情報セキュリティ製品・システムの第三者評価・認証制度について：金融分野において利用していくために

田村裕子（たむらゆうこ）／宇根正志（うねまさし）

要　旨

近年、わが国では、インターネット等のオープンなネットワークを利用したさまざまな金融サービスが提供されるようになってきている。そうしたなか、金融機関は従来のクローズド・システムでは想定していなかった新たな脅威に対抗するため、高度な情報セキュリティ技術を情報システムに組み込んで対応してきた。その結果、金融機関の情報システムが一層複雑なものとなり、当該システムが一定のセキュリティ要件を満足しているか否かの確認が容易でなくなってきている。

こうしたなか、わが国では、JISEC やJCMVP といった情報セキュリティ製品・システムを第三者が評価・認証するという制度的な枠組みが整備されてきている。第三者による評価・認証制度を利用することは、金融機関が、複雑化している情報システムのセキュリティ対策の効果を見極めるうえで有用な手段の1つであると考えられる。ただし、これらは万全というわけではなく、制度の活用に当たってはその内容や限界を正しく認識しておく必要があろう。

本稿では、JISEC 等、コモンクライテリアに基づくセキュリティ評価・認証制度と、JCMVP 等、FIPS 140-2 に基づく暗号モジュール試験・認証制度に焦点を当てて、これらの制度が整備されてきた経緯やその内容を説明する。そのうえで、金融機関がこうした制度を活用するメリットや利用する際の留意点について考察する。

キーワード：暗号モジュール、コモンクライテリア、セキュリティ評価、第三者評価・認証制度、FIPS 140-2、JCMVP、JISEC

本稿は、2008 年 2 月 5 日に日本銀行で開催された「第 10 回情報セキュリティ・シンポジウム」への提出論文に加筆・修正を施したものである。なお、本稿に示されている意見は、筆者たち個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りは筆者たち個人に属する。

田村裕子　日本銀行金融研究所（E-mail: yuuko.tamura@boj.or.jp）
宇根正志　日本銀行金融研究所企画役（E-mail: une@imes.boj.or.jp）

1. はじめに

わが国の金融機関は、1990年代後半から、インターネット等のオープンなネットワークを利用した金融サービスの提供を本格的に開始し、現在ではさまざまな金融サービスが多様な利用環境のもとで提供されるようになっている。例えば、リテール・バンキングについては、従来からのキャッシュカード業務に加えて、デビットカード業務、クレジットカード業務、インターネット・バンキング業務等にそのサービス範囲を拡大させているほか、最近一部の金融機関では電子マネーに関連する業務も開始されている。こうした業務では、インターネット等のオープン・ネットワークや、金融機関による直接的な管理が比較的困難な小売店舗の店頭に設置された端末等が利用されており、従来のシステムでは想定されなかった新たな脅威が顕現化する可能性が生じている。そのため、金融機関におけるセキュリティ対策の方針は、クローズド・システムで守るというポリシーから、オープン・ネットワークの利用を前提として情報セキュリティ技術を活用することでセキュリティを確保するという方向に変化している。

こうしたことから、金融機関の情報システムでは、最先端の高度なセキュリティ技術が活用されるようになってきている。例えば、2004年頃から普及し始めたICキャッシュカードには、暗号技術や耐タンパー技術のほか、生体認証技術も実装されるようになった。こうしたさまざまな情報セキュリティ技術が金融サービスに用いられる情報システムに組み込まれるようになり、金融機関の情報システム自体が複雑なものになってきているといえる。その結果、セキュリティ対策を実施した情報システムがセキュリティ要件を満足しているか否かを確認することが容易でなくなってきており、セキュリティ技術分野のエキスパートでなければ適切なセキュリティ評価を実施することが困難となっているのが実情であろう。

情報システムのセキュリティ評価に関しては、近年、情報セキュリティ関連の製品・システム（以下、単に、製品・システムと呼ぶ）の第三者によるセキュリティ評価・認証制度の整備が進展し、わが国においても利用可能となってきている。これは、特定の環境で利用される製品・システムが、想定される脅威に対して適切にセキュリティ対策が講じられていることを、中立的な立場の第三者が評価し、その評価結果を認証するというものである。評価を行う第三者は、セキュリティ評価について豊富な経験とノウハウを有し、信頼できる組織であることを公的な別の組織から認められるというかたちとなっている。具体的には、欧米のセキュリティ評価基準を基に作成されたコモンクライテリア（CC: Common Criteria）に基づく評価・認証制度や、暗号モジュールが満たすべきセキュリティ要件に関する米国連邦政府標準規格FIPS 140-2に基づく試験・認証制度が挙げられる。これらの制度が、わが国ではそれぞれ「ITセキュリティ評価及び認証制度（JISEC: Japan Information Technology Security Evaluation and Certification Scheme）」、「暗号モジュール試験及び認証制度（JCMVP: Japan Cryptographic Module Validation Program）」として2001年4月、

2007年4月からそれぞれ運用が開始された。こうした評価・認証制度は、情報システムのセキュリティ評価が容易でなくなってきているなかで、金融機関が適切にセキュリティ対策を講じるうえで利用できる手段の1つになると考えられる。また、中立的な第三者による評価・認証は、金融機関が自社の金融サービスの信頼性を顧客等にアピールするうえで有用な手段にもなるであろう。

ただし、こうした制度による認証を取得さえしていれば、適切なセキュリティ対策を実施することができるとは必ずしもいえないことに留意が必要である。例えば、製品・システムが想定されている環境以外で使用された場合、仮に認証を得ていたとしても当該製品・システムのセキュリティ機能が有効に機能しない可能性がある。また、製品・システムへの脅威は日々高度化しており、ある時点で認証を取得できた製品・システムを利用していても、そのセキュリティ機能は徐々に低下し、やがては期待していた効果を発揮することができなくなる可能性もある。第三者によるセキュリティ評価・認証制度を適切に利用していくに当たっては、その目的や仕組みを正しく理解するとともに、活用のあり方について検討しておくことが必要であると考えられる。

本稿では、金融サービスに用いられる情報システムが高度化していくなかで、セキュリティ評価を適切に行い一定のセキュリティ要件が満足されていることを確認しやすくするための手段の1つとして、第三者によるセキュリティ評価・認証制度を位置付けたうえで、こうした制度を活用することによるメリットや留意すべき点について考察を行う。とりわけ、わが国の金融機関による活用事例として公表されているものがまだ少ないCCに基づくセキュリティ評価・認証制度とFIPS 140-2に基づく暗号モジュール試験・認証制度に焦点を当てる。

本稿の構成は以下のとおりである。まず、2節において、金融機関によるセキュリティ対策のあり方について説明するとともに、情報システムの高度化・複雑化について説明し、そうした状況のもとで第三者による評価・認証制度を利用するメリットを考察する。3、4節では、JISEC等、CCに基づくセキュリティ評価・認証制度と、JCMVP等、FIPS 140-2に基づく暗号モジュール試験・認証制度についてそれぞれ説明する。5節では、金融機関が本制度を活用するうえでのメリットと留意点についてそれぞれ考察を行い、6節で以上の考察結果を整理して本稿を締め括る。

2. わが国の金融業界におけるセキュリティ対策と第三者評価・認証の有用性

(1) 金融分野における情報システムの安全対策

わが国の金融分野における情報システムの安全対策の実施手順については、財団法人金融情報システムセンター（FISC）によって作成されている『金融機関等コン

ピュータシステムの安全対策基準・解説書』（以下、FISC 安全対策基準と呼ぶ。FISC [2006]）[1]、および、『金融機関等におけるセキュリティポリシー策定のための手引書』（FISC [1999]）において以下のように整理されている（図 1 参照）。

1 セキュリティ・ポリシーの策定

1.1 目的・目標の設定と明確化：何を守るのか、なぜ守るのか、誰が責任を負うのかなどを明らかにし、会社としての安全対策に関する基本方針を決定する。
1.2 情報資産の洗出し：会社として守るべき重要な情報資産を洗い出す。
1.3 脅威の認識とリスクの評価：洗い出した情報資産を取り巻く脅威を認識するとともに、各脅威のリスクの程度を明らかにする。

2 セキュリティ・スタンダード（自社の安全対策基準）の策定と実施

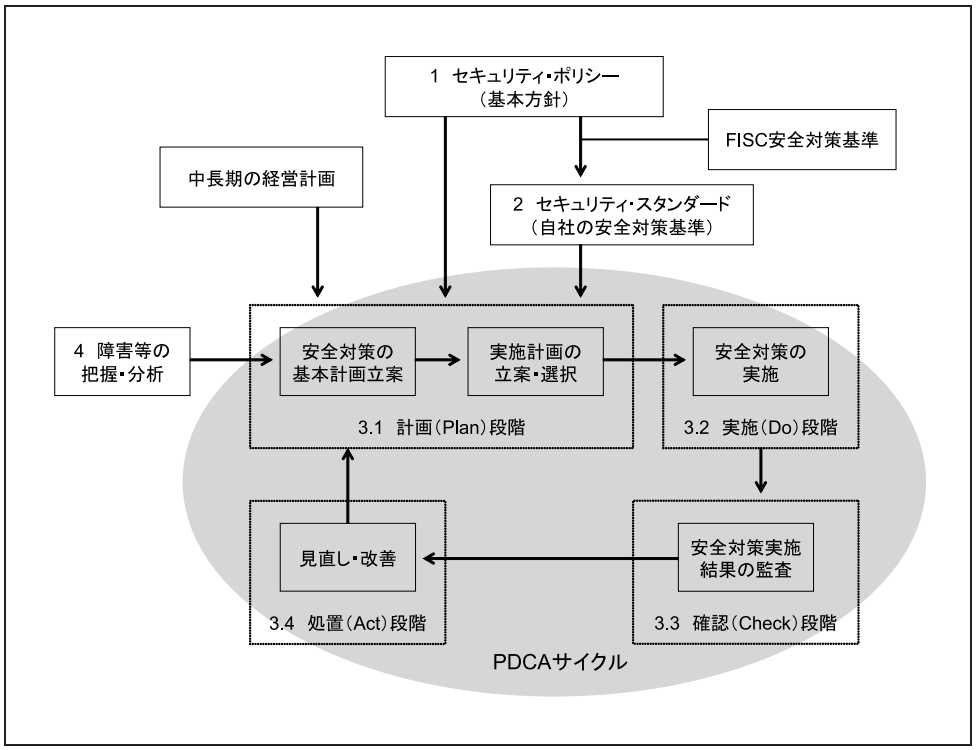
2.1 対策項目の選択と原案（ドラフト）の作成：セキュリティ・ポリシーに準拠し、具体的に何をどのように行うかを決定する。
2.2 目標とするレベルの明確化：セキュリティ・スタンダードの記述レベルを検討する材料として、個々の情報資産の重要性に基づく目標とする実施レベルを明らかにし、原案の修正を行う。
2.3 システムの対応と例外の規定：現在の技術や会社風土、投入可能なコスト等の理由によるセキュリティ・ポリシーの例外となるケースのために、例外扱いの規定を整備する。

3 安全対策の改善

3.1 計画（Plan）：対象となる組織と情報資産の識別、情報資産とリスクを評価し、セキュリティ上の弱点や課題に対して安全対策の方針を確定する。さらに、本方針を踏まえ、具体的な安全対策を選定し、実施計画を立案する。採用する記述、ハードウエア、ソフトウエアの選定、運用方針の決定、マニュアルや手順書の変更、ユーザ教育等の計画を確定する。
3.2 実施（Do）：実施計画およびセキュリティ関連文書に基づいて安全対策を実施する。
3.3 確認（Check）：独立した監査部門による監査等により安全対策の状況について客観的な評価を実施することが必要である。なお、定期的に外部監査機関による外部監査を実施することが望ましい。
3.4 処置（Act）：監査結果を基に、見直し改善を行う。

1 FISC 安全対策基準は、わが国の金融機関が提供する金融サービスに関連するコンピュータ・システムに安全対策を実施するための共通基準として策定されたものであり、各金融機関がコンピュータ・システムの適切な安全対策を実施するうえで参考にすることが期待されている。また、『金融検査マニュアル』（金融庁［2007］）にも引用されており、わが国の金融機関が情報システムの安全対策を講じる際に依拠する基準となっている。

図 1　FISC による安全対策の実施手順（FISC [2006] より引用）



4　コンティンジェンシー・プラン（緊急時対応計画）の策定：金融機関等のコンピュータ・センター、営業店、本部機構等が、不慮の災害や事故、障害等により重大な損害を被り、業務の遂行が果たせなくなった場合に、各種業務の中断の範囲と期間を極小化し、迅速かつ効率的に必要な業務を普及するために、緊急時対応計画として「コンティンジェンシー・プラン」を策定する。

FISC 安全対策基準で整理されている安全対策の実施手順のうち、上記 3 における計画（Plan）・実施（Do）・確認（Check）・処置（Act）からなるサイクル（PDCA サイクルと呼ばれる）を繰り返すことで、組織のセキュリティ・レベルを継続的に維持・改善する手法は、「情報セキュリティ・マネジメント・システム（ISMS: Information Security Management System）」と呼ばれている[2]。ISMS では、組織のマネジメントとして、自らのリスク・アセスメントにより必要なセキュリティ・レベルを決め、プランをもち、資源を配分して、システムを運用することが重要とされている（JIPDEC [2007]）。わが国の金融機関においても、PDCA サイクルにより組織のセキュリティ・レベルを一定以上に維持するためのマネジメントが進められている（日本銀行金融機構局［2007］）。

2「ISMS」は、「ISMS 適合性評価制度」（本節（3）イ．参照）の略語として狭義に使われることもあるが、本稿では、広義に安全対策を実施するためのマネジメント体系を指すものとする。

(2) 第三者によるセキュリティ評価・認証の有用性

上記手順によるセキュリティ対策の実施においては、金融業務に関する各種の要件に基づいてセキュリティ・スタンダードが策定される。セキュリティ・スタンダードの策定には、情報セキュリティ技術に関する専門知識が必要となることから、金融機関は、従来からベンダーと協力して対策を講じてきた。

ただし、近年、金融業務の多様化に伴って金融機関の情報システムが複雑化してきており、当該システムがセキュリティ要件を満足しているか否かを確認することが容易でなくなってきている。例えば、従来 ATM 等で利用するキャッシュカードは磁気ストライプ付きのカードであったが、2004 年頃から IC カード化が急速に進められており、クレジットカード機能、電子マネー機能、ポイントカード機能等が IC キャッシュカードに搭載されるようになってきている。さらに、生体認証による本人確認の機能を有するカードも徐々に普及しつつある。このように、最先端の情報技術が組み込まれるかたちで情報システムが構成されているといえる。

さらには、金融機関の情報システムへの脅威となる攻撃手法も高度化してきており、暗号技術や耐タンパー技術等の最先端の情報セキュリティ技術が実装されるようになってきている。例えば、IC カードの耐タンパー技術については、IC チップの消費電力量等から内部の暗号鍵を効率よく推定する高度な攻撃への対策も求められ始めている（NIST [2007]、田村・宇根［2007］）。その結果、情報システムのセキュリティ評価は情報セキュリティ技術分野に精通したエキスパートでなければ適切に実施することが困難となっており、セキュリティ上の問題点を見逃してしまうリスクも従来に比べて高まっている。

実際に、暗号技術を実装したソフトウエアやハードウエア（暗号モジュール）の試験・認証制度である米国・カナダの CMVP（Cryptographic Module Validation Program）の試験結果として、試験対象となった暗号モジュールの約半数がセキュリティ上の問題点を抱えており、CMVP の認証を得ることができなかったとの報告がある（NIST and CSE [2007]）。また、同報告では、暗号アルゴリズムが仕様書通りに実装されているか否かの試験において、約 27％の暗号モジュールが不適切な実装を行っていたとの結果も示されている。これらの事例は暗号モジュールに関するものであるとはいえ、暗号モジュール以外の製品・システムの評価の場合も同様の問題が存在しうると考えられる。

こうした問題に対して、セキュリティ評価をより確実なものにする方法として、製品・システムのセキュリティ評価に関して豊富なノウハウや経験を有する第三者による評価を受ける、あるいは、評価結果を参照するという方法が考えられる。第三者のセキュリティ評価を受ける方法としては、金融機関が独自に評価者を選定して行うというものや、近年整備されてきている CC に基づく評価・認証制度等の第三者による評価・認証制度を利用するというものが挙げられる。これらのうち第三者による評価・認証制度の利用では、独自評価に比べて次のメリットが期待される。

A） 評価者を選定する際には当該評価者の技術力等を審査する必要があり、そのためには金融機関自らも高い技術力を確保することが求められる。既存の第三者による評価・認証制度では、その枠組みのなかで公的機関等によって認定された評価者のリストから評価者を選択することが可能となり、金融機関が自ら評価者を審査・選定するために要する手間や労力を削減することができる。

B） 第三者の評価者による評価結果が正当であることを別の機関（認証機関）が認証し、評価の「お墨付き」を得ることができる。そうした「お墨付き」を顧客や取引相手に提示することにより、評価対象となった製品・システムのセキュリティ・レベルへの信頼を高めることが可能となる。

C） CC に基づく評価・認証制度等は海外でも運用されていることから、海外において新たな金融サービスを開始する際に、あるいは、海外の金融機関と共同で金融サービスを提供する際に、自社の製品・システムのセキュリティ評価結果を「海外でも通用するお墨付き」によって提示することで理解を得られやすい。

ただし、こうしたメリットが期待できる一方で、第三者による評価・認証制度を利用する際には、評価や認証の申請等にかかる費用の負担が必要となる[3]。

第三者による評価・認証制度を活用するか否かを検討する場合には、上記のようなメリットやコストを比較考量することになるが、評価・認証制度を活用することによって得られる効果等を定量的に算出することは現時点では困難である。ただ、今後も情報セキュリティ技術がより幅広い金融サービスに活用されるようになり、金融サービスの信頼性向上というメリットを享受できるようになる反面、情報セキュリティ上の問題が金融サービスに与える影響も大きくなっていくとすれば、第三者による評価・認証制度をどのように活用することができるかについて検討しておくことは意義があるといえる。

(3) 既存の評価・認証制度

情報セキュリティ対策を適切に実施するうえで活用することができる第三者による評価・認証の枠組みについては、運用管理面と技術面からのセキュリティ評価を目的としたものが既にいくつか整備されている（表 1 参照）。

イ．運用管理面からの評価・認証制度

情報セキュリティ対策の運用管理面からのセキュリティ評価を目的としたものとしては、わが国において 2002 年 4 月から本格運用が開始されている「ISMS 適合性

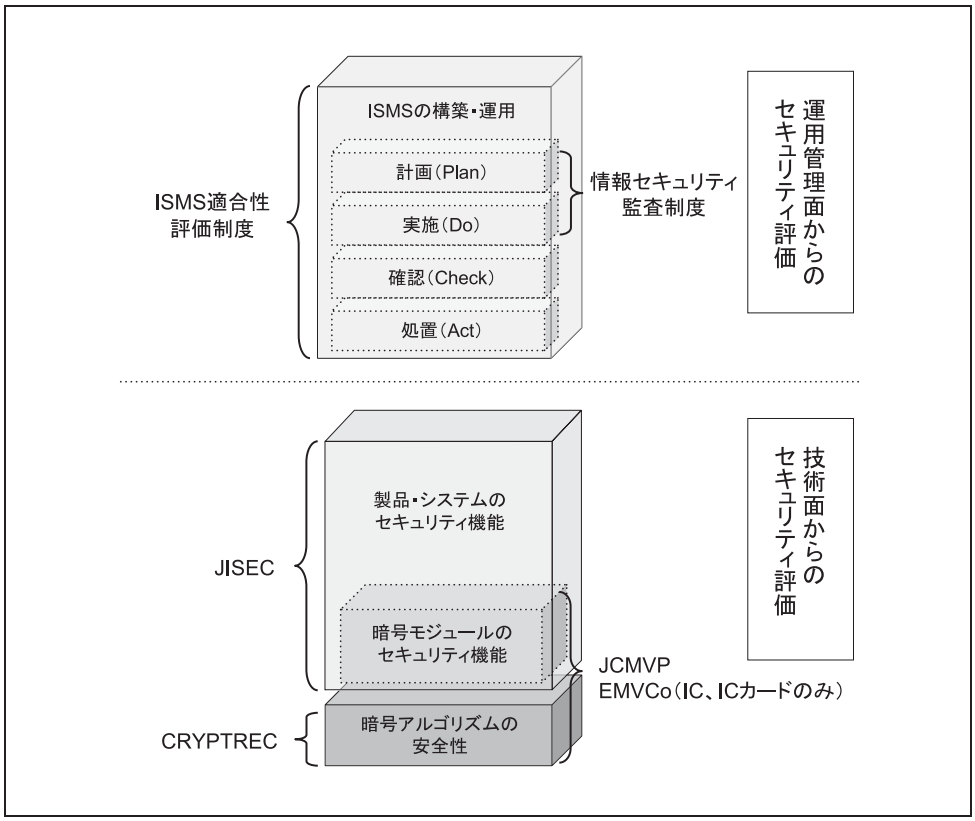
3 認証申請にかかる費用としては、例えば、JISEC（3 節参照）におけるセキュリティ評価では、評価保証レベル EAL4 での申請に約 100 万円が必要となるほか、JCMVP（4 節参照）では、セキュリティ・レベル 4 での認証申請に約 74 万円が必要となる（IPA [2006, 2007]）。また、評価や試験に必要な費用は実費となり評価機関によって異なるが、一般に、評価・試験対象の製品・システムの規模、評価保証レベル、評価を行うスタッフの熟練度等に依存するといわれている。

表１　情報セキュリティに関する既存の第三者評価・認証制度等の概要

第三者評価・認証制度	評価基準と評価方法	評価の目的	評価対象	運営主体	評価者	運用開始時期
【運用管理面】ISMS 適合性評価制度	JIS Q 27001（BS7799-2、ISO/IEC 27001）	組織として ISMS が適切に構築・運用されているか否かを評価・認証する。	組織の ISMS の運用	財団法人日本情報処理開発協会（JIPDEC）	認定機関（JIPDEC）が認定した審査登録機関（現在、約 20 社）	2002 年 4 月
【運用管理面】情報セキュリティ監査制度	情報セキュリティ管理基準：JIS Q 27002（BS 7799-1、ISO/IEC 17799）、情報セキュリティ監査基準	ISMS における計画（Plan）・実施（Do）が適切に実施されているか否かを評価する。	組織の ISMS の一部	特定非営利活動法人日本セキュリティ監査協会（JASA）	独立かつ専門的知識を有する専門家（内部監査人、外部監査人）	2003 年 3 月
【技術面】IT セキュリティ評価及び認証制度：JISEC	評価基準：CC（ISO/IEC 15408、JIS X 5070）、評価方法：CEM（ISO/IEC 18045）	製品・システムのセキュリティ機能を定義し、その機能が適切に実施されているか否かを評価・認証する。	製品・システムのセキュリティ機能	独立行政法人情報処理推進機構（IPA）	認定機関（NITE）が認定した評価機関（現在、4 社）	2001 年 4 月
【技術面】暗号モジュール試験及び認証制度：JCMVP	評価基準：JIS X 19790（FIPS 140-2、ISO/IEC 19790）、試験基準：JIS X 5091（DTR、ISO/IEC FCD 24759）	暗号モジュールが一定のセキュリティ要件を満足しているか否か、および、暗号アルゴリズムが適切に実装されているか否かを試験・認証する。米国では、CMVP の認証取得が連邦政府調達基準となっている。	暗号モジュールのセキュリティ機能	独立行政法人情報処理推進機構（IPA）	認定機関（NITE）が認定した試験機関（現在、1 社）	2007 年 4 月
【技術面】EMVCo による評価・認証の枠組み	EMVCo Security Guideline、JIL Application of Attack Potential to Smart Cards*	安全性と相互運用性を確保するため、クレジットカード業務向けの IC カードが EMVCo の規定するセキュリティ要件を満足しているか否かを試験・認証する。	クレジットカード業務向けの IC カードのセキュリティ機能	EMVCo	EMVCo が認定した独立の試験機関（現在、3 社）	2007 年 4 月
【参考】CRYPTREC による電子政府推奨暗号リスト	評価項目、評価基準については、IPA・TAO［2003］に記述。	暗号アルゴリズムを主に安全性の観点から評価し、リスト化する。わが国の電子政府調達基準となっている。	暗号アルゴリズム	暗号技術検討会（事務局：総務省、経済産業省）	評価は、暗号技術評価委員会および外部の専門家が実施。電子政府推奨暗号の監視等は、暗号技術監視委員会が実施。	2000 年 5 月

備考：*JIL（Joint Interpretation Library）は、フランス、ドイツ、オランダ、英国の IT 製品のセキュリティ評価・認証に関するエキスパートで構成される JIWG（Joint Interpretation Working Group）によって作成された文書であり、CC に基づくセキュリティ評価方法を IC カード評価に適用する場合における具体的な解釈を与えるものである。

図 2　既存の第三者評価・認証制度の評価対象



評価制度」（JIPDEC [2007]）や 2003 年 3 月から運用されている「情報セキュリティ監査制度」（JASA [2006]）がある（図 2 参照）。このうち、ISMS 適合性評価制度は、組織が構築した ISMS が認証基準（JIS Q 27001: 2006）に準拠して適切に構築・運用されているか否かを評価・認証する制度であり、既に認証を取得している金融機関も多い。評価の対象となっている業務としては、インターネット・バンキング、生体認証システム、金融商品・サービスの企画・推進・営業支援システムに関する業務が挙げられる。FISC による調査レポート（FISC [2007]）では、ISMS 適合性評価制度の利用目的について、「第三者から取組み状況を客観的に審査されることで行内の甘えを排除できるため（三菱東京 UFJ 銀行）」や、「自社内での情報セキュリティ管理に役立つのみならず、第三者による評価結果を公表することで顧客の信頼を得ることができるため（ソニー銀行）」と紹介されている。

また、情報セキュリティ監査制度は、ISMS の構成要素の 1 つである安全対策の実施結果の「確認（Check）」を第三者が行うものであり、情報セキュリティ管理基準（JIS Q 27002: 2006 を基に作成）に記述されているセキュリティ管理要件を参考に、ISMS における計画（Plan）・実施（Do）が適切に実施されているか否かを評価する制度である。ただし、本制度では、組織が実施しているセキュリティ対策のレベル

に応じて監査を受けることができるように、監査の対象を柔軟に選択することができるようになっており、情報セキュリティ管理基準の一部のみの監査を受けることも可能である。さらに、本制度では、組織の安全対策が適切であるか否かのみを判断して伝達する「保証型監査」と、ISMS の構築・運用を目指す組織に対して監査結果に基づく助言を行う「助言型監査」がある。2005 年度には、監査を受けた企業数が約 1 万件となったと報告されている（JASA [2007]）。

ロ．技術面からの評価・認証制度

技術面からのセキュリティ評価を目的としたものとしては、①2001 年 4 月に運用が開始した「IT セキュリティ評価及び認証制度（JISEC）」（IPA [2006]）、②2007 年 4 月から本格運用が開始した「暗号モジュール試験及び認証制度（JCMVP）」（IPA [2007]）、③EMVCo[4]による IC カードの評価・認証の枠組み（EMVCo [2006] 等）が挙げられる（図 2 参照）。

JISEC は、国際標準化されているセキュリティ評価基準である CC を参考にして、製品・システムのセキュリティ機能を定義し、その機能が適切に実装されているか否かを評価・認証する制度である。JCMVP は、暗号モジュールが一定のセキュリティ要件を満足しているか否かを、米国連邦政府標準規格 FIPS 140-2 を参考に策定された JIS X 19790: 2007 に基づいて試験・認証する制度である[5]。ただし、JCMVP における試験対象は、CRYPTREC（Cryptography Research and Evaluation Committees）による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中心とした「承認暗号アルゴリズム」が実装された暗号モジュールのみとなっている[6]。また、EMVCo による評価・認証の枠組みでは、クレジットカード業務において利用する IC カードが満たすべきセキュリティ要件を規定する[7]とともに、それらが実際に満たされているか否かの評価を第三者に依頼し、その評価結果を認証している。JISEC、JCMVP、EMVCo は認証を取得した対象の一覧を公開している。

4 EMVCo は、IC カードを用いたクレジットカード決済システムの相互運用性を確保することを目的として、IC カードと端末に関する仕様を定めた EMV 仕様の管理・維持・推進を行っている会社であり、Visa International、MasterCard International、JCB International の 3 社によって運営されている。

5 JISEC が評価基準として利用する CC は、すべての製品・システムに適用できるセキュリティ評価基準であり、暗号モジュールについても適用可能である（ECSEC [2004]）。ただし、CC は汎用性が高いため、特定の製品・システムに適用する際には、セキュリティ機能要件やセキュリティ保証要件（3 節（2）参照）の詳細化や要件拡張が必要となる。一方、JCMVP で利用される JIS X 19790（内容は実質的に FIPS 140-2 と同一）は、対象を暗号モジュールに限定しており、セキュリティ要求事項が具体的に規定されている。CC と FIPS 140-2 の違いについては、植村［2005a, b］において整理されている。

6 JCMVP は、独自に暗号アルゴリズムの安全性評価を実施しているわけではないが、CRYPTREC によって安全性が評価された電子政府推奨暗号を中心とした「承認暗号アルゴリズム」を選定していることから、図 2 では JCMVP の試験・認証の対象に暗号アルゴリズムを含むこととした。

7 EMVCo による評価・認証は、各クレジットカード・ブランドが独自に実施してきたセキュリティ評価（例えば、VISA [2007]）を統一した共通の評価基準に基づいて EMVCo が行うものである。

ハ．本稿での検討対象

このように、情報セキュリティの運用管理面については ISMS 適合性評価制度がわが国の金融機関によって既に活用されており、本制度を活用するメリットや留意点については十分認識されていると考えられる。一方で、技術面については、JISEC および JCMVP の金融分野における活用事例がまだ少なく、今後の検討課題となっているように窺われる。

そこで、以下では、さまざまな金融サービス向けの情報システムに適用可能な JISEC と JCMVP、および、これらのベースとなっている CC に基づくセキュリティ評価・認証制度と、FIPS 140-2 に基づく暗号モジュール試験・認証制度に焦点を当てて、それぞれ 3、4 節において紹介する。EMVCo による評価・認証の枠組みについては、クレジットカード業務のみをアプリケーションとした IC カードのみをセキュリティ評価対象としており、アプリケーションが限定されていることから、本稿の検討対象としないこととする。

3. CC に基づくセキュリティ評価・認証の枠組み

(1) これまでの変遷

1980～90 年代、欧米諸国は IT 製品に関する独自の評価基準を策定し、各国内でセキュリティ評価・認証制度を運用していた。すなわち、米国の TCSEC[8]、欧州の ITSEC[9]、カナダの CTCPEC[10]がこうした評価基準の代表例であった。ただし、各評価基準や運用方法は区々であり国際的な相互運用性に欠けるという問題があった。そこで、米国、カナダ、英国、フランス、ドイツは、これらのセキュリティ評価基準の統一を目的として、CCEB（Common Criteria Editorial Board）を組成し、評価基準の統一を目指す「CC プロジェクト」を開始した。

CCEB[11]は、1996 年 1 月に CC Ver. 1.0 を発表した後、2006 年 9 月には CC Ver. 3.1

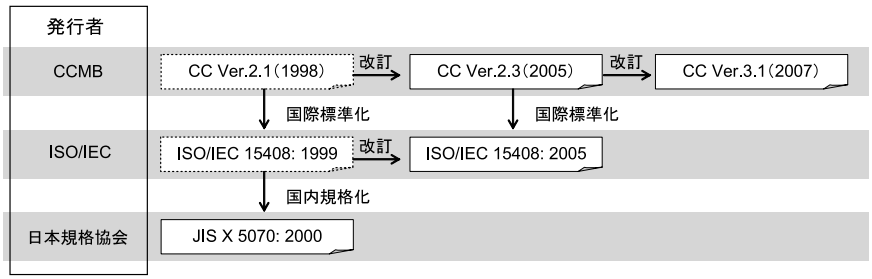
8 TCSEC（Trusted Computer System Evaluation Criteria）は、米国の国防機関において利用されるセキュリティ関連製品の評価基準書として 1983 年に策定（1985 年に改訂）された。米国では、TCSEC に基づいた評価・認証制度である TPEP（Trusted Product Evaluation Program）の運用が 1986 年から開始されている。

9 ITSEC（Information Technology Security Evaluation Criteria）は、欧州各国の統一的なセキュリティ評価基準であり、政府に加えて民間での利用も視野に入れた評価基準として 1991 年に策定された。また、欧州では ITSEC に基づく評価・認証スキームである ITSEM（IT Security Evaluation Manual）が運用されていた。

10 CTCPEC（Canadian Trusted Computer Product Evaluation）は、TCSEC と ITSEC を参照するカナダの政府機関向けの評価基準であり、1993 年に策定された。

11 CC Ver. 1.0 の完成後、CCEB は解散し、新しい CC 策定グループとして CCIB（Common Criteria Implementation Board）が発足した。CCIB は CC Ver. 2.0 への改訂作業を行い、ISO/IEC 15408: 1999 として CC が国際標準化された後、解散した。その後、CCIMB（Common Criteria Interpretation Management

図 3　CC、ISO/IEC 15408、JIS X 5070 の対応関係



備考：CC Ver. 2.1 は CCIMB によって発行された。また、点線で囲んだ標準・規格は改訂により廃止されたものを示す。

（改訂第 1 版）を、2007 年 9 月には CC Ver. 3.1（改訂第 2 版、パート 2、3 のみ）を公開している（CCMB [2006, 2007a, b]）。

CC の国際標準化については、ISO/IEC JTC1/SC27/WG3 に対して CC Ver. 1.0 が提案され、CC Ver. 2.1 が 1999 年 12 月に ISO/IEC 15408: 1999 として標準化された。また、わが国においても JIS X 5070: 2000（JISC [2000a, b, c]）[12]が ISO/IEC 15408: 1999 の国際一致規格として発行されている。さらに、国際標準の定期見直しにより、2005 年には ISO/IEC 15408: 2005（ISO and IEC [2005a, b, c]）が標準化されている。これらの対応関係は図 3 のとおりである。

（2）CC

イ．CC の構成

CC の規格書（CC Ver. 3.1）は、以下の 3 つのパートで構成されている。

- パート 1「概説と一般モデル」: CC において利用される用語、概念、土台となる評価の一般モデルの概要を規定している。
- パート 2「セキュリティ機能コンポーネント」: 評価対象の製品・システム（TOE: target of evaluation）のセキュリティ機能要件を規定している。セキュリティ機能要件は TOE に必要とされる汎用的なセキュリティ機能を示すものであり、各項目は、クラス、ファミリー、コンポーネントの 3 層構造で記述されている。

Board）が発足し、CC Ver. 2 シリーズのメンテナンスは CCIMB によって行われた（IPA [2003]）。また、CC Ver. 2.3 以降については CCMB（Common Criteria Maintenance Board）によって策定されている。

12 JIS X 5070: 2000 は、ISO/IEC 15408: 1999 のパート 1 を日本語翻訳し、パート 2、3 を原文のままとした要約形式として発行されている。

- パート3「セキュリティ保証コンポーネント」：TOEのセキュリティ保証要件と評価保証レベル（EAL: evaluation assurance level）を規定している。セキュリティ保証要件とは、セキュリティ機能が正しく実装されていることを確認するための検査項目であり、評価保証レベルは、検査対象の範囲や検査の程度を7段階（EAL 1〜7）で示すものである。EALの値が多くなるほど評価対象が広くなり、TOEの品質の保証レベルが向上する。

こうしたCCの記載内容を基に作成されたプロテクション・プロファイル（PP: protection profile）やセキュリティ・ターゲット（ST: security target）等に基づいて、製品の設計・開発・評価が行われることとなる。

ロ．PP

PPは、製品のカテゴリーごとに作成されるセキュリティ要求仕様書であり、CCをカスタマイズしたものと位置付けられる。そのため、PPは一般に業界団体や個々のユーザによって作成されることが想定される。PPは、評価機関による評価の後、公的機関として運用される登録局に登録されることにより公知になる。既存のPPは、CCプロジェクトの公式サイト[13]等から入手することができる。

ハ．ST

STは、評価対象の製品・システムごとに作成されるセキュリティ設計仕様書であり、当該製品・システムの開発者によって作成される。当該製品・システムのユーザが自身のセキュリティ要件を整理したPPが存在する場合には、それを参考にして製品固有の記述を追加することで作成することができる。一方、PPが存在しない場合には、他のユーザが作成したPPを参考にSTを作成することとなる。CCに規定されているSTの主な内容は表2のとおりである。

このように、STを作成するうえでは、ある前提となる環境で想定される脅威を明確にし、達成すべき目標であるセキュリティ対策方針を設定したうえで、求められるセキュリティ機能要件と保証要件を導出する必要がある。特に、TOEが前提条件を満たさない環境で運用される場合には、当該TOEがSTに記述されたセキュリティ機能性のすべてを提供できなくなる可能性があることに留意が必要である。例えば、金融機関の運用による対策が十分機能しうる環境での利用を前提とした製品を、そうでない環境で利用した場合には、STに記述されたセキュリティ機能要件を満足することができなくなる可能性がある。

13 http://www.commoncriteriaportal.org/

表 2　ST の主な内容

項目		内容
ST 概説	ST 参照、TOE 参照	ST を識別するための名称等、および、ST への適合を主張する TOE を識別するための名称等を示す。
	TOE 概要	TOE の使用法と主要なセキュリティ機能の特徴を簡潔に示す。
	TOE 記述	TOE を構成するすべてのハードウエア、ファームウエア、ソフトウエア、ガイダンスのリストを詳細に記述する。TOE によって提供される論理的なセキュリティ機能の特徴を詳細に記述する。
適合主張	CC 適合主張、PP 主張、適合根拠	ST と CC の適合性を記述する。また、適合を主張する PP 等が存在する場合、それらとどのように適合するかについても記述する。
セキュリティ課題定義	脅威	想定する脅威を示す。
	組織のセキュリティ方針	組織のセキュリティ方針（想定される運用環境において課せられるセキュリティ関連の規則、手続、ガイドライン）を示す。
	前提条件	TOE の運用環境に対して設定する運用条件を示す。前提条件には、運用環境の物理的条件、人的条件等がある。
セキュリティ対策方針	TOE のセキュリティ対策方針	セキュリティ課題（の一部）を解決するために TOE が達成すべき目標を記述する。
	運用環境のセキュリティ対策方針	TOE が、セキュリティ対策方針によって定義されるセキュリティ機能性を正しく提供できるように、運用環境で達成すべき目標を記述する。
	セキュリティ対策方針根拠	セキュリティ対策方針の各項目と、脅威、組織のセキュリティ方針、前提条件との対応関係を示し、これらがすべてセキュリティ対策方針によって効果的にカバーされていることを示す。
拡張コンポーネント定義	拡張コンポーネント定義	CC パート 2、パート 3 に規定されていないセキュリティ要件が存在する場合には新たなコンポーネントを定義する。
セキュリティ要件	セキュリティ機能要件	CC パート 2 のコンポーネントに基づいて、TOE のセキュリティ対策方針をより詳細に記述する。
	セキュリティ保証要件	CC パート 3 のコンポーネントに基づいて TOE の評価方法を記述する。
	セキュリティ要件根拠	選択したセキュリティ保証要件が適切であることの根拠を記述する。
TOE 要約仕様	TOE 要約仕様	TOE がどのようにすべてのセキュリティ機能要件を満たすかを、TOE のユーザが理解できるよう記述する。

(3) CC に基づくセキュリティ評価・認証制度

イ．セキュリティ評価・認証制度の枠組み

CC に基づく評価・認証制度を構成するエンティティとその役割は以下のとおりである。

- 認定機関（accreditation authority）：評価機関を認定する機関である。
- 評価機関（evaluation facility）：CC に基づいて TOE および PP の評価を実施する機関である。
- 認証機関（certification authority）：評価機関による評価結果が適正であるか否かを検証し、適正であると判断した場合には、認証した製品・システムに対して認証書と認証報告書を発行する機関である。

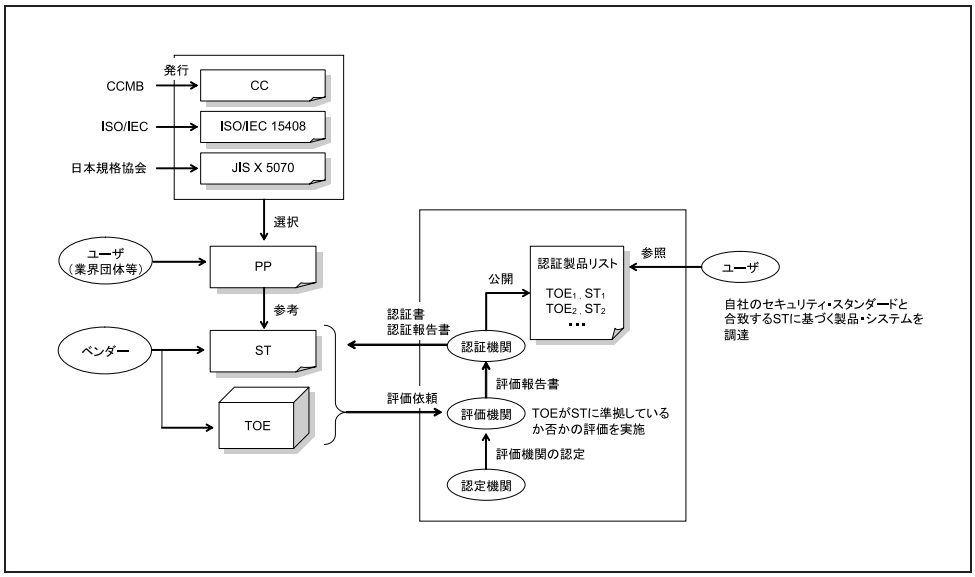
本評価・認証制度の一般的な手順は以下のとおりである（図 4 参照）。

1. ユーザ（または業界団体）は、評価対象のカテゴリごとに必要とされるセキュリティ機能要件と保証要件を CC の評価モデルを参考にして選択し、PP を作成する。
2. ベンダーは、（適用分野の PP を参考にして、）TOE の ST を作成し、ST に基づいて TOE を開発・製造する。
3. 評価機関は、ST に基づいて開発・製造された TOE を、基となった（PP および）ST とともに規定された手続に沿って評価し[14]、評価報告書を作成して認証機関に提出する。
4. 認証機関は、評価機関による評価結果が適正か否かを判断し、適正であると判断した場合には、TOE に対して認証書と認証報告書を発行する。また、認証製品リスト（ST、認証書等を含む）を作成し、一般に公開する。
5. 個々の TOE のユーザは、公開された認証製品リストを参照し、調達する製品・システムを選択する。

このように、ユーザは ST を参照することによって、その ST に対応する TOE において想定されている脅威、その脅威への対策として実装されたセキュリティ機能、その機能がどこまで保証されているかなどを知ることができる。しかし、ベンダーの意向により ST が公開されていない場合にはこうした判断を実施することが困難となる。

14 CEM（Common Methodology for Information Technology Security Evaluation）は、CC に基づくセキュリティ評価スキームであり、評価の実施に必要な評価方法が記述されている。2005 年に ISO/IEC 18045: 2005 として国際標準化されているほか、JIS TR X 0049: 2001 として公表されている。また、2006 年 9 月には CEM Ver. 3.1 が公開されている。

図４　CC に基づくセキュリティ評価・認証の枠組み



CC に基づく評価・認証制度は、例えば、米国においては、国立標準技術研究所（NIST: National Institute of Standards and Technology）と国家安全保障局（NSA: National Security Agency）によって CCEVS（National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme）として運営されており、英国においては、通信電子セキュリティ・グループ（CESG: Communications-Electronics Security Group）と貿易産業省（DTI: Department of Trade and Industry）によって UK ITSEC（UK Information Technology Security Evaluation and Certification Scheme）として運営されている。わが国では、2001 年 4 月から JISEC が運営されている（本節（3）ハ．参照）。

ロ．認証結果の相互承認

セキュリティ評価・認証のレベルを統一することによって認証済みの製品・システムの相互利用を促進させることを目的として、1998 年 10 月、欧米諸国において CC に基づくセキュリティ評価・認証の相互承認に関する協定書（MRA: Mutual Recognition Arrangement）が作成された。カナダ、フランス、ドイツ、英国、米国が MRA に調印し、これら 5 ヵ国間での国際的な相互承認アレンジメントが開始した。さらに、本協定書は 2000 年 5 月に「国際評価及び認証の相互承認に関する国際アレンジメント（CCRA: Common Criteria Recognition Arrangement）」として改訂され、参加するメンバーは認証国（CAP: certificate authorizing participants）と受入国（CCP: certificate consuming participants）に分類されることとなった。CAP は国内に評価・認証制度を有する国を指し、CCP は国内に評価・認証制度を持たず、他の参加国で認証された製品・システムを受け入れる国を指す。わが国は 2003 年 10 月に CCRA

に CAP として加盟しており、2008 年 4 月時点における CCRA 加盟国は 25 ヵ国[15]となっている。

ハ．わが国の JISEC

わが国では、2000 年 4 月に「情報セキュリティ政策実行プログラム―電子政府のセキュアな基盤構築に向けての通商産業省の貢献」が発表された。さらに、2000 年 9 月には、ISO/IEC 15408（JIS X 5070）に基づく「情報セキュリティ評価認証体制の創設」が発表され、2001 年 4 月に JISEC の運用が開始された（IPA [2006]）。JISEC を構成する機関は以下のとおりである。

- 認定機関：独立行政法人製品評価技術基盤機構（NITE: National Institute of Technology and Evaluation）
- 評価機関：有限責任中間法人 IT セキュリティセンター、株式会社電子商取引安全技術研究所（ECSEC: Electronic Commerce Security Technology Laboratory Inc.）評価センター、みずほ情報総研株式会社情報セキュリティ評価室、TÜV Informationstechnik GmbH Evaluation Body for IT-Security
- 認証機関：独立行政法人情報処理推進機構（IPA: Information-technology Promotion Agency, Japan）

JISEC では、2008 年 4 月以降 CC Ver. 3.1 改訂第 1 版と改訂第 2 版が使用可能となっている。ただし、2008 年 10 月からは CC Ver. 3.1 の改訂第 2 版の使用が必須とされている。CC および CEM は、IPA セキュリティセンター情報セキュリティ認証室によって翻訳されており、JISEC のホームページ上で公開されている（IPA セキュリティセンター情報セキュリティ認証室［2007a, b, c］）。また、JISEC は ST 段階での ISO/IEC 15408 への適合性を確認する「ST 確認」と呼ばれる制度を独自に運営している。

これまでにはデジタル複合機[16]を中心に約 170 件の製品・システムが JISEC において認証されている。

15 CAP は、オーストラリア、ニュージーランド、カナダ、フランス、ドイツ、日本、韓国、オランダ、ノルウェー、スペイン、スウェーデン、英国、米国である。CCP は、オーストリア、チェコ、デンマーク、フィンランド、ギリシャ、ハンガリー、インド、イスラエル、イタリア、マレーシア、シンガポール、トルコである。

16 複写機、プリンター、イメージ・スキャナー、FAX 等の機能が 1 つにまとめられている機器。複合機内に蓄積されたデータがネットワークを通して漏洩する脅威等が想定されることから、JISEC による評価・認証を取得しているケースが多い。

4. FIPS 140-2 に基づく暗号モジュール試験・認証の枠組み

(1) これまでの変遷

米国では、1970 年代から米国連邦政府機関で利用するための暗号アルゴリズムの標準化を行っており、1977 年には FIPS 46 として米国連邦政府標準暗号 DES を策定した。1982 年には、NSA が DES を実装するハードウエアに対するセキュリティ要件を FS 1027 として制定し、FS 1027 は 1988 年に NIST によって米国連邦政府標準規格 FIPS 140 として発行された。その後、FIPS 140 は、DES 以外の暗号アルゴリズムを実装したハードウエアを対象とする規格 FIPS 140-1 に改訂されたほか、ハードウエアのみならず、ソフトウエアやファームウエアも対象とし、暗号モジュールが満たすべきセキュリティ要件（セキュリティ要求事項と呼ばれる）を規定した FIPS 140-2 として 2001 年再度改訂された（NIST [2001]）。現在は、FIPS 140-3 への改訂作業が進められており、2007 年 7 月には FIPS 140-3 のドラフトが公開されている（NIST [2007]）。また、FIPS 140-2 については、米国からの提案により 2006 年に ISO/IEC 19790: 2006（ISO and IEC [2006]）として国際標準化され、わが国においても JIS X 19790: 2007 が ISO/IEC 19790: 2006 の国際一致規格として発行されている。これらの対応関係は図 5 のとおりである。

こうしたなか、1995 年には、NIST とカナダの通信安全機構（CSE: Communication Security Establishment）によって、FIPS 140-2 に基づく暗号モジュール試験・認証制度として CMVP の運用が開始された[17]。

(2) FIPS 140-2

イ. 暗号モジュールのセキュリティ・レベル

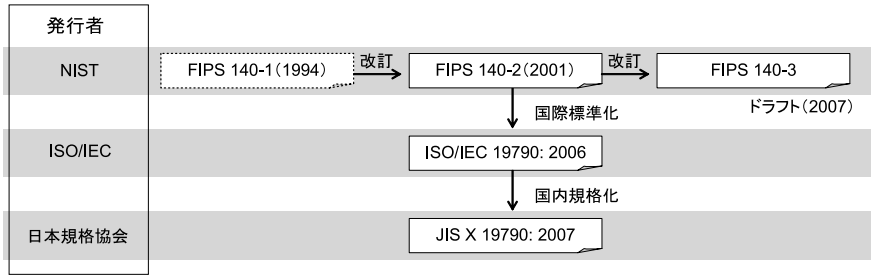
FIPS 140-2 は、暗号モジュールで保護すべきデータの重要度と使用環境に応じて適切に暗号モジュールを選択できるように、評価対象となる暗号モジュールの特性を 11 の「分野」に分けたうえで、暗号モジュールが満たすべきセキュリティ・レベルを各分野に関して 4 つに分類している（表 3 参照）[18]。

試験対象となる暗号モジュールのセキュリティ・レベルは、FIPS 140-2 に規定されているセキュリティ要求事項の充足度合いによって決定される。具体的には、暗号モジュールの各分野についてセキュリティ要求事項の充足度合いを評価し、さらにすべての分野のセキュリティ・レベルの最小値が当該暗号モジュールの「総合的な

17 当初は FIPS 140-1 を暗号モジュール評価基準として利用していた。また、CMVP では 2009 年内に FIPS 140-3 への全面移行を予定している。

18 FIPS 140-3 のドラフトでは、FIPS 140-2 では明記されていなかったサイドチャネル攻撃に対するセキュリティ要求事項が追加され、サイドチャネル攻撃への耐性等に基づいてセキュリティ・レベルが 5 段階とされている。

図 5　FIPS 140 シリーズ、ISO/IEC 19790、JIS X 19790 の対応関係



備考：点線で囲んだ規格は改訂により廃止されたものを示す。

表 3　FIPS 140-2 で規定されるセキュリティ・レベルの概要

セキュリティ・レベル	各セキュリティ・レベルの内容
レベル 1	暗号モジュールとしての基本的なセキュリティ要求事項のみが充足されることが求められるレベルである。例えば、管理運用による対策の手段が限定されている、あるいは、存在しないケースを想定した低いレベルのアプリケーションへの適用を前提としている。
レベル 2	レベル 1 に物理的セキュリティのメカニズムを強化したレベルであり、暗号モジュールに攻撃の痕跡を残す機能（タンパー・エビデンス機能）を要求する。また、暗号モジュールの操作者の権限を確認するための認証機能を最低限必要としている。
レベル 3	レベル 2 で要求されるタンパー・エビデンス機能に加えて、高い確率で攻撃を検出する機能（タンパー・ディテクション機能）、あるいは、能動的に対抗するための機能（タンパー・レスポンス機能）を要求する。また、操作者の ID を確認するための認証機能を要求する。
レベル 4	すべての不正な物理的アクセスに対して、タンパー・ディテクション機能やタンパー・レスポンス機能を要求する最も高いセキュリティ・レベルである。また、高電圧や高温等の規格外環境での使用においても暗号モジュールを保護することが要求される。

セキュリティ・レベル（Overall Level）」として示される。したがって、FIPS 140-2 に基づく試験・認証制度では、試験対象である暗号モジュールのセキュリティ・レベルを、評価結果のうち最も低いレベルで示すものであるといえる（図 6 参照）。

ロ．暗号アルゴリズムの扱い

FIPS 140-2 においては、別の FIPS として規格化されたアルゴリズムと NIST による推奨アルゴリズムを「承認暗号アルゴリズム」（FIPS 140-2 Annex A、C、D に記載）として試験対象の暗号モジュールへの実装を規定している（表 4 参照）。一方、ISO/IEC 19790: 2006 は FIPS 140-2 を基に作成されたものであるが、その承認アルゴリズムは ISO/IEC で国際標準化された暗号アルゴリズムのみとなっている。

図 6　暗号モジュールのセキュリティ・レベルの評価例

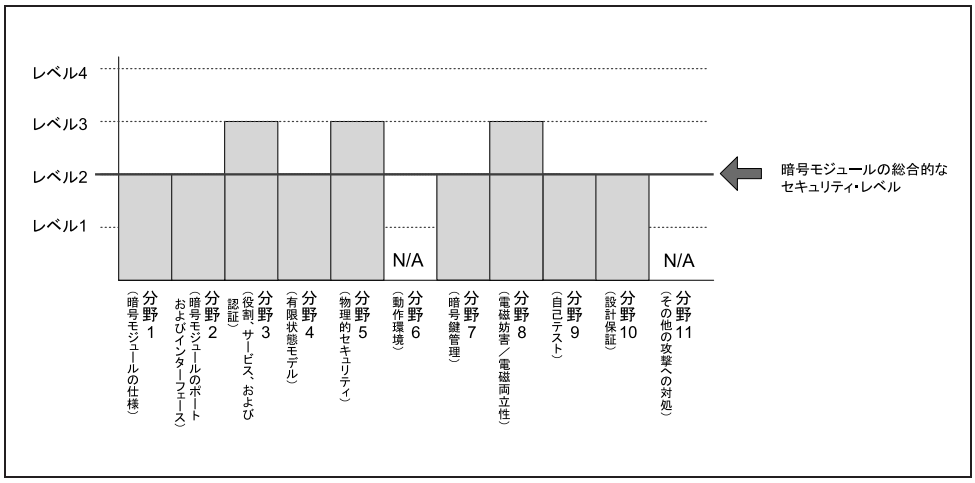


表 4　FIPS 140-2 における承認暗号アルゴリズム

技術分類		暗号名称
公開鍵暗号	署名	・DSA（FIPS 186-2 with Change Notice1）* ・ECDSA（FIPS 186-2 with Change Notice1） ・RSASSA-PKCS-v1_5（PKCS#1 v2.1）* ・RSASSA-PSS（PKCS#1 v2.1）*
	鍵確立	・AES Key Wrap Specification（Draft） ・Recommendation for Pair-Wise Key Establishment Schemes（SP 800-56A） ・FIPS Approved Mode of Operation（FIPS 140-2 Implementation Guidance）
共通鍵暗号	ブロック暗号	・AES（FIPS 197、SP 800-38A、SP 800-38D）* ・トリプル DES（SP 800-67、SP 800-38A、ANSI X9.52-1998）* ・Skipjack（FIPS 185）
その他	ハッシュ関数	・Secure Hash Standard〈SHA-1、SHA-224、SHA-256、SHA-384、SHA-512〉（FIPS 180-2 with Change Notice1）*
	メッセージ認証	・トリプル-DES MAC（FIPS 113） ・Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality（SP 800-38C） ・Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication（SP 800-38B）* ・HMAC-Keyed-Hash Message Authentication Code（FIPS 198）*
	擬似乱数生成系	・Deterministic Random Number Generators（FIPS 186-2 Appendix 3.1、FIPS 186-2 Appendix 3.2、ANSI X9.31 Appendix A.2.4、ANSI X9.62 Annex A.4、NIST-Recommended Random Number Generator、SP 800-90）

備考：表中の“*”は、JCMVP においても承認暗号アルゴリズムとなっているもの（本節（3）ロ. 参照）を示す。ただし、トリプル DES のうち、2-key トリプル DES は JCMVP における承認暗号アルゴリズムとなっていない。

ハ．セキュリティ・ポリシー

セキュリティ・ポリシー[19]は、FIPS 140-2 において規定されるセキュリティ要求事項に基づき、暗号モジュールが準拠しなければならない事項を定めたものである。FIPS 140-2 Appendix C では、セキュリティ・ポリシーの目標を、①暗号モジュールのセキュリティに関する詳細記述を提供し、暗号モジュール実装時に、ユーザがそのセキュリティ・ポリシーの達成の可否を判定できるようにすること、②暗号モジュールによって提供される保護機能やアクセス権を記述し、ユーザが自分のセキュリティ要件の達成に暗号モジュールが有用か否かを自ら判断できるようにすることとしている。このように、FIPS 140-2 に基づく試験・認証制度は、認証済み暗号モジュールのセキュリティ・ポリシーを参考にして、自社のセキュリティ・スタンダードと合致するセキュリティ機能を有する暗号モジュールをユーザが選択することができるようにすることを目指している。

ただし、セキュリティ・ポリシーでは、セキュリティ要求事項を分類した 11 の分野のうち、4 分野のみについて規定が必須とされている。そのため、記述が必須とされていないものについては、該当するセキュリティ要求事項が設定されていない、あるいは、開示されていないことがある。

(3) FIPS 140-2 に基づく暗号モジュールの試験・認証制度

イ．CMVP

CMVP は、暗号モジュールが FIPS 140-2 に準拠しているか否かを試験・認証するものである。CMVP を構成する機関とその役割は以下のとおりである。

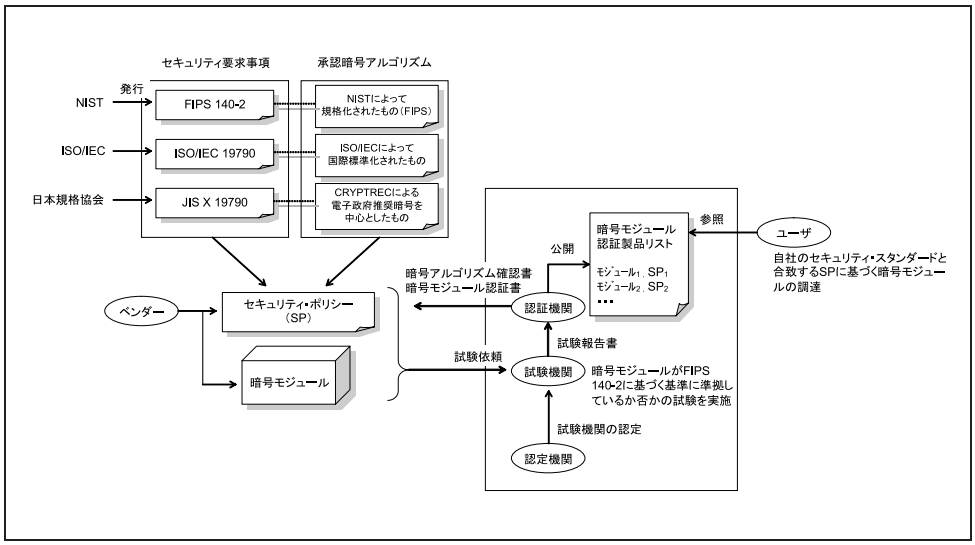
- 認定機関（accreditation authority）：試験機関を認定する機関である。政府機関である NVLAP（National Voluntary Laboratory Accreditation Program）と SCC（Standards Council of Canada）が認定機関となっている。
- 試験機関（testing laboratories）：暗号モジュールの試験を実施する機関である。「CMT（Cryptographic Module Testing）ラボラトリ」と呼ばれ、現在 13 ヵ所（米国 8 ヵ所、カナダ 2 ヵ所、英国 2 ヵ所、ドイツ 1 ヵ所）が認定されている。
- 認証機関（validation authority）：試験機関による試験結果が適正であるか否かを検証し、適正と判断した場合、当該暗号モジュールに対して認証書と認証報告書を発行する機関である。NIST と CSE が認証機関となっている。

本試験・認証の手順は以下のとおりである（図 7 参照、NIST and CSE [2007]）。

1. ベンダーは試験機関を選択し、暗号モジュールとセキュリティ・ポリシー等の必要な資料を提出する。

19 JCMVP では、「セキュリティ・ポリシ」と記述されているが、本稿では金融分野において一般的に利用されている「セキュリティ・ポリシー」という記述を採用する。

図 7　FIPS 140-2 に基づく暗号モジュール試験・認証の枠組み



2. 試験機関は、ベンダーが提出した資料を調査し、不明な点についてはベンダーと調整を行う。
3. 試験機関は、DTR（Derived Test Requirements for FIPS 140-2）[20]に沿って、暗号モジュールが FIPS 140-2 の要件に準拠することを評価し、試験報告書を作成して認証機関に提出する。
4. 認証機関は、試験機関による試験結果が適正であるか否かを判断し、適正であると判断した場合には、暗号モジュール認証書を発行する。また、暗号モジュール認証製品リスト（セキュリティ・ポリシー、暗号モジュール認証書等を含む）を作成し、一般に公開する。
5. 個々の暗号モジュールの利用者は、公開された暗号モジュール認証製品リストを参照し、調達する暗号モジュールを選択することが可能となる。

こうした試験を行う際には、暗号モジュールが承認暗号アルゴリズムを適切に実装しているか否かも試験・認証することが要求されており、暗号アルゴリズム実装試験である CAVP（Cryptographic Algorithm Validation Program）が 1995 年 7 月から NIST と CSE によって運営されている。CAVP では、CMVP と同様に、認証機関を NIST と CSE、CMT ラボラトリを試験機関としており、図 7 と同様の枠組みのもと、次の手順で試験が行われる（NIST and CSE [2007]）。

20 DTR には、暗号モジュールが FIPS 140-2 で規定されたセキュリティ要求事項を満たしているか否かを試験する際に、試験機関が参照しなければいけない試験基準やベンダーが試験機関に提出しなければならない情報等が規定されている。DTR は、ISO/IEC 24759 として国際標準化が進められているほか、2007 年には JIS X 5091 として規格化されている。

1. ベンダーは試験機関を選択する。
2. 試験機関は、暗号アルゴリズムに与えられる入力データ（リクエスト・ファイル）をベンダーに送る。
3. ベンダーは、リクエスト・ファイルを入力として暗号モジュールを動作させ、その出力データ（レスポンス・ファイル）を試験機関に送る。
4. 試験機関もレスポンス・ファイルを作成し、ベンダーから提出されたものとの比較を行う。ベンダーによるテスト結果が正しいことを確認できた場合、レスポンス・ファイルとアルゴリズム情報を認証機関に提出する。
5. 認証機関は、試験機関による試験結果が適正であるか否かを判断し、適正と判断した場合、暗号アルゴリズム確認書を発行する。また、暗号モジュール認証製品リスト（暗号アルゴリズム確認書を含む）を作成し、一般に公開する。
6. 個々の暗号モジュールの利用者は、公開された暗号モジュール製品認証リストを参照し、承認された暗号アルゴリズムが適切に実装されている暗号モジュールを選択することが可能となる。

ロ．わが国の JCMVP

わが国においても、CMVP、CAVP を参考に、JCMVP の運用が 2007 年 4 月から開始された。JCMVP は、電子政府推奨暗号リストに記載されている暗号アルゴリズム等を実装した暗号モジュールを、JIS X 19790: 2007 に基づいて第三者機関が試験・認証する制度である（IPA [2007]）。JCMVP では、現時点において、認定機関を NITE、認証機関を IPA、試験機関を ECSEC としており、現在 5 件の暗号モジュールが認証を取得している。

JCMVP では、CMVP と CAVP においてそれぞれ実施されている試験・認証を同時に実施しており、承認暗号アルゴリズムが適切に実装されているか否か、および、暗号モジュールが JIS X 19790: 2007 に準拠しているか否かが試験される[21]。また、JCMVP における承認暗号アルゴリズムは、CRYPTREC による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が中心となっている。そのため、FIPS 140-2 における承認暗号アルゴリズムのほか、わが国で開発された暗号アルゴリズムが複数含まれている（表 5 参照）。

21 試行運用を実施している FIPS 140-2 に基づく認証も継続しており、認証制度を利用する際は、FIPS 140-2 と JIS X 19790: 2007 のいずれかを選択できるようになっている。

表 5　JCMVP における承認暗号アルゴリズム

技術分類		暗号名称
公開鍵暗号	署名	・DSA （ANSI X9.30 Part1-1997、FIPS 186-2 with Change Notice1）* ・ECDSA（SEC 1） ・RSASSA-PKCS1-v1_5（PKCS#1 v2.1）* ・RSASSA-PSS（PKCS#1 v2.1）*
	守秘	・RSA-OAEP（PKCS#1 v2.1） ・RSAES-PKCS1-v1_5（PKCS#1 v2.1）
	鍵確立	・DH（ANSI X9.42） ・ECDH（SEC 1） ・PSEC-KEM
共通鍵暗号	64 ビットブロック暗号	・CIPHERUNICORN-E ・Hierocrypt-L1 ・MISTY1 ・3-key トリプル DES（SP 800-67）*
	128 ビットブロック暗号	・AES（FIPS 197）* ・Camellia ・CIPHERUNICORN-A ・Hierocrypt-3 ・SC2000
	ストリーム暗号	・MUGI ・MULTI-S01 ・128-bit RC4
その他	ハッシュ関数	・RIPEMD-160 ・Secure Hash Standard〈SHA-1、SHA-224、SHA-256、SHA-384、SHA-512〉（FIPS 180-2 with Change Notice1）*
	メッセージ認証	・HMAC 〈HMAC-SHA-1、HMAC-SHA-224、HMAC-SHA-256、HMAC-SHA-384、HMAC-SHA-512〉（FIPS 198）* ・CMAC（SP 800-38B）*
	擬似乱数生成系	・Pseudorandom Number Generators （ANSI X9.42-2001 Annex C.1、FIPS 186-2 Change Notice1 Appendix 3.1、FIPS 186-2 Change Notice1 revised Appendix 3.1、ISO/IEC 18031〈Hash_DRBG、CTR_DRBG、OFB_DRBG〉）

備考：表中の “*” は、FIPS 140-2 においても承認暗号アルゴリズムとなっているものを示す。

5. 金融分野における第三者評価・認証制度の利用状況と考察

本節では、3、4節において紹介した評価・認証制度がこれまでに金融業界でどのように利用されてきたかを整理するとともに、利用するうえでの留意点について考察する。

(1) CCに基づくセキュリティ評価・認証制度の活用

イ. 金融分野における活用に向けたこれまでの取組み

金融機関がCCに基づく評価・認証制度を活用する方法として、まず、金融分野での利用を想定したPPを参照し、そのPPと整合的なSTおよびTOEを選択する、あるいは、そうしたSTおよびTOEの実現をベンダーに働きかけるという方法が考えられる。PPには、製品・システムに必要とされるセキュリティ機能要件と保証要件を記述することになるが、これらの要件を適切に反映させることが必要であり、金融機関がPPの作成に参画することが求められる。

PPの検討に関しては、各金融機関が自社のセキュリティ・スタンダードに応じて個別に検討するという方向と、金融業界として各社のセキュリティ・スタンダードを包含する汎用的なPPを作成するという方向が考えられる。後者の方向を選択した主な検討事例として、ISO/TC68の取組みと米国のBITS（Banking Industry Technology Secretariat）[22]の取組みが挙げられる。

まず、金融分野における国際標準化を担当するISO/TC68においては、1999年頃から金融業務に適用可能な既存のPPを評価・登録する枠組みに関して検討が行われた経緯がある（宇根・中原［2000］、日本銀行金融研究所［2003］）。最終的には本スキームに関する検討は結実せず中止となってしまったものの、国際レベルでは、早くから金融機関が参照することができるPPを作成しようとする積極的な活動が行われていたといえる。

一方、BITSでは、現在「BITS製品認証制度（BPCP: BITS Product Certification Program）」が運用されている。本制度は、CCを参考にBITSが作成したプロファイル（セキュリティ要件集）に規定されているセキュリティ要件を満たしている製品・システムを認証（BITS Tested Mark）するものであり、当該製品・システムがCCに基づく認証を取得している場合にはその内容をBITSが審査する。CCに基づく認証を取得した製品・システムのうち、金融分野での利用に適していることをBITSが認証というかたちで示しているものといえる。BITSが作成したプロファイルは金融分野に特化したセキュリティ要件を最小限の範囲で規定したもの（マスター・セキュ

22 BITSは、米国の金融業界団体であるFinancial Services Roundtableの下部組織であり、電子商取引の促進を目的として1996年に大手金融機関のCEOらによって設立された非営利団体である。BITSは、金融取引におけるセキュリティを確保するため、BITS製品認証制度の運用や、さまざまなガイドラインの作成を行っている。現在、約100の米国の大手金融機関がメンバーとなっている。

リティ・クライテリアと呼ばれる）であり、そこから派生して、アプリケーション製品（例：電子請求・電子決済システム、ウェブ・ベース取引システム）やネットワーク・セキュリティ製品等を対象とする 6 つの分野のプロファイルが公開されている[23]。それぞれのプロファイルで規定されているセキュリティ要件は、「必須の要件（required）」と「望ましい要件（desired）」に分類されており、必須の要件をすべて満足している場合に認証を取得することができる。また、BITS は、これらのプロファイルを、CC に基づく評価・認証制度で利用する ST や PP を作成するうえで参考にできると述べている（BITS [2004]、Snouffer [2003]）。

これらの事例のほかにも、海外では、金融分野の業界団体が作成した PP はいくつか存在している。例えば、APACS[24]による PIN 入力デバイスの PP（APACS [2003]）や、SCSUG[25]によるクレジットカード業務向け IC カードの PP（SCSUG [2001]）がある。特に、SCSUG による IC カードの PP では、金融機関による運用でのセキュリティ対策が比較的困難な環境を想定したうえで、IC カードへの攻撃に対して能動的に防御するためのセキュリティ機能要件が記述されているなど、汎用的な IC カードの PP と比較すると相対的に高度なセキュリティ・レベルを目指した機能要件となっている（田村・宇根［2007］）。このように、アプリケーションに応じた前提条件やセキュリティ機能要件の選択が行われている。

わが国の場合、全国銀行協会や FISC の資料において CC の活用に関する記述がある。『全銀協 IC キャッシュカード標準仕様』（全国銀行協会［2006］）では、IC キャッシュカード・システムを導入する際に CC（ISO/IEC 15408）を参考にしてセキュリティ対策を進めるよう記述されているほか、FISC による『金融機関等におけるセキュリティポリシー策定のための手引書』（FISC [1999]）では、セキュリティ・ポリシーを策定するうえで、参照することが望ましい国際標準等として CC が挙げられている。このように、わが国の金融分野においても、セキュリティ対策を行ううえで CC を活用することが推奨されているといえる。

ただし、実際に CC に基づくセキュリティ評価・認証制度をわが国の金融機関が利用していることを示唆する公開情報は、筆者が知る限り非常に少ない。JISEC では、これまでに約 140 件の製品・システムが認証されているが、金融関連の製品は 2005 年に認証された『コンビニ・ボックス・バンク業務アプリケーションユニットバージョン 1.0』（三菱電機インフォメーションシステムズ［2005］）のみとなっている（2008 年 4 月現在）。コンビニ・ボックス・バンク業務は、住所・氏名の変更等の各種届出受付や口座開設申込のサービスを提供するものであり、都内のコンビニ

23 各プロファイルは、マスター・セキュリティ・クライテリアに記述されているセキュリティ要件を抜粋したものとなっている。

24 APACS（Association for Payment Clearing Services）は、英国の銀行やクレジットカード会社等の決済サービスを行う機関である。

25 SCSUG（Smart Card Security User Group）は、IC カードのユーザ団体であり、同団体による PP（SCSUG [2001]）が策定された時点でのメンバーは、国際クレジットカード・ブランドの各社、NIST、NSA 等である。

エンス・ストアに設置されている[26]。本業務のシステムを対象にJISECの評価・認証を得たことに関して、東京三菱銀行［2005］には、「社会的信頼を向上させることを目的として第三者評価・認証制度の利用を推進していく」旨の記述がある。

ロ．本制度を利用するうえでの留意点

今後わが国の金融機関がCCに基づく評価・認証制度の活用を検討していくうえで留意すべき点として、主に次の3つの事項が挙げられる。

- **留意点1：EALのみを指標として判断するのではなく、アプリケーションの想定環境やセキュリティ要件と整合的な内容となっているSTおよびTOEを選択する必要がある。**

CCに基づく評価・認証は、STに記述されている前提条件や脅威のもとでTOEのセキュリティ機能要件が充足されていることを保証するものである。したがって、STの記述にない前提条件のもとでは、セキュリティ機能要件が満足されていない可能性がある。金融機関は、STおよびTOEを選択する際に、アプリケーションの想定環境やセキュリティ要件と整合的なSTであることを確認する必要がある。例えば、2節（1）において紹介した手順に沿って安全対策を講じる場合、自社のセキュリティ・スタンダードの内容からセキュリティ機能要件等を導出し、それらと合致するSTを選択する必要がある。

また、STに記述されるセキュリティ保証レベルEALは、STが主張するセキュリティ機能の実装の確からしさをどの程度広範囲に検査したかを示すものであり、セキュリティ・レベルと密接な関連性があるともいえることから、アプリケーションに応じてEALを選択するという方法もある[27]。しかし、TOEのセキュリティ・レベルがEALのみによって決定されると誤解してしまう可能性もある。実際には、EALだけではなく、セキュリティ機能要件もTOEのセキュリティ・レベルを大きく左右する要素である。こうしたことから、STの内容を確認する際にはセキュリティ機能要件にも注目することが重要である。

- **留意点2：TOEを構成する可能性のある要素技術のなかには、もともと評価の対象となっていない、あるいは、評価が技術的に困難なものが存在し、そうした要素技術については別途評価する必要がある。**

CCに基づく評価・認証の枠組みでは、TOEに搭載される暗号アルゴリズムや暗

26 本システムは、口座番号と暗証番号を暗号化してRFIDに格納し、ユーザが記入した申込書に貼付するものである。TOEは、アプリケーション・ソフトウエアとハードウエア・セキュリティ・モジュールであり、ユーザとのインターフェースや通信路は含まれない。何らかの事故等によって申込書が第三者に盗取されRFIDのデータが読み取られた場合の暗証番号の漏洩を脅威として想定している。

27 一般に、EAL1～4までは商用システム・製品が備えるべきレベル、EAL5以上は軍事用あるいはそれに準じる用途向きとされている。金融等の高度なセキュリティを必要とする分野においては、EAL5以上を適用することが望ましいとの見方もある（遠藤［2000］）。

号プロトコル等の暗号要素技術のセキュリティ評価は対象外とされている。そのため、暗号要素技術自体が本当に十分な安全性を有しているか否かについては、別途評価が必要である。安全性の評価が行われている暗号アルゴリズムとしては、例えばCRYPTREC による電子政府推奨暗号（総務省・経済産業省［2003］）があり、こうした暗号アルゴリズムが利用されている製品・システムを調達の候補とすることが考えられる。4 節で説明した CMVP や JCMVP による認証を取得した暗号モジュールを利用するのも一案であろう（Snouffer [2003]）。

また、研究途上でありセキュリティ評価手法が確立していない技術が TOE に組み込まれている場合、評価が十分に行われていることを確認困難なケースも想定される。例えば、生体認証システムについては、既にいくつかの PP が存在するほか、BEM[28]（CCBEMWG [2002]）や ISO/IEC CD 19792[29]の策定を通じて CC に基づく評価・認証への適用に向けた検討が進められている。ただし、生体認証技術のセキュリティ評価手法の研究自体が遅れており、評価手法が確立していないのが実情である（松本・宇根［2007］、JAISA [2007]）。こうした技術が組み込まれた製品・システムを評価する際には、仮に、当該技術の効果が損なわれたとしても、製品・システムとして、あるいは、アプリケーション全体として適切にカバーされることを別途確認するなどの対応が重要であろう。

- **留意点 3：CC に基づく認証には有効期間が明示的に設定されていないことから、金融機関は、当該認証を得た製品・システムのセキュリティ機能が陳腐化していないことを別途確認する必要がある。**

情報技術の研究開発のスピードは速く、情報セキュリティ技術への攻撃手法の研究も同様であるため、一般に、ある時点で提案された情報セキュリティ技術の効果はその後時間の経過とともに低下していく。したがって、ある時点の評価によって適切なセキュリティ・レベルを確保していることを確認できたとしても、そうした確認がそれ以降も正しいという保証はない。CC に基づく認証が得られた製品・システムであっても、そのセキュリティ機能の有効性は徐々に低下し、やがては、要求されるセキュリティ・レベルを確保できなくなる可能性がある。現状では CC に基づく認証には有効期間が明示的に設定されていないことをあわせて考えると、たとえ認証を得られている製品・システムであっても、そのセキュリティ機能が陳腐化していないことを別途確認することが求められる。

これらの留意点を踏まえると、第三者の専門家の評価や試験を受けるとしても、そうした枠組みを有効に活用するためには、情報セキュリティ技術の動向を金融機関

28 BEM（Biometric Evaluation Methodology）は、CC の枠組みに基づいて生体認証システムのセキュリティ評価を行う際に留意すべき脅威やセキュリティ保証要件等を規定するものであり、CCBEMWG（Common Criteria Biometric Evaluation Methodology Working Group）によって策定されている。

29 ISO/IEC CD 19792 は、CC の枠組みに基づき、生体認証システムの安全性評価を行う際の枠組みや、安全性評価を行う際に評価者やシステム開発者に求められる条件等を規定するものである。ISO/IEC JTC1/SC27/WG3 において国際標準化に関する審議が行われている。

自らも十分に把握しておくことが重要であるといえる。米国の FSTC[30]や BITS のように、金融機関やベンダーが協力して情報技術の動向を把握し情報共有を進めることも一案であろう。また、BITS の PP 等を参考にしながら、わが国金融業界の PP を準備するという対応の有効性について今後研究を行うことも有用であると考えられる。

(2) FIPS 140-2 に基づく暗号モジュール試験・認証制度の活用

イ．金融分野における活用に向けたこれまでの取組み

金融分野においては、金融機関が PKI における認証局を運営する際に、署名生成鍵を生成・格納するデバイスへのセキュリティ要件として FIPS 140 シリーズを参照しているケースが多い。

ISO/TC68 傘下の国際標準である ISO 15782-1（ISO [2003]）[31]では、認証局が利用する暗号モジュールのセキュリティ要件として FIPS 140-2 が引用されている。そのうえで、認証局の署名生成鍵の生成・格納には、少なくともセキュリティ・レベル 3 以上の暗号モジュールを利用することとされている。また、IdenTrust[32]は、証明書ポリシー（IdenTrust [2006]）において、署名生成鍵を生成・格納するデバイスのセキュリティ要件について FIPS 140-1 および FIPS 140-2 を引用しており、HSM（hardware security module）であればレベル 3、IC カードであればレベル 2 相当のセキュリティ水準を確保することとしている。

そのほか、BITS によるプロファイル（本節（1）イ．参照）では、暗号アルゴリズムに利用する秘密鍵の破棄方法として FIPS 140-2 が参照されている。また、金融機関が CMVP による認証を取得した事例としては、ボストン連邦準備銀行と米財務省によるストアドバリュー型の電子マネーに利用する暗号モジュール（FRB of Boston and US Treasury [2006]）が挙げられる。

わが国においても、銀行に対する公開鍵証明書（IC キャッシュカード向け）を発行している全銀協認証局では、その署名生成鍵を格納する装置のセキュリティ要件として FIPS 140-1 が参照されている。すなわち、当該装置について、「FIPS 140-1 レベル 4（最高位）相当の機能を備えた耐タンパー装置である HSM を用いている」と全国銀行協会［2002］において説明されている。また、全銀協 IC キャッシュカード標準仕様に準拠した IC カード認証向けのソリューションとして、FIPS 140-2 に

30 FSTC（Financial Services Technology Consortium）は、金融業界で利用可能な重要インフラの公開技術標準を作成することを目的として 1993 年に設立された団体である。現在、約 100 以上の金融機関、ベンダー、研究組織、政府機関がメンバーとなっている。

31 ISO 15782 シリーズは、金融機関が PKI を構築し、認証機関を運営する場合の公開鍵証明書の管理方法について規定する国際標準であり、パート 1 である ISO 15782-1 では公開鍵証明書のライフサイクルやフォーマットが規定されている。

32 IdenTrust は、1999 年に米シティグループ、ABN AMRO 等によって設立された会社であり、主に加盟金融機関のルート認証局の運営を行っている。

おけるセキュリティ・レベル 4 適合の認証を受けた暗号モジュールを組み込んだ製品も提供され始めている（例えば、日本 IBM［2007］）。このように、わが国の金融業界でも、従来から FIPS 140 シリーズや CMVP に関心が向けられていたといえる。

ロ．本制度を利用するうえでの留意点

今後金融機関が CMVP や JCMVP を活用する際には、CC に基づく評価・認証に関する留意点 1、3 の事項について同様に留意することが必要である。留意点 1 に関しては、自社のセキュリティ・スタンダードと整合的なセキュリティ・ポリシーを有する暗号モジュールを選択することが求められる。

これらに加えて、次のような点にも留意する必要があろう。

- 留意点 4：現在金融分野で広く利用されている仕様の RSA、2-key トリプル DES の暗号モジュールについては、現行の JCMVP における試験の対象外である。また、2-key トリプル DES、SHA-1 については、CMVP においては現時点では対象となるものの、これらの暗号アルゴリズムに対する NIST のお墨付きの廃止（2010 年末）後は数年で認証取消しに至る見通しとなっており、現行の暗号アルゴリズムに代わって中長期的に利用する暗号アルゴリズムの選定を行う必要がある。

全銀協 IC キャッシュカード標準仕様では、公開鍵として RSA、共通鍵暗号として 2-key トリプル DES、ハッシュ関数として SHA-1 の使用を推奨しており、わが国の金融機関はこれらの暗号アルゴリズムを利用しているとみられる。一方、JCMVP では、電子政府推奨暗号リストに記載されている暗号アルゴリズムを中心に承認暗号アルゴリズムを選定している。このため、電子政府推奨暗号リストに記載されていない 2-key トリプル DES ベースのメッセージ認証子や、承認されていない仕様による RSA[33]を実装した暗号モジュールは、JCMVP による試験を受けることができないことになる。

米国やカナダで運用されている CMVP においては、2-key トリプル DES や SHA-1 が承認暗号アルゴリズムとなっており、これらを実装した暗号モジュールの試験・認証を受けることができる。ただし、2-key トリプル DES や SHA-1 は、2010 年末で NIST による米国連邦政府標準暗号としての認定を失う公算が高く（Une and Kanda [2007]）、一定の移行期間の後、CMVP における承認暗号アルゴリズムからも削除される見通しとなっている[34]。こうしたことから、これらの暗号アルゴリズムを実装

33 EMV 仕様や全銀協 IC キャッシュカード標準仕様では、独自のメッセージ認証子生成方式や RSA パディング・ルールが記述されている（鈴木・神田［2007］）。

34 FIPS 46-3 に記載されているシングル DES は、CMVP の承認暗号アルゴリズムであったが、シングル DES の安全性低下による FIPS 46-3 の廃止を受けて、2005 年 5 月に「DES 移行計画」が発表された（NIST [2005]）。本計画では、①シングル DES を実装した暗号モジュールの認証を 2005 年 5 月で中止する、②2007 年 5 月までを暗号アルゴリズムの移行期間とし、より安全性の高いアルゴリズムへの移行を促す、③シングル DES を実装している認証済み暗号モジュールについては、その認証の有効期間を移行期間終了となる 2007 年 5 月までとする、④2007 年 5 月にシングル DES を FIPS 140-2 の承認暗号アルゴリズ

した暗号モジュールは、認証の期間が数年程度に限定されてしまうとみられる。

こうした事情により、わが国の金融機関は、現在広く使われている暗号アルゴリズムを使い続ける場合、CMVP や JCMVP における暗号モジュールの試験・認証を有効に活用することが難しいのが実情である。まずは、中長期的に十分なセキュリティ・レベルを確保できると評価されている暗号アルゴリズムのなかから金融業務に利用するのに相応しいものを選択することが必要であろう。その際に、CMVP や JCMVP において現在承認暗号アルゴリズムとなっているものを候補として位置付けることが考えられる。

- **留意点５：暗号モジュールへの物理的な攻撃に関するセキュリティ要求事項が明確になっていない部分があり、セキュリティ評価の手法も十分確立していないことから、そうした攻撃への対応を別途検討する必要がある。**

サイドチャネル攻撃や故障利用攻撃等の物理的な攻撃に関しては、FIPS 140-2 においては具体的なセキュリティ要求事項が規定されておらず、「これらの攻撃への対策が暗号モジュールに適用されている場合には、暗号モジュールのセキュリティ・ポリシーにその対策を記述すること」とされているのみである。このため、サイドチャネル攻撃が脅威となる IC カードのような暗号モジュールの認証結果を参照する際には、同攻撃の手法や対策技術をフォローしたうえで、当該モジュールのセキュリティ・ポリシーに適切な対策が記述されているか否かを確認する必要がある。また、サイドチャネル攻撃に限らず、暗号モジュールに対する新たな攻撃手法が提案されることも十分に考えられるため、金融機関はそうした動向も把握しておくことが必要である。

現在ドラフトが公開されている FIPS 140-3 においては、サイドチャネル攻撃のうち、タイミング攻撃、電力攻撃、電磁波攻撃が試験対象に規定されている。特に最高位のセキュリティ・レベル 5 においては、これらすべての攻撃を想定した試験が行われるかたちとなっている。このような物理的な攻撃に関しては、学会における研究発表の足元の動向をみると、基本的にはアドホックなセキュリティ評価が中心であり、体系的なセキュリティ評価手法の確立には今後の研究開発の進展を待つ必要がある（Macé, Standaert, and Quisquater [2007]）。こうしたことから、金融機関は、サイドチャネル攻撃に関する試験がどのように行われるかについて状況を把握しておくとともに、別の対策（運用も含む）についてもあらかじめ考慮しておくことが望ましいと考えられる。

ムから削除することとされた。実際に表 4 に示したように、シングル DES は承認暗号アルゴリズムから削除された。

6. おわりに

オープンなネットワーク等を活用した金融サービスの多様化に伴い、金融機関の情報システムが複雑なものになってきている。さらに、各種のセキュリティ上の脅威に対抗するために、高度な情報セキュリティ技術が組み込まれていることも、金融機関の情報システムの複雑化に拍車をかけているといえる。その結果、当該情報システムのセキュリティを適切に評価することが容易でなくなってきている。

こうした問題に対応する方法の1つとして、わが国において近年整備されてきたJISECやJCMVPによる情報セキュリティ製品・システムの第三者評価・認証制度を活用することが考えられる。こうした制度を利用するメリットとしては、(A)金融機関が自ら評価者を審査・選定するための手間や労力を削減可能である、(B)認証機関による評価結果への「お墨付き」によって、評価対象の製品・システムのセキュリティに関する信頼をアピールしやすい、(C)海外でも運用されていることから、海外の顧客等にも認証結果に対する理解を得られやすいといった点が挙げられる。

ただし、こうした制度を適切に利用していくうえで、いくつか留意すべき点が存在する。例えば、①評価・認証の内容が金融のアプリケーションの想定環境やセキュリティ要件と整合的であることを確認する必要がある、②評価対象外の要素技術や評価が事実上困難な要素技術については別途評価する必要がある、③認証の有効期間が明示的に設定されておらず、セキュリティ機能が陳腐化していないことを別途確認する必要があるといった項目が挙げられる。

JISECやJCMVPといった制度が金融業務向けの情報システムにおけるセキュリティ評価にとって実際どの程度効果的なのかについては、当該アプリケーションの内容に応じて考慮し、判断していくことになろう。そうした際には、上記のようなメリットや留意点を考慮しつつ、検討することが必要である。こうした第三者によるセキュリティ評価・認証制度の効果について、実際の評価事例等も参照しつつ、今後検討を深めていくことはわが国の金融業界における重要な課題であろう。

参考文献

植村泰佳、『CC と FIPS 140-2 の比較と活用法（第 1 回）』、ECSEC、2005 年 a
（http://www.ecsec.jp/library/pdf/CC&FIPS140-2.pdf）
――、『CC と FIPS 140-2 の比較と活用法（第 2 回）』、ECSEC、2005 年 b
（http://www.ecsec.jp/library/pdf/CC&FIPS140-2-2.pdf）
宇根正志・中原慎一、「最近の金融業務における情報セキュリティ評価・認定を巡る動向について」、『金融研究』第 19 巻別冊第 1 号、日本銀行金融研究所、2000 年、193～238 頁
遠藤文夫、「情報セキュリティ評価基準について」、『郵政研究所月報』2000 年 4 月号、郵政省郵政研究所、2000 年
金融庁、『金融検査マニュアル（預金等受入金融機関に係る検査マニュアル）』、金融庁、2007 年
財団法人金融情報システムセンター（FISC）、『金融機関等におけるセキュリティポリシー策定のための手引書』、FISC、1999 年
――、『金融機関等コンピュータシステムの安全対策基準・解説書第 7 版』、FISC、2006 年
――、「ISO 等の標準規格の動向と金融機関における活用事例」、『金融情報システム』No. 290、FISC、2007 年、50～69 頁
財団法人日本情報処理開発協会（JIPDEC）、『情報セキュリティマネジメントシステム適合性評価制度の概要』、JIPDEC、2007 年
（http://www.isms.jipdec.jp/doc/ismspanf.pdf）
社団法人日本自動認識システム協会（JAISA）、『バイオメトリクス・セキュリティ・コンソーシアム安全ワーキング・グループ平成 18 年度活動報告書』、JAISA、2007 年
情報処理振興事業協会（IPA）・通信・放送機構（TAO）、『暗号技術評価報告書（2002 年度版）CRYPTREC Report 2002』、IPA・TAO、2003 年
鈴木雅貴・神田雅透、「IC カードに利用される暗号アルゴリズムの安全性について：EMV 仕様の実装上の問題点を中心に」、『金融研究』第 26 巻別冊第 1 号、日本銀行金融研究所、2007 年、31～52 頁
全国銀行協会、『全銀協 IC キャッシュカード標準仕様（第 2 版）』、全国銀行協会、2006 年
――、『全銀協認証局について』、全国銀行協会、2002 年
総務省・経済産業省、『電子政府推奨暗号リスト』、総務省・経済産業省、2003 年
田村裕子・宇根正志、「IC カードを利用した本人認証システムにおけるセキュリティ対策技術とその検討課題」、『金融研究』第 26 巻別冊第 1 号、日本銀行金融研究所、2007 年、53～100 頁
電子商取引安全技術研究組合（ECSEC）、『「システム LSI チップのセキュリティ評価」に関する調査研究報告書』、経済産業省、2004 年
東京三菱銀行、『CSR レポート 2005』、東京三菱銀行、2005 年

（http://www.bk.mufg.jp/minasama/csr/pdf/syosai.pdf）
特定非営利活動法人日本セキュリティ監査協会（JASA）、『JASA パンフレット―公正かつ公平な情報セキュリティ監査を目指して―』、2006 年
（http://www.jasa.jp/download/downf/JASA_Profile.pdf）
―――、『情報セキュリティ監査制度 知って得する情報セキュリティ講座』、2007 年
（http://www.jasa.jp/lamsa/jyoho.html）
独立行政法人情報処理推進機構（IPA）、『暗号モジュール試験及び認証制度』、IPA、2007 年
（http://www.ipa.go.jp/security/jcmvp/documents/open/jcmvp_pamphlet071019.pdf）
―――、『ISO/IEC 15408 のセキュリティ評価・認証』、IPA、2006 年
独立行政法人情報処理推進機構セキュリティセンター、『セキュリティ評価・認証の動向』、IPA、2003 年
（http://www.ipa.go.jp/security/ccj/cc_tutorial/cc_history/cc_history.html）
独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室、『セキュリティ評価のためのコモンクライテリア　パート 1：概説と一般モデル バージョン 3.1 改訂第 1 版』、IPA、2007 年 a
―――、『セキュリティ評価のためのコモンクライテリア　パート 2：セキュリティ機能コンポーネント バージョン 3.1 改訂第 1 版』、IPA、2007 年 b
―――、『セキュリティ評価のためのコモンクライテリア　パート 3：セキュリティ保証コンポーネント バージョン 3.1 改訂第 1 版』、IPA、2007 年 c
日本アイ・ビー・エム（IBM）株式会社、『IC キャッシュカード取引におけるセキュリティー強化の実現』、日本 IBM、2007 年
（http://www-06.obm.com/jp/finance/solutions/fsn/jun2007_ic.html）
日本銀行金融機構局、『リスク管理と金融機関経営に関する調査論文―事例からみたコンピュータ・システム・リスク管理の具体策』、日本銀行金融機構局、2007 年
日本銀行金融研究所、『ISO/TC68/SC2-SC6 国内検討委員会議事録（平成 15 年 12 月 8 日）』、日本銀行金融研究所、2003 年
日本工業標準調査会（JISC）、『JIS X 5070-1:2000 セキュリティ技術―情報技術セキュリティの評価基準―第 1 部：総則及び一般モデル』、財団法人日本規格協会（JSA）、2000 年 a
―――、『JIS X 5070-2:2000 セキュリティ技術―情報技術セキュリティの評価基準―第 2 部：セキュリティ機能要件』、JSA、2000 年 b
―――、『JIS X 5070-3:2000 セキュリティ技術―情報技術セキュリティの評価基準―第 3 部：セキュリティ保証要件』、JSA、2000 年 c
松本　勉・宇根正志、「バイオメトリクス認証の実用におけるぜい弱性と対策」、『電子情報通信学会誌』第 90 巻第 12 号、電子情報通信学会、2007 年、1051～1055 頁
三菱電機インフォメーションシステムズ株式会社（MDIS）、『コンビニ・ボックス・バンク業務アプリケーションユニットセキュリティターゲットバージョン 1.0』、MDIS、2005 年

Association for Payment Clearing Services (APACS), *PIN Entry Device Protection Profile Ver. 1.37*, APACS, 2003.

Banking Industry Technology Secretariat (BITS), *BITS Product Certification Program (BPCP) Frequently Asked Questions (includes Common Criteria Alignment)*, BITS, 2004.

Common Criteria Biometric Evaluation Methodology Working Group (CCBEMWG), *Common Methodology for Information Technology Security Evaluation—Biometric Evaluation Methodology Supplement Version 1.0*, CCBEMWG, 2002 (http://www.cesg.gov.uk/site/ast/biometrics/media/BEM_10.pdf).

Common Criteria Maintenance Board (CCMB), *Common Criteria for Information Technology Security Evaluation—Part 1: Introduction and general model Version 3.1, Revision 1*, CCMB, 2006.

———, *Common Criteria for Information Technology Security Evaluation—Part 2: Security functional components Version 3.1, Revision 2*, CCMB, 2007a.

———, *Common Criteria for Information Technology Security Evaluation—Part 3: Security assurance components Version 3.1, Revision 2*, CCMB, 2007b.

EMVCo, *EMV Security Guidelines: EMVCo Security Evaluation Process*, EMVCo, 2006.

IdenTrust, *Identity Certificate Policy [IP-ICP], Operating Rules and System Documentation Release 3.1a*, IdenTrust, 2006.

International Organization for Standardization (ISO), *ISO 15782-1, Certificate management for financial services—Part 1: Public key certificates*, ISO, 2003.

———, and International Electrotechnical Commission (IEC), *ISO/IEC 15408-1: 2005, Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model*, ISO, 2005a.

———, and ———, *ISO/IEC 15408-2: 2005, Information technology—Security techniques—Evaluation criteria for IT security—Part 2: Security functional requirements*, ISO, 2005b.

———, and ———, *ISO/IEC 15408-3: 2005, Information technology—Security techniques—Evaluation criteria for IT security—Part 3: Security assurance requirements*, ISO, 2005c.

———, and ———, *ISO/IEC 19790: 2006, Information technology—Security techniques—Security requirements for cryptographic modules*, ISO, 2006.

Federal Reserve Bank (FRB) of Boston and US Treasury, *FRBB ePurse v2on ActivCard Applet v2 on Cyberflex Access 64k v1, FIPS 140-2 Level2 Cryptographic Module Security Policy Revision 1.6*, FRB of Boston and US Treasury, 2006.

Macé, François, François-Xavier Standaert, and Jean-Jacques Quisquater, "Information Theoretic Evaluation of Side-Channel Resistant Logic Styles," *Proceedings of CHES 2007*, LNCS4727, Springer-Verlag, September 2007, pp. 427–442.

National Institute of Standards and Technology (NIST), *DES Transition Plan*, NIST, 2005 (http://csrc.nist.gov/groups/STM/common_documents/DESTranPlan.pdf).

———, *Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Module*, NIST, 2001.

———, *Federal Information Processing Standards Publication 140-3 (DRAFT), Security Requirements for Cryptographic Module*, NIST, 2007.

———, and Communications Security Establishment (CSE), *Frequently Asked Questions for the Cryptographic Module Validation Program*, NIST, 2007.

Snouffer, Ray, *The Security Testing and Metrics Group: CMVP, NIAP, and C&A*, NIST, 2003 (http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2003-12/Snouffer_Dec_2003.pdf).

Smart Card Security User Group (SCSUG), *Smart Card Security User Group Smart Card Protection Profile (SCSUG-SCPP), Version 3.0*, SCSUG, 2001.

Une, Masashi, and Masayuki Kanda, "Year 2010 Issues on Cryptographic Algorithm," *Monetary and Economic Studies*, Vol. 25, No. 1, Institute for Monetary and Economic Studies, Bank of Japan, 2007, pp. 129–164.

VISA, *Chip Card Products—Testing and Approval Requirements, Version 1.0*, VISA, 2007.