電子政府推奨暗号と暗号モジュール認証制度

今井秀樹（中央大学） 山岸篤弘（IPA）

概要 2000 年から始まった我が国電子政府システム向けの暗号技術評価プロジェクトである CRYPTREC の活動概要，CRYPTREC の成果を活用するための暗号モジュール試験及び認証制度を概説し，これらの活動と標準化活動との関連について述べる．

1. はじめに

我々の身の回りには，携帯電話，スマートフォン，電子商取引，デジタル放送といった情報を扱うシステムや，高速道路での自動料金収受システム（Electronic Toll Collection (ETC)システム），交通系 IC カードシステムや少額決済の電子マネーシステムなどが，身近に利用されるている．これらのシステムでは，不正利用への対応，個人情報保護や通信の秘密の確保の目的で暗号技術が多用されている．逆に，暗号技術の利用なしにはシステムとして成立しない状況にあると言っても過言ではない．暗号技術で最も重要なことは，その安全性である．即ち，安全性を評価することが，暗号技術を利用するシステムの安全性の根幹をなすと言える．そこで，本稿では我が国での暗号技術の安全性評価プロジェクトである CRYPTREC[1]プロジェクトと CRYPTREC を構成した各委員会の活動と国際標準化活動が，我が国の暗号応用製品の市場開拓にどう貢献したかについて考察する．さらには，暗号技術を利用した暗号モジュール製品の試験及び認証制度の成立過程を紹介する．

2. CRYPTREC 以前

2.1 暗号アルゴリズム研究の再開

我が国での暗号技術に関する研究開発活動は，第二次世界大戦後，防衛・外交・警察といった特定分野で細々と維持されている状況であった．しかし，1970 年代に入り米国での DES(Data Encryption Standard)暗号の公表，Diffie と Hellman による公開鍵暗号原理[1]と公開鍵暗号の一つである RSA 暗号[2]の（再）発見[2]を契機として，第 2 次世界大戦の終結と共に停止した我が国での暗号技術に関するアカデミックな活動が再開された．1982 年の松本等による「明るい暗号研究会」，1983 年の暗号情報セキュリティシンポジウム(SCIS)や 1988 年の電子情報通信学会情報セキュリティ研究専門委員会（ISEC 研究会）の創設は，このアカデミックな活動の活発化を象徴する出来事であった．

1990 年代に入ると Internet の商用化，Internet 接続可能な PC(Windows95-PC)の普及が進み，暗号技術を用いた電子商取引システムやデジタルコンテンツ著作権管理(Digital Rights Management)システム等の研究開発が活発化した．しかし，暗号技術は，デュアル・ユース（軍民共用）技術であるため，対共産圏輸出統制委員会(COCOM)やその一部機能を引き継いだ「通常兵器及び関連汎用品・技術の輸出管理に関するワッセナー・アレンジメント[3]」（通称：ワッセナー協約）においての輸出規制対象品目（技術）となっている．そのため，米国で一般的に利用されていた DES 暗号や RSA 暗号を利用するためには極めて強い制約が存在し，我が国のアカデミア，産業界の両方で自由に利用できる国産暗号アルゴリズムの開発を目指し，暗号アルゴリズムの研究開発が一気に活発化した．

2.2 安全性評価への取り組み

1990 年代には，各研究機関から数多くの暗号アルゴリズムが提案された．更に，それらの暗号の安全性を評価するために，解読（攻撃）が繰り返された．このような暗号解読（暗号解析）の重要性は共通鍵暗号で顕著に表れた．1990 年の CRYPTO’90 で，Biham と Shamir によって提案された差分解読法（Differential Cryptanalysis）[3]は， 1977 年に米国標準暗号として制定された DES 暗号の解読可能性を示唆し，暗号解析（暗号アルゴリズムの安全性評価）の研究に大きな影響を与えた． 暗号アルゴリズムの安全性評価を行う上で，統計学的な安全性評価だけでは不十分であり，暗号解読の立場からの安全性評価が重要であることが明らかとなったのである．

1993 年には松井が線形解読法[4]を提案し， 1994 年には解読に必要なデータ量が現実的とは言えないものの，

[1] Cryptography Research and Evaluation Committees の略．電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討するプロジェクト．

[2] 1997 年になって，公開鍵暗号の原理は 1969 年に James Ellis（英国），RSA 暗号は 1973 年に Clifford Cocks（英国）により，それぞれ発見されていたことがわかった．

[3] The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies

DES 暗号解読に世界で初めて成功した[5,6]．差分解読法と線形解読法は，ブロック暗号の安全性を評価するための有力な指標となっていった．現在でも，それぞれの解読法に対する平均確率，特性確率でブロック暗号の安全性を評価することが一般的に行われている．

このような暗号解読技術の進歩を受け，我が国でも安全性評価を組織的に行う動きが始まった．1995 年に通信・放送機構(TAO[4])では，横浜リサーチセンター(YRC, Yokohama Research Center)を開設し，辻井中央大教授（当時：現中央大学研究開発機構教授）を中心に，大学や企業から研究者を招集し，暗号アルゴリズムの数学的安全性に関する調査研究を開始した．YRC は 5 年間の時限機関であったが，2000 年には，「共通鍵ブロック暗号の選択/設計/評価に関するドキュメント」（通称：ブロック暗号ガイドブック）が作成された[7]． また，政府側でも，郵政省が「暗号の在り方に関する研究会」を組織し，暗号技術の健全な発展を進めるための検討を開始した．

2.3 実用化への動き

1990 年代に入ると学術的な進歩だけでなく，商用 Internet 環境の出現を背景に暗号技術の応用に対する動きも活発化してくる．公衆交換電話網経由であれば回線接続時に通信先を特定することができたが，Internet 経由の場合，接続先を特定することは容易ではない．つまり，ネットワーク上で利用者が相互に相手を確認（認証）する仕組みや安全に通信を行う仕組みが必要となり，公開鍵暗号技術を利用した公開鍵暗号基盤 PKI(Public Key Infrastructure)が提案された．PKI の基本的な原理は，利用者の公開鍵の正当性を証明する認証書(Digital Certificate)を信頼できる第三者機関としての認証機関 CA(Certification Authority)が発行し，それを信頼の根拠として，利用者相互の認証(Authentication)を行うことにある．また，安全に通信を行う仕組みとしては，PKI を用いて共通鍵暗号の鍵共有を行う SSL(Secure Socket Layer)や暗号メール S/MIME などが開発された．

ネットワークだけでなく，日常生活の中でも暗号技術の利用が始まった．具体的にいえば，交通システムと携帯電話システムの分野である．特に，交通システム分野の一つである ETC システムでは，限定的な形ではあったが暗号技術を含めて方式の選定が行われた．しかし，ETC システムでの暗号技術の選定経緯は，電子政府システムの構築時に調達システム毎に暗号選定のための提案活動や選定活動が生じ得ることを暗示し，電子政府システムの構築時に，混乱が生じることが懸念された．このような事態を回避し，電子政府で安全な暗号技術を容易に利用できるようにするため電子政府推奨暗号リストの作成が企画された．

3. 電子政府推奨暗号リスト

政府機関における暗号技術の利用に関しては，米国連邦政府の様にオープンな政府標準を定めた上で政府機関にそれに従うことを強制する場合と英国政府の様に政府への納入を希望するベンダのみに情報を開示する場合とに大別できる．まず，両国の制度を概観した後，我が国の取り組みを紹介する．

3.1 米国での政府標準暗号

米国連邦政府では，標準技術研究所(NIST, National Institute of Standards and Technology)にて，連邦政府で利用する情報セキュリティ技術の標準を制定することが法律で定められている．

NIST が 1976 年に FIPS(Federal Information Processing Standard) -46 として制定した DES 暗号や 2001 年に DES 暗号の後継暗号として制定した FIPS-197 AES(Advanced Encryption Standard)がその例である．特に，AES の選定時には，各国から 21 方式の暗号アルゴリズムが提案され，最終的にベルギーから提案された RIJNDAEL が選出された．この選考の過程では，各国の研究者から評価論文が CRYPTO 等の国際学会へ投稿されたり，NIST が主催した 1997 年のプレ AES 候補コンファレンスを含め 4 回の学術会議が開催されたりした[8]．暗号アルゴリズムの安全性の評価を多くの専門家が参加する公開の場で行うという AES 選考の方法は，我が国における暗号技術の安全性評価に大きな影響を与えただけでなく，現在 NIST が行っている次期ハッシュ関数の開発にも継承されている．

3.2 英国での政府用暗号

英国では政府機関で利用する暗号技術には，英国政府通信本部(GCHQ[5])の傘下にある通信電子セキュリティグループ(CESG[6])の管轄下にある．CESG では，米 NIST とは異なり，英国政府機関で使用する暗号のアルゴリズムを公開していない．そのため，CESG では CAPS[7]と呼ばれる制度を運用している[9]．CAPS では，英国政府機関へ暗号組込製品の納入を希望する企業に対して，英国

[4] Telecommunications Advancement Organization of Japan

[5] Government Communications Headquarter
[6] Communications-Electronics Security Group
[7] CESG Assisted Products Service

政府機関向けの暗号アルゴリズムを開示することを含めた支援を行っている. CAPS に従って製造された製品は, CESG による認証を得たことになるため，企業にとっては政府向けの市場へのアクセス機会が増えることになる. 更に，CESG は 2002 年に CAPS に加えて，米国とカナダが運用している暗号モジュール試験及び認証制度(CMVP, Cryptographic Module Validation Program)への参加も表明した.

3.3 電子政府推奨暗号リスト

3.3.1 2000 年度の活動概要

2000 年に我が国政府は, 2003 年度に電子政府システムの構築を目指すことを宣言した．電子政府システムでは，機密性の確保，アクセス制御，データ完全性といったセキュリティ機能を実現する必要がある．それまで我が国での政府用の暗号に関する標準は検討されてこなかった. そのため，1999 年から開催された郵政省の「暗号の在り方研究会」や情報処理振興事業協会(IPA)の研究[10]では，電子政府システムの構築を行う際には，使用する暗号アルゴリズムは，安全性評価に基づき選定を行うべきことが指摘されていた.

そこで，2000 年 4 月に情報処理振興事業協会（当時）セキュリティセンターでは，暗号技術評価委員会(CRYPTREC)を立ち上げ，電子政府システムで使用される暗号技術の安全性評価と選定作業に着手した．第一回の暗号技術評価委員会では, 米国の AES の選定プロセスに範をとり，電子政府向けの暗号技術を広く公募することとし，2002 年度完成を目指して「安全性が一定水準以上であり，10 年間は安心して利用できる暗号アルゴリズムのリスト」を作成することとなった.

公募に対する応募暗号アルゴリズムについては, まず, 仕様書等の提出書類の審査を行い，暗号アルゴリズム評価のために十分な情報が提出されているか，また，暗号解読に直結する明らかな欠陥が有るかを審査することになった．この審査を通過した暗号アルゴリズムは，暗号解読の観点から安全性の評価が実施されることとなった[11].

そのため，暗号技術評価委員会の下に，「共通鍵暗号技術評価委員会（委員長 : 金子東京理科大教授）」と「公開鍵暗号評価委員会（委員長 : 松本横浜国立大学教授）」を設置し，国内の大学および企業で暗号の研究に携わっている研究者を委員として招聘した．共通鍵暗号技術評価委員会では，共通鍵暗号（ブロック暗号，ストリーム暗号）のほかハッシュ関数，擬似乱数生成器の評価も実施することとなった．公開鍵暗号技術評価委員会では，署名用途だけでなく，鍵共有，守秘，認証の用途で使用する公開鍵暗号技術の評価を担当することとなった.

この第一回暗号技術評価委員会の審議結果を受け，共通鍵暗号技術評価委員会と公開鍵暗号技術評価委員会のそれぞれで具体的な公募条件を審議し，2000 年 6 月から 7 月の 1 ヶ月間提案を受け付けた．その結果，47 件の暗号アルゴリズムが提案された．スクリーニング評価と詳細評価の結果，34 件の提案が安全性の推移状態を監視する対象（「監視状態」）となり，2001 年度以降にも詳細な分析を継続することとなった.

3.3.2 2001 年度の活動概要[12,13,14]

2001 年度に入ると通信・放送機構[8](TAO)（当時）も暗号技術評価委員会の運営事務局となり, CRYPTREC は名実共に日本における暗号技術の唯一の安全性評価の拠点となった．更に，欧州における暗号技術の安全性評価プロジェクトである NESSIE[9]との情報交換を行うなどの活動も行われた．しかし，2000 年度の公募準備期間が短かったこと等の理由から，2001 年 8 月から 9 月の期間に再度公募を行った． また，応募される見込みはないが，電子政府システムを構築するために必要不可欠と考えられる暗号技術や「電子署名及び認証業務に関する法律施行規則」，及び「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に関わる指針」で取り上げられた暗号技術等に対しては，事務局提案の暗号技術として安全性評価の対象として加えた．事務局で提案した暗号技術としては，3-key Triple DES, AES, SHA-1, RSA-OAEP, ECDSA，DSA 等である．その結果，2001 年度には，63 方式が評価対象となった.

また，2001 年度には暗号技術の利用に関し政策的な観点から検討を行うことを目的として，総務省技術総括審議官と経済産業省商務情報局長の連名の下で暗号技術検討会が組織された．暗号技術検討会では，電子政府システムにおける暗号技術が備えるべき要件の整理，暗号の利用方法，調達方法に関する調査・検討が開始された.

3.3.3 2002 年度の活動概要[15,16]

2002 年度は，2000 年度と 2001 年度の評価結果を基に暗号技術検討会からの選定方針に基づき，具体的な電子政府推奨暗号リストを構成する作業が行われた．また，

[8] 2004 年に，独立行政法人通信総合研究所と統合され独立行政法人情報通信研究機構(NICT)となった,
[9] New European Schemes for Signature, Integrity, and Encryption

暗号技術検討会では，電子政府推奨暗号リストの活用法や残された課題についての検討を実施した．第一回暗号技術評価委員会での方針に従い，10 年後の 2013 年頃までは安心して利用可能な暗号技術をリスト化した. 但し，当面電子政府システムを構築する際に必要不可欠な暗号技術，言い換えれば，2003 年時点で，市場で入手可能な暗号技術を含んでいた. 例えば, AES 暗号(FIPS-197)は，2001 年に米国連邦政府標準暗号となったが, 2003 年の時点では日本国内で入手可能な製品はなく，従って，電子政府システムに組み込むことは困難と考え，国内でも入手可能な 3-Key Triple DES もリストに含めた.

また，暗号技術検討会暗号調達ガイドブック作成 WG（リーダー：佐々木東京電機大学教授）では，電子政府推奨暗号リストを用いて，暗号製品を調達する際のガイドブックの作成を行った．このガイドブックの中で，調達仕様の検討・仕様書作成の段階で暗号技術への要件を記述すべきであることが指摘されている.

このガイドブックには，納品後の検査時点で，「暗号製品・システムが正しく納品されていることをシステムと切り離して個別に評価することは困難である．」（「暗号調達のためのガイドブック」p.47 より抜粋）との指摘がある．「4. 暗号モジュール認証制度」で紹介する暗号モジュール試験及び認証制度は，この指摘に基づいた活動であり，第三者機関に各種のテストを行わせ，暗号モジュールに対するセキュリティ要件との適合性を評価する制度である.

4. 暗号モジュール認証制度

CRYPTREC 事務局の一員である IPA セキュリティセンターでは，電子政府推奨暗号リストの利用環境整備の一環として, 2000 年度から暗号アルゴリズムが暗号モジュール[10]に正しく実装されていることを認証する手法についての検討を行った．暗号アルゴリズムが「正しく実装されていること」を確認する手法としては，経済産業省からの委託を受け IPA セキュリティセンターで制度構築を進めていた CC(Common Criteria)認証と米国とカナダが運用していた CMVP が検討の俎上に挙げられた.

4.1 Common Criteria(CC)[17]

CC 認証制度は，情報セキュリティ製品全般を対象として製品の評価を行う枠組みである．欧州中心に運用されていた ITSEC[11]と TCSEC[12]等を統合して国際標準となった評価基準である．評価基準（第 1 部：導入と一般モデル，第二部：セキュリティ機能要件，第三部：セキュリティ保証要件）と評価方法(CEM[13])から構成され，それぞれ ISO/IEC 15408 と ISO/IEC 18045 として国際標準となっている.

暗号モジュール製品のセキュリティ評価を CC の枠組みを用いて実施することも可能であり，例えば，暗号モジュールの一つである IC カード(Smart Card)のセキュリティ評価は CC を用いて行われることが多い.

しかし, CEM には暗号アルゴリズムの確認方法に関する規定がないため，評価者に暗号アルゴリズムとその実装方法についての知識が必要とされる.

一方，国内の CC 評価機関には，暗号アルゴリズムに詳しい評価者がいなかったため，電子政府推奨暗号リストに対応した暗号モジュールを CC 認証制度で評価することは難しい状況にあった.

4.2 CMVP[18]

米国における暗号モジュールの認証は，1977 年に制定された FIPS 46 Data Encryption Standard と共に始まった．1FIPS 46 の制定に伴い，1982 年に GSA[14]が作成した DES 暗号を利用した暗号装置に対する一般的要求(FS1027)に端を発している．FS1027 は，その後，NIST に移管され 1988 年に FIPS 140 Security Requirements for Cryptographic Modules として制定され[15]，1994 年には，サポートする暗号アルゴリズムが拡張された FIPS 140-1 へと改訂された．FIPS 140-1 の制定に伴い 1995 年からは CMVP[16]として運用が開始された．さらに，FIPS 140-1 は，2001 年にソフトウエアやファームウエアも対象とした FIPS 140-2 に改訂され現在に至っている．現在の CMVP は，米連邦政府機関が使用する暗号モジュール製品に対する共通的な認証制度であり，セキュリティ要件を定めた FIPS 140-2 と試験方法を定めた DTR(Derived Test Requirements)を用いて，暗号モジュールとしての適合性を，第三者の試験機関で試験し確認する制度である．具体的には，暗号モジュールのベンダは，認定された試験所(CST[17] laboratory)に試験対象となる暗号モジュールの適合性試験を要請する．CST では，DTR に定められた手

[10] 暗号モジュールとは，暗号化機能，ハッシュ機能，署名機能等のセキュリティ機能を実装したハードウェア，ソフトウェアの集合体のことである.

[11] Information Technology Security Evaluation Criteria
[12] Trusted Computer System Evaluation Criteria
[13] Common Evaluation Methodology
[14] GSA：General Services Administration、米共通役務庁
[15] FIPS 140 は，2 回定期見直し（改訂）を受けており，現在は FIPS 140-2 となっている.
[16] Cryptographic Module Validation Program
[17] CST: Cryptographic and Security Testing

順に従い，FIPS140-2 に対する適合性を試験し，その結果を米国 NIST に報告する．NIST は CST からの報告書を精査し，問題がなければ暗号モジュールに対して認証書を発行すると共に認証済み製品リストに追加してゆく．

CST で実施する暗号モジュール試験は，暗号アルゴリズムの適合性試験と暗号モジュールのセキュリティ要件に関する適合性試験の 2 段階に分かれる．暗号アルゴリズムの適合性テストは，NIST が FIPS や Special Publications 800 シリーズで承認された暗号アルゴリズムが，正しく実装され処理されているかの確認を行う過程である．現在では，承認された暗号アルゴリズムの確認手続きは，CAVP[18] として独立した制度となっている．CMVP で認証された暗号モジュールの総数は，制度がが発足した 1975 年以降 2011 年 6 月までに, 1,500 を超えている．

4.3 暗号モジュール試験及び認証制度[19]

4.3.1 制度設計と準備段階

我が国でも 2002 年度の CRYPTREC 暗号技術検討会報告書に基づき，2003 年度から CRYPTREC 暗号モジュール委員会（委員長：松本横浜国立大学教授）を設置し，暗号モジュール評価に関する検討を開始した．暗号モジュール委員会では，米国の FIPS 140-2 に範をとり，暗号モジュールに対するセキュリティ要件の検討を行った．

一方，米国は 2003 年に ISO/IEC JTC1 SC27 に対して，FIPS 140-2 を基に暗号モジュールのセキュリティ要件の国際標準を作成することを提案した．このような背景の下，IPA では国内での認証制度の創設に向け，制度の検討や試験要員・認証要員の育成，試験に使用するツール群の整備といった準備を開始した．

認証制度については，既存の認証制度に関する国際規格に基づいた制度を創設する必要があり，先行している CC 認証や米国・カナダの CMVP と同様に，認証機関は ISO Guide 65[19]に準拠し, 試験機関は ISO/IEC 17025[20]に準拠する制度とすることとした． IPA では CC に係わる評価認証制度の運営を行っていたため，CC と同様独立行政法人製品評価技術基盤機構(NITE[21])から認定を受けることとした．

また，IPA では，暗号モジュール試験及び認証制度の創設を前提として試験要員･認証要員の育成を開始した．そのため，IPA では 2003 年，2004 年に米国やカナダの暗号モジュール試験機関(CST Lab.)を訪問し，実態調査を行うと共に試験要員育成への協力を打診した．その結果，カナダと米国の CST Lab.が試験要員・認証要員の育成を支援してくれることとなった．

国内の CC 評価機関を中心に試験要員候補の推薦を依頼した．暗号モジュールの用途は多岐にわたるため，認証要員には，暗号技術に関する知識だけでなく，コンピュータシステムから半導体・情報家電にいたる幅広い業務経験を有するベテラン技術者（研究者）を選定し採用した．この試験要員および認証要員は，2004 年から 2006 年にわたり米国・カナダの CST で CMVP における試験に関する教育と訓練をうけた．

4.3.2 暗号モジュール試験及び認証制度

米国の FIPS 140-2 をベースに 2003 年から ISO/IEC JTC1 SC27 で標準化活動が行われていた暗号モジュールに対するセキュリティ要件は，2006 年に ISO/IEC 19790 として標準化が完了した. ISO/IEC 79790:2006 は, 翌 2007 年に日本工業標準暗号モジュールセキュリティ要件 JIS X 19790:2007 として制定された．また，同時に JIS X 19790:2007 に対応する暫定的な暗号モジュール試験要件 JIS X 5091:2007[22]が制定された. この日本工業規格の制定をを受け, IPA では 2006 年 6 月から我が国における暗号モジュール試験及び認証制度(JCMVP[23])の試行運用を開始し，2007 年 4 月には正式な運用へと移行した．

現在，JCMVP では，一般社団法人 IT セキュリティセンター 評価部, 独立行政法人 情報処理推進機構 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 評価センター，一般財団法人 日本品質保証機構 関西試験センターの 4 つの試験機関が NITE から認定されている．この試験機関の中には, 米国の CMVP 試験機関としても認定を受け機関もあたり, 希望すれば, JCMVP と CMVP 両制度の認証を受けることも可能となっている．

5. 標準化への貢献

5.1 暗号アルゴリズムの国際標準化

暗号アルゴリズムの国際標準化も DES から始まった．

[18] CAVP：Cryptographic Algorithm Validation Program
[19] ISO Guide 65 は，認証を行う機関が，第三者機関として適格であり信頼できると認められるために遵守しなければならない一般要求事項
[20] ISO/IEC 17025 は，試験機関の能力に関する一般要求事項であり，試験機関の能力を，認定機関が認定する際の基準としても利用される．
[21] NITE: National Institute of Technology and Evaluation
[22] 暗号モジュール試験要件は，国際標準 ISO/IEC 24759 の成立とその JIS 規格化を受け，2009 年 10 月に JIS X 5091 を廃止し，JIS X 24759:2009 に切り替えられた．
[23] Japan Cryptographic Module Validation Program

1980 年半ばに，ISO/TC 97/SC 20（暗号技術）で DES の国際標準化が進められた[20]．しかし，DES の国際標準化を提案した米国自身が，暗号アルゴリズムの強度評価が困難であること，暗号製品は米国の武器輸出規制の対象であることの 2 点を理由に標準化提案を取り下げた．そこで, SC20 としては暗号アルゴリズムの標準化を断念し，1991 年に暗号アルゴリズムの登録制度(ISO/IEC 9979:1991)が制定された[24][21]．2004 年 5 月時点では，全世界で 24（内，13 が日本から登録）の暗号アルゴリズムが登録された[22].

暗号アルゴリズムの登録制度は，加盟各国の NB(National Body)を窓口として，ISO/IEC 9979 で定めた登録機関に，暗号アルゴリズムの名称を登録する制度である．但し，暗号アルゴリズムを秘匿したまま登録することが可能であり，暗号アルゴリズムの安全性評価も実施されていないため，暗号を利用する者にとって有効な制度ではなかった．特に，暗号登録制度は各国 NB が係わって登録されるため，各国の暗号政策を反映される筈であった．しかし，我が国では ISO/IEC 9979 が逐語訳の翻訳 JIS X 9979 となったこと，我が国の暗号政策が未成熟であったことなどの要因から，登録された暗号アルゴリズムの過半が日本から提案された暗号アルゴリズムで占められ，暗号アルゴリズム登録制度は実質的な意味を失ってしまった．

そこで, 2000 年に ISO/IEC JTC1 CS27/WG2 において，改めて暗号アルゴリズムの国際標準化が始まった．2000 年からの標準化活動では，暗号アルゴリズムを提案する際に，提案国の NB は提案する暗号アルゴリズムの安全性評価情報を提供することが求められた．しかし，我が国の NB である本会情報規格調査会 SC27 専門委員会は賛助会員企業を中心に組織されているため，暗号アルゴリズムに対する中立的な安全性評価を行うことは困難であった．そこで，同時並行的に暗号アルゴリズムの安全性評価を行っていた CRYPTREC と連携し，CRYPTREC が作成した評価報告書を基に SC27/WG2 向けの安全性評価報告を作成した（図 1 参照）．その結果，CRYPTREC の評価報告書が効果的に活用されることにより，2003 年に制定された国際標準暗号規格(ISO/IEC18033)では，日本が提案した 5 つの暗号アルゴリズムが選定された．

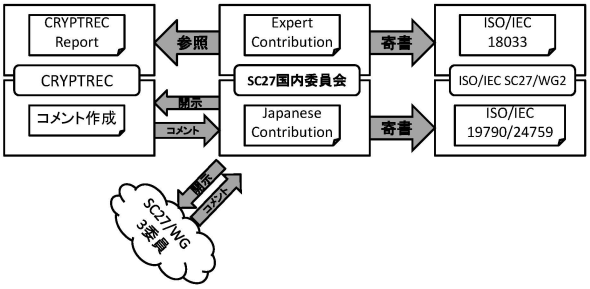

図 1．CRYPTREC と標準化

5.2 暗号モジュールに関わる国際標準

4.3.1 で紹介した様に，我が国では 2003 年度から CRYPTREC 暗号モジュール委員会で暗号モジュールに対するセキュリティ要件の検討を開始した[23][24][25]．一方，同じ年に ISO/IEC JTC1 SC27/WG3 で米国の FIPS 140-2 をベースにした暗号モジュールに対するセキュリティ要件の国際標準化が始まったため，暗号モジュール委員会でも，SC27/WG3 での国際標準化作業への支援を開始した[23].

CRYPTREC 暗号モジュール委員会は, 情報規格調査会の了解の下， SC27/WG3 で審議中の Working Draft(WD)の開示を受け，WD に対するコメントの作成を行い，国際標準規格 ISO/IEC 19790:2007 と ISO/IEC 19790 に対応する試験規格 ISO/IEC 24759 の充実に貢献した．

CRYPTREC 各委員会の活動や ISO/IEC 19790 や ISO/IEC 24759 の標準化は, 我が国の暗号モジュール試験及び認証制度の創設を加速し，我が国で「安全な」暗号モジュールを利用した暗号応用製品の市場を開拓しつつある．

6. 今後の課題とまとめ

6.1 今後の課題

6.1.1 暗号アルゴリズムの安全性評価

2002 年度に完成し公表した電子政府推奨暗号リストは，「向こう 10 年間は安全に利用できる」暗号アルゴリズムを選んで作成したリストであり, 2013 年以降に関しては改めて安全性評価を行う必要がある．そのため，CRYPTREC では，2013 年度完成を目指して，電子政府推奨暗号リストの改訂作業に着手した．そのため，2009 年度には，ブロック暗号，ストリーム暗号，メッセージ認証コード，暗号利用モード，エンティティ認証[25]のアルゴリズムを新たに公募し，現在の電子政府推奨暗号リ

[24] ISO/IEC 9979 は，1994 年に JIS X 5060-1994 として制定された．

[25] エンティティ認証とは，情報通信に関わる機器やプログラム等の存在（エンティティ）が正当なものであるか否かを確認することである．

ストに掲載した暗号アルゴリズムと併せて再評価作業を行っている.

また，現在の電子政府推奨暗号リストに掲載された暗号アルゴリズムの利用が当初の想定より偏っていることがわかってきた．特に提案者以外の第三者が製品に組み込んで出荷した例は，ごく少数に留まっている．電子政府推奨暗号リストの掲載されている暗号アルゴリズムの数が多すぎることがその原因と考えられ，結果として知名度の高い暗号アルゴリズムだけが利用されるという状況にある.

そこで，次期リストでは，暗号アルゴリズムのライフサイクルも考慮し，推奨候補暗号リスト，電子政府推奨暗号リスト，運用監視暗号リストの 3 リスト構成とすることが決定しており，現在，電子政府推奨暗号リストに掲載する暗号アルゴリズムの基準について検討している.

この検討の過程で，今後の暗号アルゴリズムの安全性評価のための人材の育成・確保等の課題があることが明らかにされた．人材の育成・確保については，大学や企業だけでなく，公的な研究機関の関与も視野に入れて，国全体で考えてゆく必要がある.

6.1.2 暗号モジュール試験及び認証

Smart Card の様な暗号モジュールに対しては，サイドチャネル攻撃などの新しい攻撃手法の出現があり，安全性の評価指標の確立が急務であり，独立行政法人産業技術総合研究所情報セキュリティ研究センターが中心となって開発した Side-channel Attack Standard Evaluation Board(SASEBO)シリーズの様な標準的な実験環境の開発と実験結果に基づいた安全性評価指標の研究が活発に行われている.

6.2 まとめ

本稿では，2000 年から始まった暗号アルゴリズムの安全性評価とそれに引き続いて始まった暗号モジュール試験及び認証制度について，それぞれの制度が設立された背景からその制度の創設，運用の状況について概観した．いずれの活動も我が国では前例のない活動であり，先行する欧米の制度も参考にし，試行錯誤を繰り返しながら運用に至った制度である．暗号技術は，情報セキュリティの根幹をなす技術であり，通常の技術とは異なり，「攻撃・解析」のような制御不能な脅威が存在する．そのため，絶え間のない「基準」の見直しが必要であり，「基準作り」のための基礎的な研究を地道に積み重ねる必要があることを指摘しておきたい.

最後に，本稿をまとめるにあたり，貴重なコメントをいただいた独立行政法人情報処理推進機構技術本部セキュリティセンター評価認証室近藤次長に感謝いたします.

参考文献

1) Diffie, W. and M. E. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, Vol.IT-22, pp.644-654, November 1976.
2) R.L.Rivest,A.Shamir,and L.Adelman, "A Method for Obtaining Digital Signature and Public-key Cryptsystems", MIT Laboratory for Computer Science; Thechnical Memo LCS/TM82(1977)
3) Biham, E. and A. Shamir. "Differential Cryptanalysis of DES-like Cryptosystems", Advances in Cryptology - CRYPTO '90. Springer-Verlag(1990).
4) Matsui, M. and Yamagishi, A. “A new method for known plaintext attack of FEAL cipher”. Advances in Cryptology - EUROCRYPT 1992
5) Matsui, M. “Linear cryptanalysis method for DES cipher”. Advances in Cryptology - EUROCRYPT 1993.
6) Matsui, M. “The first experimental cryptanalysis of the data encryption standard”. Advances in Cryptology - CRYPTO 1994
7) 通信・放送機構,「共通鍵ブロック暗号の選択／設計／評価に関するドキュメント」， 通信・放送機構，2000
8) AES home page, http://csrc.nist.gov/archive/aes/index.html
9) CESG Assisted Products Service (CAPS), http://www.cesg.gov.uk/products_services/iacs/caps/index.shtml
10) 情報処理振興事業協会，平成１１年度成果報告，「政府調達情報セキュリティ標準（基準）の策定～中間成果報告～」，2000 年 3 月
11) 暗号技術検討会，「暗号技術検討会 2000 年度報告書」，http://www.meti.go.jp/policy/netsecurity/downloadfiles/cryptrec2000.pdf
12) 暗号技術検討会，「暗号技術検討会 2001 年度報告書」，http://www.meti.go.jp/policy/netsecurity/downloadfiles/cryptrec2001.pdf
13) 暗号技術評価委員会,「CRYPTREC Report 2001 暗号技術評価報告書(2001 年度)」，http://www.ipa.go.jp/security/fy13/report/cryptrec/c01.pdf
14) 暗号技術検討会，「要件調査ワーキンググループ報告書」，http://warp.ndl.go.jp/info:ndljp/pid/258151/www.soumu.go.jp/s-news/2002/pdf/020416_2_b.pdf
15) 暗号技術検討会，「暗号技術検討会 2002 年度報告書」，http://www.meti.go.jp/policy/netsecurity/downloadfiles/Crypt_Report.pdf
16) 暗号技術評価委員会,「CRYPTREC Report 2002 暗号技術評価報告書(2001 年度)」，http://www.cryptrec.go.jp/report/c02_report.pdf
17) Common Criteria（CC），http://www.ipa.go.jp/security/jisec/index.html
18) Cryptographic Module Validation Program (CMVP) , http://csrc.nist.gov/groups/STM/
19) 暗号モジュール試験及び認証制度(JCMVP), http://www.ipa.go.jp/security/jcmvp/index.html
20) 情報処理学会情報規格調査会，SC 27 における情報セキュリティ標準化の動向, http://www.itscj.ipsj.or.jp/topics/security.html
21) 日本工業規格, データ暗号技術ー暗号アルゴリズムの登録手続, http://www.ipa.go.jp/security/enc/jis-x-5060-1994.html
22) 情報処理推進機構， ISO/IEC 9979 に基づく暗号アルゴリズム登録状況, http://www.ipa.go.jp/security/enc/regist-3.html
23) CRYPTREC Report 2004, http://www.cryptrec.go.jp/report/c04_mod.pdf
24) 「CRYPTREC Report 2004 暗号モジュール評価基準 第 0.1 版」，http://www.cryptrec.go.jp/report/c04_mod_secreq_v0_1.pdf

25)　「CRYPTREC Report 2004 暗号モジュール試験基準　第0.1 版」, http://www.cryptrec.go.jp/report/c04_mod_dtr_v0_1.pdf

今井　秀樹（正会員）
E-mail: h-imai@imailab.jp
昭 41 東大・工・電子卒．昭 46 同大学院博士課程了．工博．同年横浜国大講師．昭 47 同助教授．昭 59 同教授．平 4 東大教授（生産技術研）．平 17 産総研情報セキュリティ研究センター長兼務，平 18 中央大教授，東大名誉教授，平 23 中央大理工学研究所長併任．現在に至る．この間，符号理論，暗号と情報セキュリティ，通信方式などの研究に従事．電子情報通信学会（信学会）著述賞，論文賞，米澤メダル，猪瀬賞，業績賞，功績賞，IEEE シャノン記念論文賞，BCS ウィルクス論文賞，総務大臣表彰，経済産業大臣表彰，内閣官房長官表彰，大川賞，NHK 放送文化賞など受賞．著書「情報理論」「符号理論」「暗号のおはなし改訂版」など．信学会理事，監事，IEEE 情報理論ソサイエティ会長，IACR 理事，IEEE 東京支部長，同日本カウンシルチェア，暗号技術検討会（CRYPTREC）座長などを歴任．IEEE・IACR・信学会フェロー，信学会名誉員．日本学術会議会員，名誉博士（韓国，仏国）．

山岸　篤弘（正会員）
E-mail: a-yamagi@ipa.go.jp
昭 53 横浜国大・工・情報卒．昭 55 同大学院修士課程了．同年日本電気株式会社入社．昭 58 三菱電機入社．平 18 東大・大学院博士課程了．博士（情報理工学）．平 11 情報処理振興事業協会非常勤研究員．平 18 独立行政法人情報処理推進機構セキュリティセンター・暗号グループ・グループリーダー．平 23 同主任研究員．現在に至る．この間，符号理論，暗号と情報セキュリティなどの研究に従事．電子情報通信学会論文賞．情報処理学会業績賞受賞．

投稿受付：2011 年 7 月 4 日
採録決定：2011 年 7 月 26 日
編集担当：中田登志之（日本電気）