおよそ 7 割、変わらないと想定している企業がおよそ 3 割であった。なお、取り扱う暗号モジュール製品の種類を減らすことを想定している企業はなかった。(図 3.4)

取扱製品を増やす理由として、「開発各社がリリースする暗号モジュール製品種の増減に合わせて、取扱を増やす」を選んだ販売窓口が全体の約 6 割を占めている。この結果から、販売窓口の多くは開発元の製品開発の動向によって取扱製品の種類の増減を決めており、今後も開発元での新たな製品開発が進み製品の種類が増加すると見込んでいることが分かる。(図 3.5)

なお、それぞれの暗号モジュール販売窓口に 5 年後に取り扱う暗号モジュール製品の数の想定を尋ねた。その回答の 1 社当りの平均値は 4.81 製品である。それを現在の取扱製品数の平均値(2.31 製品)で除した販売窓口 1 社当りの取扱製品数の今後 5 年間の伸び率は約 2.08 倍となる(表

3.2)。そこで、既存の暗号モジュール製品販売窓口が取り扱う製品数について、今後 5 年間の伸び率の予測値を 2.08 倍とする。

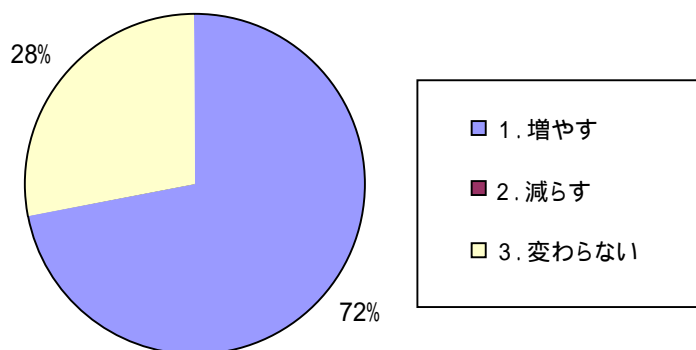


図 3.4 今後 5 年間ににおける暗号モジュール製品の取扱製品数の想定 (N=25)

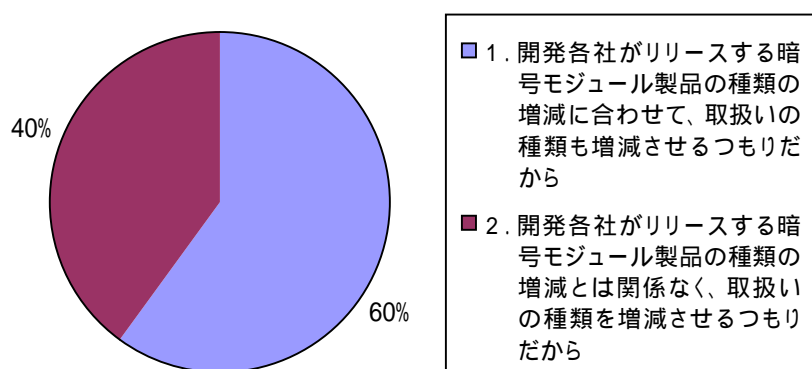


図 3.5 今後 5 年間に暗号モジュール製品の取扱製品数を増やす理由 (N=17)

表 3.2 販売窓口 1 社当りの暗号モジュール製品の取扱製品数

	現在 (2002 年度) (a)	5 年後 (2007 年度) の想定 (b)	今後 5 年間の伸び率 (b/a)
販売窓口 1 社当りの取扱製品数 (平均値)	2.31 製品	4.81 製品	2.08 倍

一方、暗号モジュールを需要する側である暗号関連製品の販売窓口を対象としたアンケートの回答を基に、5 年後における自社製品に搭載する暗号モジュールの種類を増減について集計した結果、増えると回答した企業が全体の約 6 割を占めた。一方、搭載する暗号モジュールの種類は減ると回答した企業は、全体の 1 割に満たなかった。(図 3.6)

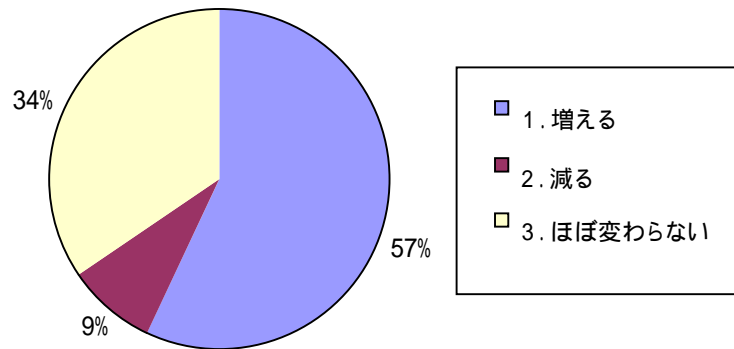


図 3.6 暗号関連製品に搭載される暗号モジュール製品数の増減の想定 (N=93)

増えると予想する理由として、「暗号モジュールを搭載する製品を開発する側が、搭載可能な暗号モジュールを揃えるようになるため」と回答した企業が、全体の約 6 割を占めた。ただし、インタビューでは販売窓口や有識者から、暗号部分については出来合いの暗号モジュール製品を組み込んで製品やシステムを開発するメーカー等が増えていること、そして今後もそのような動きが増加する可能性が高いことなどの見解が示された。このことから、開発元が自社の暗号関連製品に搭載可能な暗号モジュールをすべて自社で開発するのではなく、他社から調達して提供するような動きが増えてくる方向に向かう可能性があると考えられる。(図 3.7)

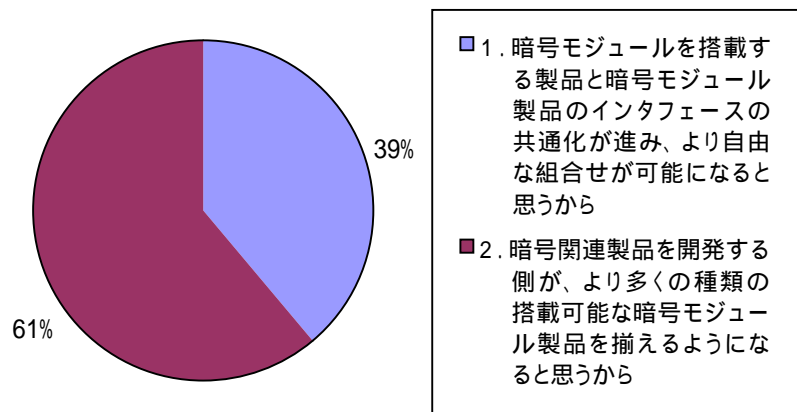


図 3.7 搭載される暗号モジュール製品数が増える想定の理由 (N=54)

ただし、少ないながらも、減らすと回答した企業においては、その理由として“市場全体を通じて、暗号関連製品に搭載される暗号モジュールが少数の暗号モジュール製品に絞り込まれていく”と考えているところが多い。(図 3.8)

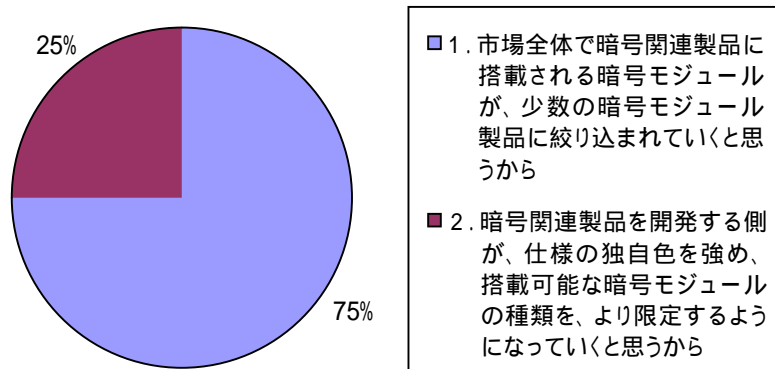


図 3.8 搭載される暗号モジュール製品数が減る想定の原因 (N=4)

c. 販売窓口の市場動向の捉え方

インタビューにおいては、今後も暗号モジュール製品の種類は、大幅には増加しないだろうという意見が多く見られたのに対して、供給側であるモジュール製品の販売窓口、需要側である暗号関連製品の販売窓口に対するアンケートともに、取扱製品を増やすという回答が多かった。

これらの動きから、暗号モジュール製品を販売する窓口等は、市場において収斂された暗号モジュール製品について、取扱製品の種類を増減させるものと推測される。

(2) 今後 5 年間の国内市場における暗号モジュール製品数の推移予測

a. 算出の前提及び考慮すべき要因

今後 5 年間 (2002 年から 2007 年まで) の暗号モジュール製品の種類の推移を予想するに先立ち、推計の範囲と基準値を以下のように設定した。

【推計の範囲】

- 推計の対象範囲を、日本国内で販売されている暗号モジュール製品とした。フリーソフトのような無償で提供される製品については、推計の対象外としている。

【基準値】

- 暗号モジュールの販売窓口のアンケート結果を基に、現在、国内で販売されている暗号モジュール製品の種類を算出し、これを基準値として今後 5 年間における予測を行った。

b. 考慮すべき要因と今後 5 年間の増減に関する仮説

今後 5 年間に暗号モジュールの製品数の増減を考えるに当たり、暗号モジュール製品の販売窓口に対するアンケート調査では捕捉し切れない、国内市場に新規に参入するベンダの動向について以下に示す仮説を設定した。

【想定される暗号モジュールを開発する国内ベンダの数】

- 暗号モジュール製品を開発するベンダの数は、今後 5 年間で微増にとどまる。インタビューにおいては、暗号モジュールを開発できる国内企業は、大手電機メーカー等に限定されるという意見や新規参入が難しく、新興のベンチャー企業が事業を継続していくのは難しいという意見が多く見られ、国内における開発ベンダの数は大幅に増加しないと考える。

【海外ベンダの新規参入】

- FIPS140 の認証取得した海外ベンダを中心に、新規参入が続く。既に、日本市場で販売されている暗号モジュール製品の半数以上が海外の製品であることを考えると、今後も海外ベンダの開発製品が日本市場への参入があると考ええる。

c. 今後 5 年間の国内市場における暗号モジュール製品数の予測値

暗号モジュール製品を販売する販売窓口を対象としたアンケートの回答結果から 5 年後の国内市場で販売される暗号モジュール製品の数の予測値を算出した。表 3.3 に示すとおり、この予測では 5 年後の製品は 141 製品である。この値は現在の 61 製品の 2.3 倍に当る。なお、この製品数の算出にあたっては、暗号分野における有識者、暗号モジュールの需要側である SI 事業者、暗号モジュールの販売窓口のインタビューでの意見等を考慮した。

【算出の方法】

1.国内市場に既参入の開発元・販売窓口の製品

- アンケートにて捕捉した暗号モジュール製品 : 61 製品
- 既存の開発元が既存の販売窓口を通じて販売される製品数の伸び : 2.08 倍
表 3.2 に示した販売窓口 1 社当り取扱製品数の今後 5 年間の伸び率を用いた

2.国内市場に未参入の開発元・販売窓口の製品

- 5 年間で新規参入する海外開発元 : 3 社
NIST の FIPS140 取得製品リストを参照して、日本に進出していない開発元のうち、今後 5 年間に国内市場に参入する企業を見積もった
- 新規参入する海外開発元の 1 社当りの国内市場投入製品数 : 4.81 製品
各開発元の製品を国内の販売窓口一社が独占的に取り扱うことを想定し、表 3.2 に示した販売窓口 1 社当り取扱製品数に関する 5 年後の想定の平均値をそのまま用いた

表 3.3 国内市場で販売される現在の暗号モジュール製品の数と 5 年後の予測値

	現在(2002年度)	5年後(2007年度)
国内市場に既参入の開発元・販売窓口の製品:(a)	61 製品	127 製品 (= 61 製品 × 2.08 倍)
国内市場に未参入の開発元・販売窓口の製品:(b)	0 製品	14 製品 (= 4.81 製品 × 3 社)
国内市場で販売される暗号モジュール製品:(a)+(b)	61 製品	141 製品
今後 5 年間の伸び率 : (5 年後)/(現在)	2.3 倍 (=141 製品/61 製品)	

4. 暗号モジュール評価・認証制度のニーズ分析

4.1 評価・認証制度に関する暗号関連製品供給サイドの関心、ニーズ

(1) 暗号モジュール第三者評価の必要性に関する認識

a. 需要側の関心についての認識と現在の対応状況

現状の日本国内での調達において、「FIPS140 認証取得」などの暗号モジュールの第三者評価を要求されることがほとんどないこともあり、現状では、販売代理店は第三者評価の必要性をあまり感じてはいない。いまのところ、一部の政府調達で、第三者認証でなくてもよい「FIPS140 相当」(FIPS140 と同等の検証を行っている)を加点要素とするケースが現れているが、第三者評価が必要な FIPS140 の認証取得を要求するまでには至っていない。政府調達以外では、金融機関および医療分野で FIPS140 に関心が持たれ始めている程度というのが、暗号モジュール製品の販売窓口が持っている感触である。

いま、国内で入手可能な FIPS140 認定製品があるが、それらの製品は海外の市場(ほとんどの場合、アメリカとカナダ)の要求に適合するために認証を取得したものである。国内での第三者評価の認知が限定的であるため、海外で開発・製造された製品が日本の国内市場を意識して FIPS140 の認証を取得したというケースはインタビューやアンケートの範囲では見当たらなかった。また、国内で開発・製造されている製品で FIPS140 の認証を取得しているケースはなく、一部の国内調達に対応するために、自己検証によって「FIPS140 相当」を表示するにとどまっている。

b. 国内暗号モジュール評価・認証制度のニーズ

インタビューでは、国内の暗号モジュール評価・認証制度の創設を積極的に求める意見は少なく、反対に消極的な意見すらある。その理由としては、暗号モジュール製品市場において認証の有無が製品の重要な評価要因となっていないことと、認証取得が課された場合の開発コストの増大がある。

例えば、既に高い市場占有率を持っている暗号モジュール製品販売窓口では、デファクトスタンダードないしはブランドの信頼性が需要サイドにおける暗号モジュール製品の選択の基準と考えており、認証の有無は重要でないと考えている。また、別の暗号モジュール製品販売窓口からは、「お墨付き」がつくことによる営業的なメリットを期待する反面、認証制度が創設され認知されることによって、コストをかけて認証を取得しなければならない状況になることを危惧する意見があった。

これらを踏まえると、現時点において、暗号モジュール製品の販売窓口の間で、暗号モジュールの第三者評価に関するニーズが顕在化しているとは言い難い。また、将来を見据えた場合でも、第三者評価やそれを前提とした国内の認証制度の創設を積極的に求める傾向は見られない。ただし、政府調達に対応して「FIPS140 相当」の表示を行っている現状を見ると、今後、政府調達を始めとする国内調達が第三者評価に基づく認証取得を要求するようになれば、認証の取得に動く可能性は十分に考えられる。

c. 暗号モジュール評価・認証制度への対応意向

暗号モジュール製品の販売窓口に対するアンケート調査において、販売窓口に対して取扱製品ごとに、国内に暗号モジュール評価・認証制度が創設された際に当該製品について認証を取得させる意思があるか尋ねた。

その結果は、ほとんどの製品について「制度の内容に依存する」という回答であり、「取得しない」と回答している製品は既に FIPS140 の認定を取得しているものだけであった。一方、条件をつけずに「取得する」と回答している製品には、FIPS140 の取得を予定している国産製品と海外で FIPS140 を取得済みの輸入製品が含まれている。

表 4.1 国内の暗号モジュール評価・認証制度が創設された場合の取得意思 (N=56)

選択肢	認証を取得する意思があるか	製品数
1	はい	6
2	いいえ	3
3	制度の内容に依存する	47

販売窓口が認証取得の意思があると回答した製品について、その取得において期待する効果を質問した。回答は「同種の製品との差別化」、「政府調達における有利な扱い」、「民間調達における有利な扱い」、「販売における機能・性能の説明のしやすさ」に満遍なく散らばっている。また、この中で最も重視する事柄についても、それぞれに散らばっている。なお、認証取得の意思があるという回答が少なかったため、定量的な傾向を明らかにすることはできなかった。

また、販売窓口が認証取得の意思がないと回答した製品についてその理由を質問した。回答は、「認証を必要としていない」、「認証を必要とする販売先を想定していない」、「(販売窓口としては)開発側で対応する問題と考えている」が選ばれている。なお、この質問についても、認証取得の意思がないという回答が少なかったため、定量的な傾向を明らかにすることはできなかった。

表 4.2 認証取得において期待する効果 (N=6)

選択肢	認証を受けることによってどのような効果を得ること期待しているか	製品数	優先度					回答なし
			1	2	3	4	5	
1	同種の製品との差別化	5	2	0	2	0	0	1
2	政府調達における有利な扱い	4	1	2	0	0	0	1
3	民間調達における有利な扱い	4	1	1	2	0	0	0
4	販売における機能・性能の説明のしやすさ	4	1	1	0	2	0	0
5	その他	0	0	0	0	0	0	0

表 4.3 認証を取得するつもりがない理由(複数選択、N=3)

選択肢	認証を受けるつもりがない理由	製品数
1	認証を必要としていない	1
2	認証を必要とする販売先を想定していない	2
3	後続製品で対応する	0
4	開発側で対応する問題と考えている	1
5	その他(具体的に)	0

d. 暗号モジュール評価・認証制度への対応の条件

暗号モジュール製品の販売窓口に対するアンケート調査では、「制度の内容に依存する」という回答について、さらに認証を取得するための条件を質問した。その回答として多かったものは、「認証が政府調達要件になる」と「認証が民間調達の製品選択の指標として普及する」の2つである。このことから、国内の暗号モジュール評価・認証制度に対応するか否かの判断の基準を、需要側の評価・認証制度に対する動向に置く傾向が強いことが窺える。このことは、インタビューで広範に利用される制度となることを求める声や、認証取得が政府調達要件になった場合には、取得への対応に向けて動く可能性が示唆として得られたことと整合した結果といえる。

表 4.4 認証を取得しようとする条件(複数選択、N=45)

選択肢	認証を受ける条件とその優先度	製品数	優先度1	優先度2	優先度3	優先度4	優先度5	回答なし
1	認証取得に要する適切な費用	8	0	5	0	1	0	2
2	短い評価期間	6	0	0	4	0	1	1
3	認証が政府調達の要件になる	33	13	14	3	0	0	3
4	認証が民間調達の製品選択の指標として普及する	39	24	11	0	2	0	2
5	相互認証により海外の認証取得が容易になる	8	0	1	7	0	0	0
6	その他(普及度と要する費用の兼ねあい)	2	0	0	0	0	0	2
6	その他(中立性)	3	3	0	0	0	0	0

これらを踏まえると、暗号モジュール製品の販売窓口が自社取扱製品について認証の取得に向けた対応をとるための条件は、需要側から取得を促す力が働く環境が整うことにある。すなわち、第三者評価の実施や認証の取得によって販売面で有利な扱いを受ける状況になること、あるいは、それによって初めて調達に参加できるようになるケースが出てくること、評価・認証制度に対応する条件と考えられる。

この結論から、国内で流通する暗号モジュール製品が暗号モジュール評価・認証制度に対応するよう促す上で重要になるのは、制度のプロモーションの仕方であると考えられる。そして、そのプロモーションも、暗号モジュール製品の開発元や販売窓口を対象とするものよりも、暗号モジュール製品やそれを組み込んだ暗号関連製品を調達するユーザ側を対象とする方が効果的であることが見えてくる。

(2) 評価・認証制度の国際相互承認の必要性に関する認識

輸入した海外製品を取り扱う販売窓口、国内で開発された製品を取り扱う販売窓口のいずれも、海外評価・認証制度との相互承認の必要性を指摘している。インタビューにおいて、積極的に、国内に閉じた評価・認証制度を支持する意見はなかった。

輸入した海外製品取り扱う販売窓口と国内で開発された製品を取り扱う販売窓口では、相互承認の必要性に関する指摘の意図は、もちろん異なっている。前者の場合、米国やカナダで取得した FIPS140 の認証がそのまま日本国内でも通用することを希望して、相互承認を求めている。一方、後者の場合、国内で認証を受けた製品の海外での販売拡大に繋がることを期待して相互承認を求めている。ただし、これらいずれの意図も、取得しやすい国で認証を取得し、相互承認によってその認証をそのまま他国での営業・販売において利用できるようになることを望んでいるという点では共通している。

なお、暗号モジュール製品の販売窓口および CRYPTREC 評価委員会メンバーに対するインタビューでの国内で開発された暗号モジュール製品に与える相互承認の影響に関する見通しは、どちらかというとな否定的である。具体的には、国内市場については、相互承認によって海外と国内の評価・認証制度が区別なくなると、既に FIPS140 を取得しグローバルに普及している海外製品がさらに有利になる可能性があることが指摘されている。また、国内で開発された製品の輸出に関しては、現在、積極的な外販を行っている暗号モジュール製品メーカーが国内にほとんどないため、今後、認証を取得しても海外で営業的に成功する製品が現れる可能性はあまり高くないことが指摘されている。

(3) 国内暗号モジュール評価・認証制度に関する意向・要望

国内の暗号モジュール評価・認証制度が創設されることを仮定した場合に、暗号モジュール販売窓口が制度に望むこととして、「政府調達以外への評価・認証の普及」、「国内製品の海外展開の契機となる評価・認証」を挙げることができる。

これらはいずれも、認証を取得することによっての営業・販売面でのメリットが得られる範囲の広さを確保することを念頭に置いた要望である。ここには、認証を取得した製品をより多く販売することにより、認証取得に掛かる費用を広く薄く配賦し、製品価格への影響をできる限り抑えたいという意図が現れている。

a. 政府調達以外への評価・認証の普及

国内で暗号モジュール製品の開発も行っている販売窓口では、政府調達のためだけの認証取得、あるいは特定の顧客のためだけの認証取得に止まるようだと費用負担が重いと考えている。そのため、制度を創設するのであれば、より広範な暗号関連製品の調達において利用される制度となって、取得のためのコスト負担を希釈できるようになることを期待する声強い。

なお、暗号モジュール製品の販売窓口では、認証取得に要する費用を考慮すると、要求される製品の範囲は高いレベルのセキュリティが必要な用途に限られると想定している。いずれの販売窓口も、暗号を利用した製品が増えていくことを予想しているが、今後、暗号を利用した製品は一般に広く行き渡るような低価格のプラットフォームが中心と考えられている。今後、認証取得を要求される製品の範囲が広がる場合でも、そうした単価の安い製品にまで広がることは好ましくないと考えている。

b. 国内製品の海外展開の契機となる評価・認証

前述のように、インタビューでは、海外の制度との相互承認を求める意見が主流であった。相互承認によって、既に FIPS140 の認証を取得している海外製品は新たに日本国内の認証を取得することになる。このことは、海外製品を取り扱う販売窓口にとっては歓迎すべきことであり、同じ企業で開発も行っている国内の販売窓口にとっては脅威であるはずだが、後者の立場の販売窓口からも相互承認のない評価・認証制度を求める声はない。

同じ企業で開発も行っている国内の販売窓口が、海外の制度との相互承認を求める理由は、国内市場の問題よりも、海外に拡販できる契機となることを期待する意識の方が強い点にある。これは、認証取得のために増加するコストを海外での拡販によって希釈しようという発想に基づくものであると考えられる。

ただし、現実には海外での拡販を阻害しているものとして、認証制度の他に暗号製品に関する輸出規制もあるという指摘もあった。国内での市販実績がない製品の輸出では、鍵長と輸出相手国によっては一般包括許可が認められず、煩雑な手続きを必要とする個別許可を申請しなければならない。この指摘は、このように手続き面での負担が大きくなる可能性がある現在の輸出規制の緩和を求めるものである。

c. 認証のための評価体制について

現在のところ、日本国内の IT セキュリティ製品評価・認証制度では、製品の評価を行う評価機関としての認定 (ASNITE 認定) を受けているのは公益性のある 2 団体だけである。しかし、暗号モジュールの評価・認証制度において評価を行う機関が公的な団体である必要があると考える販売窓口はなく、CMVP のように民間企業が評価機関となっても構わないという意見が主流であった。一部には、競合することによって、コストや評価の質の面での改善が期待できることを期待し、より多くの評価機関が名乗りをあげる環境を望む意見もあった。

組織形態以外での評価機関の資質としては、評価に当たって開示した情報の機密保持や評価する側のスキルについての言及があった。その背景には、いずれの販売窓口も、実際に国内で評価機関を立ち上げるに当たっての人材確保が容易でないと考えていること、国内で開発を行っている企業の技術者が製品の評価業務に割かれる可能性を認識していることがある。

(4) 今後の市場の動向と評価・認証制度の関連に関する認識

今後、暗号の用途が広がり、ユビキタス化の方向に向かうことは販売窓口共通の認識である。しかし、市場の拡大の方向がより単価が低いコモディティの方向と考えられており、現状、数十億円規模とそれほど大きくない暗号モジュール製品の市場が、今後、劇的に大きな市場になっていくことは期待できない。

このことは、各暗号モジュール販売窓口も認識しており、市場の範囲が広がっても、市場規模が飛躍的に大きくなると考えてはいない。このように、今後も暗号モジュール製品単体での一社あたりのビジネスボリュームを期待することはできないため、今後の暗号モジュール製品市場に参入する企業が増える可能性についても否定的な意見が多かった。

製品の形態別に見ると、OS やアプリケーションソフトウェアあるいはハードウェアへの組み込みを前提とした暗号ライブラリなどのソフトウェア製品は、既に米国の特定企業の製品が市場をほぼ独占している状態にある。その企業では、これまでプラットフォームの増加に合わせて製品の種類を増やしており、今後も新たなプラットフォームが増えるのに合わせ、製品の種類を増やしていくことが考えられる。この企業の製品と競合する製品として、フリーウェアやオープンソースが台頭してきているが、この企業以外でソフトウェア製品を単体で外販している企業は国内にはほとんどない。今後も、既に流通している製品との相互運用性やブランドの信頼感などといった販売面の制約から今後も登場する見通しは低い。

一方、耐タンパー性を備えたハードウェアとしての暗号モジュール製品は、ソフトウェア製品ほどの独占は進んでいない。また、販売窓口の市場感では、製品やブランドが淘汰されるような状況にはなく、製品の数も漸増傾向と認識されている。

4.2 評価・認証制度に関する暗号関連製品需要サイドの関心、ニーズ

(1) 暗号モジュール評価の必要性に関する認識

a. 現在の関心と対応状況

暗号関連製品とその他のソフトウェア・ハードウェア組み合わせてシステムを構築・提供する立場であるSI事業者に対して行ったインタビューでは、暗号モジュールの第三者評価や認証制度には一定の関心を示している。しかし、実際には、システムの中で使用する暗号モジュール製品について、第三者評価や認証の取得を求められることはほとんどないというのが現状である。また、顧客との間で暗号アルゴリズムの実装の安全性が話題に上ることも、電子政府関連の調達以外ではほとんどないようである。

暗号モジュールの評価・認証に関して一定の関心を示しているものの、SI事業者の関心はシステム全体としてのセキュリティを実現することに関する関心の方が強い。また、顧客に対する訴求点もシステム全体として実現しているセキュリティであると考えており、システムのコンポーネントである暗号モジュールの評価・認証によって顧客に価値をアピールする意向は強くない。

b. 暗号モジュール評価・認証制度のニーズ

暗号モジュール製品を選定・調達する立場として、SI事業者は暗号が実装された製品の暗号の安全性を評価することの困難さを認識しており、独自にそれを行うことは不可能と考えている。そのため、評価・認証制度が設立され、認証の取得という形で暗号の実装の安全性が表示されるようになることは必要であるという意見が聞かれた。しかし、顧客に提供するシステムで使用する暗号関連製品の選定において、FISP140 認証取得製品や自己評価を行っている製品を優先するポリシーを持っているSI事業者は、今回のインタビュー対象の中にはなかった。

こうしたことや前述の対応の現状を踏まえると、SI事業者では、暗号モジュール評価・認証制度の制定を必要と考えてはいるものの、現状、制度がなくても暗号モジュール製品の選定や顧客向けの

対応において、それほど困っていない。そのため、実態としては、SI 事業者はいま差し迫った必要性を感じていないと推測できる。

c. 暗号モジュール評価・認証制度への対応の条件

現状では、暗号モジュール評価・認証制度の必要性を感じているものの、既に国内で入手可能である FIPS140 認定製品を優先的に選定するなどの対応は特になされていない。また、今後も、提供するシステム全体としてのセキュリティの実現に関心が向いている限り、SI 事業者が積極的に暗号モジュール評価・認証制度に着目して製品選定における対応を変えていくとは考えにくい。そのため、SI 事業者が暗号モジュール評価・認証制度を意識して製品の選定・採用を行うようになるための条件として、彼らの顧客であるエンドユーザの意識の変化と提供を受けるシステム要件への反映が重要と考えられる。

(2) 評価・認証制度の国際相互承認の必要性に関する認識

既に海外に FIPS140 に基づく認証制度があり、それを取得している製品が供給されている事実を踏まえ、敢えて国内に閉じた認証制度を創設するよりも、国際的な相互承認が行われることが望ましいという意見があった。ただし、SI 事業者としての営業上、国内の暗号モジュール評価・認証制度と海外の同種の制度との相互承認が必要であるという意見は聞かれなかった。

(3) 国内暗号モジュール評価・認証制度に関する意向・要望

既にカナダで FIPS140 の認証を取得した製品を取り扱っている事業者からは、エンドユーザの混乱を避けるために、FIPS140 と同様の国内制度の早急な立上げを望む声があった。また、自社で開発した暗号関連製品を提供している小規模の SI 事業者からは、小規模の企業でも負担可能な費用で認証を取得できるようにすることと、認証を取得しない製品の販売に制限・制約を課すような制度にならないことを希望する意見があった。

製品の評価の体制については、インタビューの中で、大手の SI 事業者から、公的機関が中立性を担保するならば評価を民間企業が行うことは問題ないという意見があった。

(4) 今後の市場の動向と評価・認証制度の関連に関する認識

a. リリースされる製品の増減および取扱製品の増減

SI 業者が対象に多く含まれている暗号モジュール製品以外の暗号関連製品の販売窓口を対象に行ったアンケート調査では、今後 5 年間で自社が取り扱う製品の増減に関して「増やす」という回答が最も多い。「増やす」以外の回答は、すべて現状維持を想定しているという回答(アンケートでの回答は「変わらない」)であり、取り扱う暗号関連製品を減らすことを想定していると回答した販売窓口はない。(図 4.1)

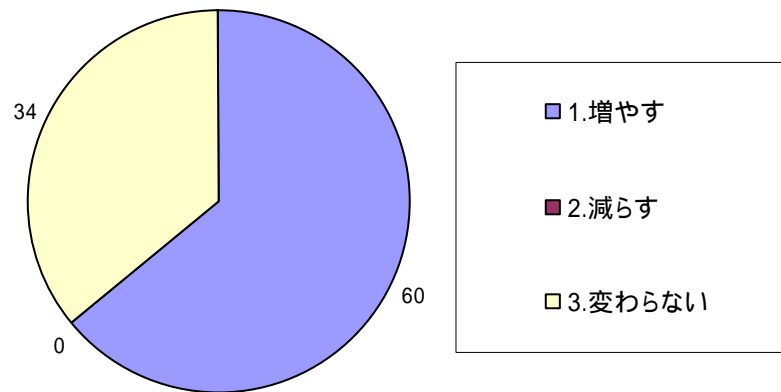


図 4.1 今後5年間における自社取扱の暗号関連製品の増減に関する想定 (N=94)

取扱製品を増やす理由としては、開発各社からリリースされる製品の種類の増加に合わせて取り扱う製品を追加する場合と、販売窓口の事業戦略として取り扱う製品の範囲を広げていく場合がある。アンケート調査ではこれら両方の理由が拮抗しており、このことから、市場にリリースされる暗号関連製品の種類が今後も増えていくという見方がSI事業者にはあり、また、積極的に取扱製品を増やすトレンドにあることが窺える。(図 4.2)

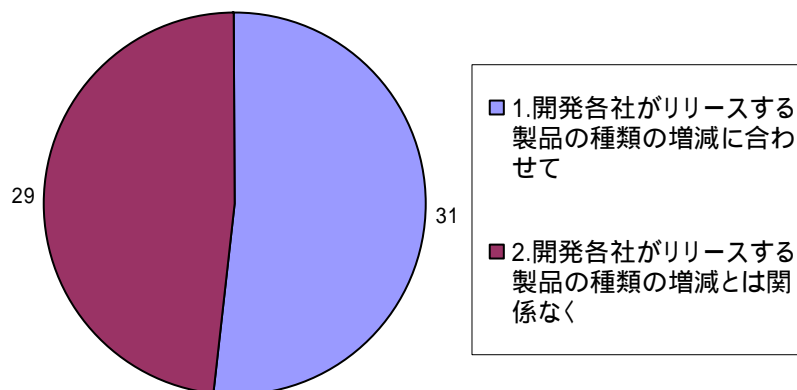


図 4.2 今後5年間における自社取扱の暗号関連製品を増やす理由 (N=60)

SI事業者に対して実施したインタビュー調査でも、このアンケート結果同様、今後もリリースされる製品の増加・取扱製品数の拡大を想定が聞かれた。ただし、マーケットでの「勝ち組」がはっきりしてきており、今後は減る可能性があるという意見もSI事業者に対するインタビューの中ではあった。

b. 暗号関連製品に搭載される暗号モジュールの動向

前述のように、暗号モジュール製品以外の暗号関連製品の販売窓口に対するアンケート調査では、暗号関連製品に搭載可能な暗号モジュールについて、種類が増えると想定している回答者が大半を占めている(図 4.3)。なお、増える理由としては、暗号関連製品を開発する各社が搭載可能なモジュールを増やすからと回答した販売窓口が 30 社、インターフェースが共通化されて組み合わせの自由度が増すからと回答した販売窓口が 20 社、その他が 3 社であった。

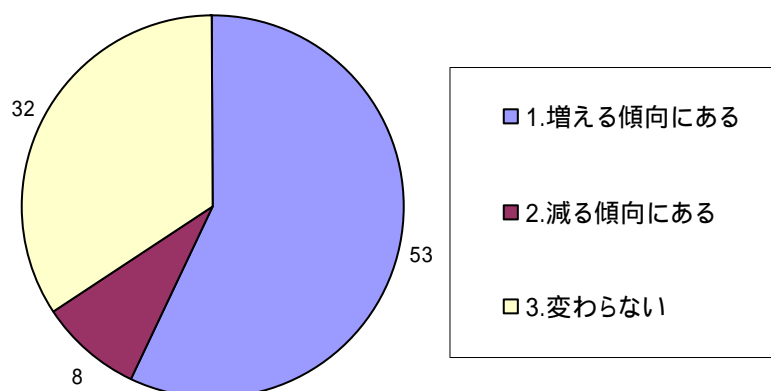


図 4.3 自社取扱の製品に搭載可能な暗号モジュールの種類を増減に関する想定(N=93) (再掲)

SI 事業者に対するインタビュー調査では、自社製品持つ SI 事業者は自社製品を組み込む傾向が強いという指摘があった。また、関連性のある複数の暗号モジュール製品を含む暗号関連製品を一連のシリーズとして提供している製品ベンダーが珍しくないため、自社製品を持たない SI 事業者でも、同一のベンダーの製品をそろえる傾向が少なからずあると考えられる。

こうした傾向が続く限り、今後も複数のベンダーの製品を組み合わせた製品やシステムの構築が行われる可能性は低いと考えられる。そして、暗号モジュール製品の増え方も、新しいベンダーから新しい製品が出ることによって増えるよりも、既存のベンダーが製品のラインアップを拡充することによって増える形が中心になると考えられる。

4.3 評価・認証制度に関する制度運営サイドの見解と意向

(1) IT セキュリティ評価認定制度の現状から見る国内暗号モジュール評価・認証の意義

a. 海外での認証取得と比較しての負担の軽減

暗号モジュール評価・認証制度に類似した先行例というべき、現在、ISO15408 に基づく IT セキュリティ製品の国内の評価・認証制度が 2001 年 4 月から運用されている。IT セキュリティ製品の評価・認証制度は海外でも既に立ち上がっており、そうした制度と日本の認証との相互承認の準備も進め

られている。そうした現状を踏まえると、評価や認証の申請の獲得において、海外との競合が発生する可能性が考えられる。

しかし、現実には、国内をベースに開発された製品にとって、国内で評価を受け認証を取得する方が海外で行うよりも有利であるため、国内製品の評価や認証が海外で行われる可能性は低いと評価機関では考えている。国内で評価を受けて認証を取得するメリットとしては、認証取得までに必要となるドキュメント作成などにおいて言語の問題に煩わされないこと、時差による連絡の時間的なロスが避けられることを挙げている。

こうした IT セキュリティ製品評価・認証制度の現状を基に考えると、国内の暗号モジュール評価・認証制度の創設によって、国内をベースに開発を行っている暗号モジュール製品は認証を取得しやすくなることが期待できる。現在は、暗号モジュールの認証を取得するためには、CMVP などの海外の制度を利用せざるを得ず、そのために開発ドキュメントから申請書類に至るまで英語で作成する必要がある。そうした負担が障害となって、認証の取得に二の足を踏んでいる開発者や販売窓口にとって、国内での暗号モジュール評価・認証制度の創設は、認証取得を具体的に検討する契機となることが期待できる。

b. 相互承認による海外市場への展開の可能性拡大

現在、ISO/IEC15408 に基づく認証制度の国際的な相互承認スキームである CCRA (Common Criteria Recognition Arrangement) への参加申請が現在進められており、2003 年春から夏の間に参加することが予定されている。このスキームへの参加によって、国内の IT セキュリティ製品評価・認証制度と海外の制度との間の相互承認が実現することになる。

IT セキュリティ製品評価・認証制度では、海外の制度との相互承認は、輸出を想定している国内製品に ISO/IEC15408 に基づく認証を要求する海外調達に参加できるメリットをもたらすことが指摘されている。しかし同時に、相互承認によって、海外の認証を取得した製品が認証を要求する国内調達に参加できるようになる可能性も考えられる。この点については、電子政府の実現において海外製品の利用が不可欠になっている反面、日本向けにローカライズされる海外製品がそれほど多くないため、相互承認が行われても現状とそれほど変わらないという意見があった。

現在、国内では、既にいくつもの FIPS140 を取得した海外の暗号モジュール製品が販売されており、一方、国内で開発された暗号モジュール製品はほとんど輸出されていない。それを踏まえ、IT セキュリティ製品評価・認証制度での指摘を暗号モジュールに当てはめて考えると、国内製品の輸出に関しては IT セキュリティ評価・認証制度での指摘と同様に考えることができる。つまり、国内で開発されている暗号モジュール製品にとって、国内での暗号モジュール評価・認証制度の設立と海外の制度との相互承認の実現は海外展開におけるハンディの一つを解消する効果を期待できる。

(2) 暗号モジュール評価・認証制度における評価機関立ち上がりの条件

a. 評価のビジネスとしての成立に十分な市場規模

日本の IT セキュリティ製品評価・認証制度や海外の ISO/ISC15408 に基づく認証制度では、認証を交付する認証機関とは独立した評価機関が製品の評価を行う形態をとっている。この形態は、アメリカとカナダにおける暗号モジュール評価・認証制度 CMVP でも同様である。

通常、評価機関は民間法人であり、対価を得て行う事業として評価を行っている。そのため、製品の評価がビジネスとして成立することが、評価・認証制度の下で評価機関が立ち上がることの重要な条件となる。そして、民間法人のビジネスとして評価事業が成立するためには、ある程度の市場規模がなければならない。IT セキュリティ製品あるいは暗号モジュール製品の評価をビジネスとして見る場合、市場の規模を測る基本的な尺度は評価依頼の件数、あるいは評価の対象となる製品数である。評価機関に対するインタビューでも、暗号モジュール評価・認証制度の創設を仮定した場合に、その評価機関になることを検討する要素として、期待できる評価依頼の件数が挙げられている。

日本の IT セキュリティ製品評価・認証制度の下での認証製品は、2002 年 12 月末の時点で 2 製品しかなく、セキュリティターゲット(ST)確認製品を加えても 3 製品にとどまっている。また、現在、国内の各評価機関で評価中の製品について公表されている数値はないが、評価機関に対するインタビューなどから、ST 確認を目的とするものを含めて 10 製品を超える程度であると考えられる。この件数は、評価中であることを公表しているものだけでも 30 製品ある³米国の認証制度と比較すると少ない。また、国内にある評価機関は認定評価機関が 2 団体、その他の評価機関が 7 団体であることを踏まえると、評価を実施中の製品数が一桁である評価機関もあることが推測できる。

こうした IT セキュリティ製品評価・認証制度の下での評価機関の利用件数に関する問題は、暗号モジュール評価・認証制度が創設する場合にも通じる問題である。IT セキュリティ製品評価・認証制度における評価の件数が米国と比べて少ない理由として、国内の制度が創設されて間もないことや、対象となる IT セキュリティ製品の製品数の違いが挙げられているが、これらはそのまま暗号モジュールにも当てはまる。また、インタビューでは第三者評価に関するユーザサイドの認知・関心が高まっていないことを理由として挙げる評価機関もあったが、これについても、暗号モジュール製品販売窓口のインタビュー結果を見る限りそのまま暗号モジュールにも当てはまることである。

b. 評価を行う人材の確保

既に始動している日本国内の IT セキュリティ製品評価・認証制度であるが、各評価機関では製品の評価を行う人材の確保に苦労している。一部の評価機関では、対象となる製品の開発を行っている企業から人材を出向で受け入れ、評価の実務を実施しているという実態もある。こうした背景としては、IT セキュリティ製品に関わる人材層と製品の評価に関するノウハウを持った人材層の薄さがあることがインタビューで指摘されている。

³ 2003 年 2 月 14 日の時点で、米国 National Institute of Standards and Technology (NIST) の Common Criteria Evaluation and Validation Scheme (CCEVS) の Web サイトに「Products and protection profiles in evaluation」として公表されている製品の数。この Web サイトにこのような形で情報を公表するか否かは評価を依頼するスポンサーが選択できるようになっている。

こうした状況を踏まえて暗号モジュール評価・認証制度に目を転じると、暗号関連製品に関わる人材層は IT セキュリティ製品に関わる人材層よりも薄いと考えられる。そのため、現状をベースにして考えると、IT セキュリティ製品評価・認証制度以上に人材難が深刻になることが予想できる。そのため、それぞれの機関が暗号モジュールの評価を行うことができる人材を確保できることも、実際に国内で暗号モジュール評価・認証制度の下に評価機関が立ち上がるための条件となる。

(3) 暗号モジュール評価・認証制度の海外相互承認の実現性

国内の暗号モジュールの販売窓口は海外相互承認に肯定的であり、また IT セキュリティ製品評価・認証制度を見る限り国際相互承認が評価機関の評価に対して新たな制約を課す可能性も低い。そのため、暗号モジュールの認証を申請する側と評価する側の意向によって、国際相互承認に向けた取り組みが阻害されることは、今のところ考えにくい。

相互承認によって、国内で開発された暗号モジュール製品の海外市場へのアクセスが容易になっていくことが期待できる。しかし、国内市場に目を転じると、既に FIPS140 の認証を取得している海外からの輸入製品との競争において不利にならないように、国内で開発された製品は認証取得をいっそう強く迫られる可能性がある。そして、もしそうなった場合、国内で開発された製品が積極的に認証取得に動くことだけでなく、認証の取得を見合わせ販売もやめてしまう製品が出てくることも予想される。

国内で開発された製品の認証取得が進まない段階で相互承認が行われ、政府調達における暗号モジュール評価・認証取得の加点要素化や要件化が進むと、国内で開発された製品が国内市場から排除されることになり兼ねない。IT セキュリティ製品の場合、日本語化などのローカライズが必要になるタイプの製品が少なからずあるため、相互承認に起因するそうした可能性に対する配慮は必要と考えられていないようである。しかし、暗号モジュールはその性質上、海外の製品を日本向けにローカライズする必要があまりなく、既に多くの海外製品が国内市場に入り込んでいることを考慮する必要がある。

(4) 暗号モジュール評価・認証制度創設に向けた課題

IT セキュリティ製品評価・認証制度における評価機関のインタビューから、暗号モジュール評価・認証制度創設に向けて、どのような課題が示唆されるかを整理した。ここでは、「ユーザへの評価・認証制度の普及」、「関係するプレイヤーへに行き渡るだけの人材の確保」および「国内での暗号モジュール開発に与える影響への配慮」を課題として挙げる。

a. ユーザへの評価・認証制度の普及

CMVP のように複数の評価機関が民間ベースで立ち上がり、暗号モジュール評価・認証制度を円滑に発足させ安定的に運営するためには、評価がビジネスとして成立することが必要である。そのため条件としては、当然、十分な件数の評価依頼および認証申請を確保することが必要となる。

そのためには、十分な件数を確保するためには、暗号モジュールを組み込んだシステムのユーザである官公庁や民間企業などへの認知・普及が課題になる。暗号モジュール販売窓口に対するアンケートおよびインタビュー調査の結果からわかるように、評価を依頼しうる販売窓口(あるいは開発

者)が認証取得に動くための主たる要因は需要サイドの動向にある。従って、暗号モジュールやそれを組み込んだシステムを提供する側に対する啓発によって、評価の依頼・認証の取得が広がる可能性は低い。やはり、コストをかけて評価と認証申請を行う以上、それに見合う営業上のメリット(あるいはデメリット)によって販売窓口や開発者の意欲を高めることが、評価ビジネスの成立という点からも必要である。

具体的な普及策として、現在、進んでいる政府調達での暗号モジュール評価・認証取得の加点要素化・要件化を更に推進することは不可欠である。また、さらに民間への広がりを生むために、システム構築の際に使用する暗号モジュールの選定において認証取得製品を優先することを促す指針等を作成・公表するといった取り組みも必要である。

b. 関係するプレイヤーに行き渡るだけの人材の育成

前述のように、現状のまま暗号モジュール評価・認証制度を創設した場合、評価に携わる人材が不足し、制度が円滑に機能しない状態に陥る恐れがある。また、評価機関だけでなく、認証機関や認証対象の製品を開発する企業においても、制度に対応した取り組みを行う人材の確保に苦慮することになると考えられる。

そうした事態にならないために、制度の創設までに、暗号モジュールの評価・認証に関する知識とスキルを身に付けた人材の育成が課題となる。この人材の育成では、育成対象とする人材像と人数を絞り込んだ少数精鋭の育成を指向するのではなく、暗号モジュールの評価・認証制度を支える人材層の拡充を図ることを志向することが望ましい。ある程度の人材の流動性が生まれるくらいに層が厚くならなければ、育成した人材が認証機関・評価機関・評価・認証を受ける企業のそれぞれに行き渡らず、評価・認証制度全体としての機能を阻害することにもなりかねない。

c. 国内での暗号モジュール開発に与える影響への配慮

政府や民間企業などへの暗号モジュール評価・認証の普及が進んでも、日本国内の評価・認証を受ける暗号モジュールが少ないと、日本での評価ビジネスとしての成立は困難になる。ドキュメンテーションの言語の問題などがあるため、日本で認証を取得しようとする製品は、日本国内に開発のベースを置いている製品にほぼ限られる。そのため、海外で開発された暗号モジュールに国内の市場が席卷されてしまうようなことがあると、国内での暗号モジュールの評価ビジネスの成立が危うくなる。

そうした危惧を現実にしないうえにも、官民の調達における暗号モジュール評価・認証への対応の進捗を意識して、国内の評価・認証制度の創設とその取得に向けた国内の開発元や販売窓口の対応を進めることが課題となる。国内で開発された暗号モジュールの認証取得が進まない状況の下での国内の官民の調達における認証取得の要件化は、既に FIPS140 認証を取得している海外製品に有利に働く。国内の暗号モジュール開発を縮小させる可能性があるそのような状況を生まないためにも、政府や民間企業への暗号モジュール評価・認証の普及スピードに合わせて、制度創設に向けた取り組みを進捗させることが必要である。

(5) 国内の暗号モジュール評価・認証制度に求められる要件

a. 先行する他の評価制度との関係

既に日本国内では、情報セキュリティに関連する評価・認証制度として、IT セキュリティ製品評価・認証制度の他に、情報セキュリティマネジメント適合性評価制度 (ISMS) も運用されている。暗号モジュール評価・認証制度が創設された場合、情報システムのユーザやシステムの構築を行う SI 事業者は、先行するこれらの制度との関連を意識しながら対応することになると考えられる。

そのため、暗号モジュール評価・認証制度と先行する他制度との間に、運営体制に関する基本的な枠組みや制度・基準の仕組みに関する乖離が生じることは好ましくない。これらの評価・認証制度が統一感ある一連の制度となるよう関係を整理し、情報システムのセキュリティを実現する場面で生かされるような配慮が望ましい。そのためには、これらの制度の棲み分けを明確化することや、制度やベースとなる基準の改訂の同期を図ることにより制度相互の関連性を担保することが、配慮として必要である。

さらに進んだ取り組みとして、これらの認証のいずれかを取得することによって、他の認証の取得における手続きや審査を簡略化するという形での制度間の連携が、認証取得を希望する側から要望される可能性はある。これが実現すると、認証取得しようとする側にとっての費用負担の軽減が期待でき、認証取得までの期間の短縮も期待できる。そのため、評価・認証制度の普及および認証取得製品の拡大という観点だけで考えると、検討に値することと考えられる。

ただし、それを実施した場合、制度の運用の負担が大きくなるため好ましくないという意見が評価機関からあった。また、簡略化の審査によって、海外の同種の制度との認証要件の差異が生じる可能性がないかについても精査する必要がある。そのため、こうした連携の実施に当たっては、制度普及以外の側面について十分な検討を踏まえた上で実施べきであろう。

b. 制度の運営体制

現在の日本の IT セキュリティ製品評価・認証制度では、ASNITE 認証を取得している評価機関は情報機器メーカーが共同で設立した公的な位置付けを持つ 2 つの機関だけである。ただし、この他に、ST の評価を実施できる評価者がいる評価機関が 7 機関ある。これら 7 機関はいずれも民間の企業・団体であり、セキュリティ製品を開発・製造を行っている民間企業やセキュリティ製品を使用したシステムを構築し顧客に納入している民間企業も含まれている。

このように、評価対象の製品を開発・製造する企業や評価対象の製品の販売窓口に類する企業が評価機関となる例は、海外 IT セキュリティ製品評価・認証制度でもある。また、FIPS140 の評価・認証でも、暗号モジュールの開発・製造・販売を行っている企業が評価機関に名を連ねている。このことを懸念する声はなく、そうした企業を含めた多くの選択肢ができることが望ましいという意見が評価機関の中にもある。

国内の暗号モジュール評価・認証制度の運営体制でも、こうした先行する制度に倣い、評価機関について評価能力以外の適格要件の設定を避け、間口を広く開けておくべきであると考えられる。そうすることにより、IT セキュリティ評価・認証制度との類似性から、認証の仕組みに関する一般の理

解が進みやすくなることが期待できる。また、FIPS140 と類似した仕組みになることにより、国際相互承認もスムーズに進められることが期待できる。

4.4 評価・認証制度の需要規模予測

(1) 算出の前提および考慮すべき要因

a. 国内の評価・認証制度の対象となる製品の範囲

これまでの分析の結果を踏まえ、今後5年間(2002年度から2007年度まで)の間に国内の暗号モジュール評価・認証制度の対象となる製品数、および評価・認証の申請件数を予測する。なお、この予測は需要として考える範囲全体の規模予測であり、その範囲にある製品が想定するサイクルで必ず申請を行うことを前提にして件数を求める。そのため、実際に評価・認証の申請の件数は、歩留りを考えて何らかの係数を乗じて求める必要がある。

予測に当たって、国内の暗号モジュール評価・認証制度の対象製品(以下、「評価・認証対象製品」という)としてカウントする製品の種別の範囲を以下のように設定した。

【評価・認証対象製品を抽出する種別の範囲】

- この調査で定義している「暗号モジュール製品」すべて
- この調査で定義している「暗号モジュール製品以外の暗号関連製品」のうち、証明書発行・管理用サーバソフトウェアとVPNゲートウェイソフトウェア

後者を対象に含めた理由は、この種の製品にFIPS140の認定を受けている製品が存在していることによる。

ただし、国内で入手可能な暗号モジュール製品のうち、これまでのアンケート結果およびインタビュー結果を踏まえた分析から、以下の条件に合致する製品は評価・認証対象製品とはならないものと想定する。

【評価・認証対象製品に含めない製品】

- 開発元が海外の企業である製品
開発のベースが海外にあると考えられ、販売先も日本だけではない製品と考えられる。そうした製品が、取って日本で認証を取得する可能性は低い。
- 国内の暗号モジュール評価・認証について「取得しない」と回答している製品

b. 現時点での潜在需要規模

まず、現時点で実際に評価・認証を申請しうる製品数の予測では、評価・認証対象製品のうち、政府調達における暗号モジュール評価・認証取得の加点要素化や要件化の動きに反応しうる製品に

着目する。そして、アンケート調査において以下の条件に適合する回答があった製品が、評価・認証を取得しうるものと想定する。

【製品群 - 評価・認証を取得しうる製品】

- 国内の暗号モジュール評価・認証を取得する意思がある暗号モジュール製品
アンケート調査では「国内の評価認証を取得する意思があるか」の問いに対し「はい」と回答している製品が対象
- 政府調達の要件になるならば、国内の暗号モジュール評価・認証を取得すると意向を持つ暗号モジュール製品
アンケート調査では「認証が政府調達の要件になる」を評価・認証取得の最優先の条件あるいは2番目の条件とした製品が対象
- 評価・認証対象製品のうち、証明書発行・管理用サーバソフトウェアとVPNゲートウェイソフトウェア
国内の評価・認証取得の意向や条件を尋ねる設問がないため、予測では便宜上、今回の調査で確認された同種の海外製品におけるFIPS140取得率(48製品中19製品 = 39.6%)を乗じた製品数を用いる

なお、上記3項目に合致するもののうち、既にFIPS140を取得している製品およびその取得予定が具体化している製品は除外する。

アンケート調査で回答のあった製品から、評価・認証対象製品の条件に合致するものを抽出し、現時点で評価・認証を申請しうる製品数を求め、表4.5に示した。表中、ハードウェアで評価・認証を申請しうるものとして抽出された製品は、大手印刷会社が開発元の手電機メーカー仕様のICカードである。また、ソフトウェア・ライブラリで評価・認証を申請しうるものとして抽出された製品のうち、5製品は大手電機メーカーが開発元の暗号ライブラリ製品である。なお、アンケートで確認した評価・認証対象製品である「VPNゲートウェイ、証明書発行・管理サーバ等」の11製品のうち、9製品までが大手電機メーカーまたはその関連企業が開発した製品である。

このように、アンケート調査で確認した評価・認証対象製品のうち14.4製品が、仮に現時点で国内の暗号モジュール評価・認証制度が創設された場合に評価・認証を申請する可能性がある製品数ということになる。なお、取得する認証のレベルは、既にFIPS140を取得している同種の製品もとに、「ハードウェア」はレベル2または3、「ソフトウェア・ライブラリ」はレベル1、「VPNゲートウェイ、証明書発行・管理サーバ」はレベル2または3と予測した。

表 4.5 現時点で評価・認証を申請しうる製品数

	アンケート調査で確認した評価・認証対象製品	うち、現時点で評価・認証を申請しうる製品 (製品群)	予測される取得レベル
暗号モジュール製品			
ハードウェア (IC カードを含む)	6 製品	1 製品	レベル 2,3
ソフトウェア・ライブラリ	18 製品	9 製品	レベル 1
暗号モジュール製品以外の暗号関連製品			
VPN ゲートウェイ 証明書発行・管理サーバ	11 製品	4.4 製品	レベル 2,3

現時点で制度が制定された当初に申請しうる製品と想定しているため、ここでは申請の件数は製品数と等しい 14 件と予測することができる。なお、この件数は、取得費用負担の忌避や営業方針の変更などによって、申請を取り止めることまでを考慮していない。そのため、取得件数の実現値はこれよりも低い値になることを想定している。

(2) 今後 5 年間を見通した暗号モジュール評価・認証制度の潜在需要規模予測

a. 今後 5 年間の増減に関する仮説

前項で求めた現時点での評価・認証を申請しうる製品数および評価・認証申請の件数を基準値として用い、5 年後の評価・認証を申請しうる製品数および評価・認証申請の件数を予測する。なお、5 年後の予測では、以下に示す 2 つのケースを設定する。

<p>予測するケース</p> <p>【ケース 1】 政府調達において現在進んでいる暗号モジュール評価・認証の加点要素化・要件化の動きが順調に進行することを想定したケース</p> <p>【ケース 2】 5 年後までに、政府調達に加え、民間調達においても暗号モジュール評価・認証の加点要素化・要件化の動きが現れ始めることを想定したケース</p>
--

また、アンケート調査で以下の条件に合致する回答があった製品は、現時点では国内の評価・認証を取得する可能性はないが、5 年後には国内の評価・認証を取得しうる製品になっていると想定する。

【製品群 - 5年後に評価・認証を取得しうる製品 A(想定)】

- 既に FIPS140 の認証を取得している製品
既に認証を取得しているので、しばらくは改めて日本で取得する必要はない。ただし、バージョンアップやバリエーションの拡大の際に、日本での取得に切り替える可能性があるため、将来の予測においては対象の範囲に加える。
- FIPS140 の認証取得予定が具体化している製品
現在予定が具体化している FIPS140 の認証を取得した後、しばらく日本で取得する必要はない。ただし、バージョンアップやバリエーションの拡大の際に、日本での取得に切り替える可能性があるため、将来の予測においては対象の範囲に加える。

なお、ケース 2 での予測では、5 年後に評価・認証をし得しうる製品として、以下の条件を満たすものも考慮する。

【製品群 - 5年後に評価・認証を取得しうる製品 B(想定)】

- 民間調達の要件になるならば、国内の暗号モジュール評価・認証を取得すると意向を持つ暗号モジュール製品
アンケート調査では「認証が政府調達の要件になる」を評価・認証取得の最優先の条件あるいは 2 番目の条件とした製品
ただし、アンケート調査で「認証が政府調達の要件になる」を評価・認証取得の最優先の条件あるいは 2 番目の条件とした製品は含まない(すなわち、製品群とは重複しない)

5 年後の予測にあたり、今後 5 年間(2002 年度から 2007 年度まで)に評価・認証対象製品は、国内市場で販売される暗号モジュール製品の製品数の伸びに比例して増加するものと仮定する。従って、5 年後における製品群 の製品数および製品群 の製品数は、現時点での値に、国内市場で販売される暗号モジュール製品の製品数の今後 5 年間における伸び率を乗じたものになる。なお、この伸び率として、表 3.3 に示した今後 5 年間の伸び率 2.3 倍を用いる。

また、評価・認証申請件数は製品数だけでなく、製品の仕様変更やバージョンアップの発生の仕方に依存する。しかし、仕様変更やバージョンアップのサイクルは、個々の企業の戦略や市場動向、製品の特性によって様々である。事実、FIPS140 では、単一の製品が数ヶ月の間に複数回認証を取得しているケースもあれば、最初の認証取得から 7 年後に再び認証を取得しているケースもある。このように、実績から仕様変更やバージョンアップに伴う申請のサイクルに関する傾向を一般化することは困難であるため、それぞれ以下のように想定して申請件数を予測する。

【評価・認証件数の予測に当たっての想定】

- いずれの製品も 2 年のサイクルで仕様変更またはバージョンアップを実施し、既に認証を取得している製品はそのタイミングで改めて評価・認証を申請するものとする
- 現時点で評価・認証を申請しうる製品の半数は 2 年のサイクルの中間にあり、残り半数は 2 年のサイクルの切り替わりにあるものとする
- 今後 5 年間に新たに評価・認証を申請する製品は 5 年後の時点で半数が 2 年サイクルの中間にあり、残り半数はサイクルの切り替わりにあるものとする

b. 5 年後の潜在需要規模(ケース 1)

今後 5 年間の国内の暗号モジュール評価・認証の対象製品数伸びに関する仮定を用いて、5 年後の暗号モジュール評価・認証制度の潜在需要規模がどの程度増加するのかを予測する。その結果を表 4.6 に示す。

表 4.6 5 年後に発生しうる評価・認証申請の予測値(ケース 1 製品数ベース)

	現時点で評価・認証を申請しうる製品 (製品群)	現時点で FIPS140 取得済/取得予定 (製品群)	5 年後評価・認証を申請しうる製品	予測される取得レベル
暗号モジュール製品				
ハードウェア (IC カードを含む)	1 製品	1 製品	3.3 製品	レベル 2,3
ソフトウェア・ライブラリ	9 製品	1 製品	21.7 製品	レベル 1
暗号モジュール製品以外の暗号関連製品				
VPN ゲートウェイ 証明書発行・管理サーバ	4.4 製品	2 製品	12.1 製品	レベル 2,3

【5 年後に評価認証を申請しうる製品数の算出方法】

それぞれの製品区分について、以下の〔 〕と〔 〕の和を 5 年後評価・認証を申請しうる製品数とした。

〔 〕製品群 の製品数の 2.3 倍(今後 5 年間における暗号モジュール製品数の伸び率)

〔 〕製品群 の製品数

5 年後に発生しうる申請の件数は、現時点とは異なり、製品数と等しくはならない。それは、今後 5 年間、それぞれの製品が異なる時点で最初の評価・認証の取得を行い、異なるサイクルで仕様変更やバージョンアップを行うことに起因する。

前述の「評価・認証件数の予測に当たっての想定」に従うと、表 4.7 のように、5 年後における 1 年間の申請件数は 5 年後の製品数のちょうど半分である 19 件(端数は四捨五入)ということになる。

表 4.7 5年後に発生しうる評価・認証申請の予測値(ケース1 件数ベース)

	5年後の評価・認証を申請件数	予測される取得レベル
暗号モジュール製品		
ハードウェア (ICカードを含む)	2件	レベル2,3
ソフトウェア・ライブラリ	11件	レベル1
暗号モジュール製品以外の暗号関連製品		
VPN ゲートウェイ 証明書発行・管理サーバ	6件	レベル2,3

〔5年後に発生しうる評価・認証申請の件数の算出方法〕

それぞれの製品区分について、以下の式によって算出した。(端数は四捨五入)

$(5\text{年後評価・認証を申請しうる製品数}) \div \{ \text{仕様変更・バージョンアップのサイクル}(2\text{年}) \}$

c. 5年後の潜在需要規模(ケース2)

以上は、政府調達における暗号モジュール評価・認証の加点要素化や要件化のみを想定したものであったが、今度は、今後5年間で民間調達における暗号モジュール評価・認証の要件化が並行して進んだ場合を想定する。

アンケート調査で、国内の暗号モジュール評価・認証を取得する条件として「民間調達における要件化」を挙げた製品数を表4.8に示す。なお、この製品数には「政府調達における要件化」を合わせて条件としていた製品を含まない。なお、5年後、この製品数も全体の製品数の伸び率(2.3倍)に合わせて増加するものとする。

表 4.8 民間調達での要件化を評価・認証取得の条件としている製品数

	アンケート調査で 確認した評価・認証 対象製品	民間調達での 要件化が取得の 条件である製品 (製品群)	5年後における 製品群の製品数 (想定値)	予測される 取得レベル
ハードウェア (ICカードを含む)	6製品	3製品	6.9製品	レベル2,3
ソフトウェア・ライ ブラリ	18製品	3製品	6.9製品	レベル1
VPN ゲートウェイ 証明書発行・管 理サーバ	11製品	0製品	0製品	レベル2,3

〔算出方法〕

それぞれの製品区分について、製品群の製品数の2.3倍(今後5年間に於ける暗号モジュール製品数の伸び率)、した件数を5年後における製品群の製品数とした。

なお、「VPNゲートウェイ、証明書発行・管理サーバ」については、この件に関する設問がないため、便宜上、行政機関の相互接続性担保のために政府調達での要件化によって、取得意向のある製品はすべて評価・認証の申請を行うと想定した。従って、この製品区分において製品群に該当する製品はない。

今後5年間で民間調達における暗号モジュール評価・認証の要件化が進んだ場合を想定し、5年後の評価・認証を申請しうる製品数を予測した結果を表4.9に示す。また、ケース1のときと同じ想定に基づいて予測した5年後の申請件数の予測を表4.10に示す。

このように、民間調達における暗号モジュール評価・認証の要件化が進んだ場合の評価・認証申請件数は25件となり、政府調達だけを想定した件数から6件増加する。

表 4.9 5 年後に発生しうる評価・認証申請の予測値(ケース2 製品数ベース)

	現時点で評価・認証を申請しうる製品 (製品群)	現時点で FIPS140 取得済/取得予定 (製品群)	5 年後評価・認証を申請しうる製品	予測される取得レベル
暗号モジュール製品				
ハードウェア (IC カードを含む)	1 製品	1 製品	10.2 製品	レベル 2,3
ソフトウェア・ライブラリ	9 製品	1 製品	28.6 製品	レベル 1
暗号モジュール製品以外の暗号関連製品				
VPN ゲートウェイ 証明書発行・管理サーバ	4 製品	2 製品	12.1 製品	レベル 2,3

[5 年後に評価認証を申請しうる製品数の算出方法]

それぞれの製品区分について〔 〕～〔 〕の和を 5 年後評価・認証を申請しうる製品数とした。

〔 〕製品群 の製品数の 2.3 倍(今後 5 年間における暗号モジュール製品数の伸び率)

〔 〕製品群 の製品数

〔 〕5 年後における製品群 の製品数(表 4.8 参照)

表 4.10 5 年後に発生しうる評価・認証申請の予測値(ケース2 件数ベース)

	5 年後の評価・認証を申請件数	予測される取得レベル
暗号モジュール製品		
ハードウェア (IC カードを含む)	5 件	レベル 2,3
ソフトウェア・ライブラリ	14 件	レベル 1
暗号モジュール製品以外の暗号関連製品		
VPN ゲートウェイ 証明書発行・管理サーバ	6 件	レベル 2,3

[5 年後に発生しうる評価・認証申請の件数の算出方法]

それぞれの製品区分について、以下の式によって算出した。(端数は四捨五入)

$(5 \text{ 年後評価・認証を申請しうる製品数}) \div (\text{仕様変更・バージョンアップのサイクル}(2 \text{ 年}))$

d. 5 年後の潜在需要規模(ケース比較)

政府調達での要件化が進んだ場合、政府調達の要件化と民間調達への浸透が合わせて進んだ場合の 2 つのケースについて予測を行った評価・認証申請件数の予測値を取りまとめる。

製品区分別に、現時点での評価・認証申請件数とそれぞれのケースにおける 5 年後の評価・認証申請件数の予測値を表 4.11 に示す。また、それを評価・認証のレベル別に整理しなおしたものを表 4.12 に示す。なお、申請件数のレベル別の整理は、前述の製品区分別に予測した取得レベルどおりに、各製品が評価・認証を申請することを想定して行った。

表 4.11 現時点と5年後に発生しうる評価・認証申請件数の予測値(製品区分別)

	(現時点) 政府調達での要件化	5年後の1年間	
		(ケース1) 政府調達での要件化	(ケース2) 政府調達での要件化、 民間調達への浸透
暗号モジュール製品			
ハードウェア (ICカードを含む)	1件	2件	5件
ソフトウェア・ライブラリ	9件	11件	14件
暗号モジュール製品以外の暗号関連製品			
VPNゲートウェイ 証明書発行・管理サーバ	4件	6件	6件
計	14件	19件	25件

表 4.12 現時点と5年後に発生しうる評価・認証申請件数の予測値(レベル別)

	(現時点) 政府調達での要件化	5年後の1年間	
		(ケース1) 政府調達での要件化	(ケース2) 政府調達での要件化、 民間調達への浸透
レベル2,3	5件	8件	11件
レベル1	9件	11件	14件
計	14件	19件	25件

e. 評価・認証対象製品の暗号アルゴリズム

国内の暗号モジュール評価・認証制度を創設した際に評価対象の多くの製品が採用し、評価機関および認証機関における優先的な対応が必要になる暗号アルゴリズムを予測する。予測に当たっては、アンケート調査で確認できている製品について、現時点で対応済および今後対応予定の暗号アルゴリズムを調べ、その傾向が評価・認証の潜在需要の範囲に含めた製品全体に当てはまるものと仮定した。

現時点で多くの製品が対応している暗号アルゴリズムを表4.13の「現時点での対応アルゴリズム」の列に示した。これらのアルゴリズムが、いま暗号モジュール評価・認証制度を創設すると仮定した場合に、評価機関および認証機関で優先的な対応が必要な暗号アルゴリズムと考えられる。

また、多くの製品が今後対応予定としている暗号アルゴリズムを表4.13の「今後対応予定のアルゴリズム」の列に示した。これらのアルゴリズムが、今後、暗号モジュール評価・認証制度を運営していた場合に、評価機関および認証機関で対応する暗号アルゴリズムを追加する上で優先すべきと考えられる。

表 4.13 評価・認証対象製品が対応済および対応予定の主要な暗号アルゴリズム

		現時点での対応アルゴリズム 現時点で評価・認証を行う場合、 優先的な対応が必要なアルゴリズム	今後対応予定のアルゴリズム 今後、増加する評価・認証において 優先的に追加対応すべきアルゴリズム
公開鍵暗号	署名	RSASSA-PKCS-v1_5 ・ハードウェア 2製品 ・ソフトウェア・ライブラリ 6製品 ・VPN ゲートウェイ、 証明書発行・管理サーバ 6製品	RSA-PSS ・VPN ゲートウェイ、 証明書発行・管理サーバ 4製品
	守秘	RSAES-PKCS-v1_5 ・VPN ゲートウェイ、 証明書発行・管理サーバ 5製品	
共通鍵暗号	64 ビットブロック暗号	3-Key Triple DES ・ハードウェア 4製品 ・ソフトウェア・ライブラリ 5製品 ・VPN ゲートウェイ、 証明書発行・管理サーバ 7製品	
	128 ビットブロック暗号	AES ・ハードウェア 2製品 ・ソフトウェア・ライブラリ 2製品 ・VPN ゲートウェイ、 証明書発行・管理サーバ 3製品	Camellia ・ハードウェア 1製品 ・ソフトウェア・ライブラリ 3製品

表中の製品数は、アンケート調査で国内暗号モジュール評価・認証の対象として確認されている製品における対応済製品数および対応予定製品数を示す

5. 提言

暗号アルゴリズムの実装レベルでのセキュリティ評価基準に基づく暗号モジュール評価認証制度は、暗号を利用する情報システムのセキュリティ確保のためには必要不可欠である。

しかし、前述した調査結果からもわかるように、暗号モジュール評価認証制度を国内で立ち上げるためには、政府調達における要件化の推進が非常に重要な条件となる。

本章では、政府調達における要件化が行われることを前提とし、さらに本制度を国内で立上げるために必要な方策についての提言を行う。

5.1 提言の概要

(1) 評価・認証に対するニーズの顕在化

4.1 節及び 4.2 節で見たとおり、現状では、暗号モジュール製品販売窓口(ベンダー)と SI 事業者の暗号モジュール評価・認証に対する姿勢は、ユーザ側のニーズが顕在化すれば対応するという消極的なレベルに止まっている。わが国の情報セキュリティシステムを高度化するためには、こうした姿勢を転換させ、評価・認証を積極的に取得させる必要がある。評価・認証の対象が増加すれば、評価事業への参入企業・団体の増加を促すこととなり、評価制度の健全な発展を期待することができる。と考える。

このような観点から、情報システムのユーザ側の関心と行動を喚起することに焦点を当て、「情報セキュリティシステムにおける暗号モジュールの位置付けとその高信頼化のための評価・認証制度の位置付けの明確化」と「認証取得の要件化に向けた支援」を提言する。なお、これらの詳細を、それぞれ 5.2 節の(1)および(2)に示す。

(2) 制度運営体制の整備と認証取得によるインセンティブの明確化

インタビュー調査やアンケート調査の結果からもわかるように、評価スキルをもった人材の確保および育成は、暗号モジュール評価・認証制度の創設に向けた大きな課題である。また、開発も行っている暗号モジュール製品の販売窓口からは、海外展開の契機となるような相互承認の実現が要望として挙げられている。

このような観点から、以下に示す「暗号モジュール評価・認証に関わる人材の育成」、「暗号モジュール評価を受託する評価機関の立上げ促進」および「国内で開発される暗号モジュール製品の販路拡大の支援」を提言する。なお、これらの詳細を、それぞれ 5.3 節の(1)～(3)に示す。

<p>「評価・認証に対するニーズの顕在化」 (情報システムのユーザ側の関心・行動を喚起することに照準)</p> <ul style="list-style-type: none"> ・「情報セキュリティシステムにおける暗号モジュールの位置付けとその高信頼化のための評価・認証制度の位置付けの明確化」 ・「認証取得の要件化に向けた支援」 	<p>制度のプロモーションに関する提言</p>
<p>「制度運営体制の整備と認証取得によるインセンティブの明確化」 (評価スキルをもった人材の確保及び育成、制度に対する開発元・販売窓口の期待・要望への対応に照準)</p> <ul style="list-style-type: none"> ・「暗号モジュールの評価・認証に関わる人材の育成」 ・「暗号モジュール評価を受託する評価機関の立上げ支援」 ・「国内で開発される暗号モジュール製品の販路拡大の支援」 	<p>制度の仕組み・運営に関する提言</p>

図 5.1 提言の全体像

5.2 ニーズの顕在化および掘り起こしに必要と考えられる施策の提言

(1) 情報セキュリティシステムにおける暗号モジュールの位置付けとその高信頼化のための評価・認証制度の位置付けの明確化

【提言のポイント】

- ・ 情報セキュリティ全体における暗号モジュールが果たす役割の理解形成を図る
- ・ 暗号モジュールの高信頼化のための評価・認証制度の位置付けを明確化
ユーザ側に理解形成を図る
- ・ 既存の制度(IT セキュリティ製品評価・認証制度、ISMS 等)や暗号モジュール評価・認証制度を活用し、セキュアな情報システムを構築する手法をユーザ側に提示する

暗号モジュール評価・認証に関して、ユーザ側の意識・関心を高めるためには、政府調達が先導的に範を示すことが重要である。ユーザ側の認知・理解を段階的に深められるような方法で評価・認証の意義やその制度をアピールしていく必要がある。

まず、情報セキュリティ全体における暗号モジュール評価・認証制度の位置付けを明確化し、ユーザ側の理解形成を図り、次に、ユーザ側の取組みに対して、既存の制度(IT セキュリティ製品評価・認証制度、ISMS 等)や暗号モジュール評価・認証制度をどのように活用すれば、セキュアな情報システムの構築が容易となるかの手法を提示できることが望ましい。

(2) 認証取得の要件化に向けた支援

【提言のポイント】

- ・ システムの代表的な用途とそのシステムに組み込まれる暗号モジュール製品が取得しておくべき認証のセキュリティレベルの対応付けを指針にしてまとめる

情報システムなどの調達において、暗号モジュール評価・認証制度の位置付けを理解したユーザ側が、販売窓口に対して、実際に認証取得の要求をすることができるようになるためには、システムの代表的な用途とそのシステムに組み込まれる暗号モジュール製品が取得しておくべき認証のセキュリティレベルの対応付けをまとめた指針が必要である。さらに、その指針について、社会的なコンセンサスが得られていることが望ましい。

ただし、ユーザ側からの販売窓口に対する認証取得の要求が急速に増加した場合、国内の暗号モジュール開発元や販売窓口が期間的に対応しきれない可能性がある。製品間の公平な競争を担保するため、政府調達における要件化や民間への働きかけは、製品の認証取得の動向を見ながら漸進的に進めることが望ましい。

5.3 国内暗号モジュール評価・認証制度の姿

(1) 暗号モジュール評価・認証制度に関わる人材の育成

【提言のポイント】

- ・ 暗号モジュール評価・認証制度に関係するプレイヤー（開発元・評価機関・認証機関など）ごとに評価スキルを持つ人材の育成を行う
- ・ 制度創設の初期段階では公的な人材育成機関を設置して、集中的な人材育成を行い、その後、民間の育成プログラム主体の育成に移行させる

暗号モジュール評価・認証制度に関係するいずれのプレイヤー（開発元・審査機関・認証機関など）も、この制度に対応する人材を必要としている。制度を円滑に運営し、健全な発展を進める上で効果的な人材育成策を行うべきである。具体的には、プレイヤーごとに育成する人材の目標人数を設定して人材育成を実施することが考えられる。その結果、暗号モジュール製品の開発元や認証機関にも評価のスキルを持った人材が育つようになり、評価機関で育成した人材が外に流出することを抑制する効果が期待できる。さらに、評価機関の人材と共通の知識・ノウハウを持つ人材が暗号モジュール製品の開発元にも配置されることにより、評価機関とのコミュニケーションが円滑化され、評価期間を短縮できるという効果も期待できる。

制度創設の初期段階では公的な人材育成機関を設置し、認証機関となる団体/暗号モジュールの開発元・販売窓口/評価機関となりうる企業・団体から募集した人材を対象に、集中的な人材育成を行い、制度立上げに必要な人材層を形成できた時点で、民間主体の育成プログラムに移行させることが望ましい。

(2) 暗号モジュール評価を受託する評価機関立上げの促進

【提言のポイント】

- ・ 企業・団体内における既存の人材の割当てによって新規に評価事業の立上げが可能で、かつ評価事業への強い参入意思を持つ企業・団体を対象に、評価スキルを持った人材の集中的な育成を行う
- ・ コンサルティング事業の実施など、評価以外に事業として成り立たせるための工夫が必要である

人材を育成する対象となる企業・団体の選定においては、企業・団体内における既存の人材の割り当てによって、新規に評価事業を立上げることができる企業・団体であるかどうか重要なポイントである。この条件に合致する企業・団体としては、IT セキュリティ製品評価・認証制度の評価機関、ISMS の審査登録機関、セキュリティ・システムの構築やコンサルティングを行っている SI 事業者などがある。こうした条件に合致する企業・団体の中から、暗号モジュールの評価ビジネスへの参入意欲の強い企業・団体を選定し、選定した企業・団体を対象に、人材の集中的な育成をすることが評価機関の早期立上げには有効である。

また、予測した評価依頼件数を考慮すれば、評価機関の継続的な運営のためには、コンサルティング事業の実施など、評価以外に事業として成り立たせるための工夫が必要である。

(3) 国内で開発される暗号モジュール製品の販路拡大への支援

【提言のポイント】

- ・ 早期に国内の暗号モジュール評価・認証制度を創設し、認証取得製品が出揃うような環境を整える
- ・ 海外制度との相互承認を早期に実現する
- ・ 日本が国際的なデファクト・スタンダードを築き、国内で開発される暗号モジュールが優位性を獲得しうる領域におけるアプリケーション開発を支援・促進する

国内で開発される暗号モジュール製品の国内販路については、既に FIPS140 による認証を取得している海外製品との競合を考慮し、今後、拡大していく官民の暗号モジュール製品を組み込んだ製品・情報システムの調達で不利にならないことを考えなければならない。そのためには、早期に国内の暗号モジュール評価認証制度を創設し、かつ人材育成の支援や評価・認証費用の補助などにより、国内の認証取得製品が出揃うような環境を整えることが必要である。

また、国内で開発される暗号モジュール製品の海外展開については、海外製品と同等の扱いを受けられるよう、国内の暗号モジュール評価・認証制度と海外制度との相互承認の実現が望まれる。その分野に対する政策的支援としては、家庭電化製品や携帯電話などによるユビキタス・コンピューティングの領域における暗号を利用した先進的なアプリケーションの開発支援が挙げられる。海外の企業がまだ本格的に手がけていない、このような領域で、日本が国際的なデファクト・スタンダードを築くことができれば、その領域で利用される暗号モジュールについては、高い競争優位性を獲得できるはずである。