1. 21世紀初頭の暗号技術

8. 評価体制と標準化の内外動向

神田 雅透
NTT情報流通プラットフォーム研究所
kanda.masayuki@lab.ntt.co.jp

松本　勉
横浜国立大学 大学院 環境情報研究院
tsutomu@mlab.jks.ynu.ac.jp

金子 敏信
東京理科大学 理工学部 電気工学科
kaneko@ee.noda.tus.ac.jp

今井 秀樹
東京大学 生産技術研究所
imai@iis.u-tokyo.ac.jp

AES（Advanced Encryption Standard）プロジェクトが契機となり，世界中の多数の暗号研究者らによる多様な攻撃を受けても脆弱性が発見されなかった暗号を学術的に安全な暗号として広く利用していこうという流れが，最近世界的に強まっている．米日欧で行われた3つのプロジェクト（AES, CRYP-TREC, NESSIE）もこの流れに沿ったものである．また，ISO/IEC でも，これらの成果を受けて，ISO/IEC 国際標準暗号の策定を精力的に進めている．

本稿では，各プロジェクトが，どのような経緯や体制のもとで客観的な評価に基づいて安全な標準・推奨暗号を策定したのか，その成果がどのように利用されていくのかについて，その概要を解説する．さらに，ISO/IEC における最近の標準化動向について述べる．

米国政府標準暗号

米国商務省標準技術局NIST（National Institute of Standards and Technology）には，コンピュータセキュリティ法（1987年）や情報技術管理改革法（1996年）などによって，連邦政府内の情報セキュリティ推進に関する強力な権限が法的に与えられている．

これに基づいて，NISTは暗号技術やセキュリティ製品の評価方法，運用マネジメントガイドラインなど，広範囲にわたって標準規格を策定し，多数のFIPS（Federal Information Processing Standards）規格やSP（Special Publications）文書として登録・発行している．暗号技術に関連したところでは，FIPS 197 AESのほか，FIPS 180-2 Secure Hash Standard（暗号学的ハッシュ関数），SP 800-38C CCM モード（認証機能付暗号処理）などが新たに発行されている．

連邦政府システムにおいて，FIPS規格は，適用除外の承認を得たものを除き，該当する規格を遵守する強制規定であるのに対し，SP文書は参考情報として公開される．FIPS規格に登録された暗号技術[1)]が米国政府標準暗号と呼ばれるのはこのためである．

FIPS規格に登録された暗号技術に対しては5年ごとの再審査規定があり，今後5年間の解読技術の進展動向や計算機性能の向上などを考慮してFIPS規格として継続することがふさわしいかどうかをNISTが判断する．ふさわしくない，あるいは新しい暗号の追加が必要と判断すると，新たな暗号の策定がNISTのミッションとして加わる．たとえば，FIPS 197を策定したAESプロジェクトは，1993年のFIPS 46-1 DES再審査で次期標準暗号の必要性が明記されたことの延長線上で実施された．

また，NISTは安全性に問題が生じ始めた暗号技術についてどのように対処すべきかなどの方針も打ち出す．DESの場合，2002年にTriple DESかAESへの2年以内の移行を求めており，2004年のFIPS 46-3 DES/Triple DES再審査でFIPS規格からDESを削除することが決まっている．

電子政府推奨暗号

日本では，ミレニアム・プロジェクトやe-Japan戦略で2003年度までに電子政府の基盤構築を行うことが目標に掲げられた．その具体的施策となるe-Japan重点計画「6. 高度情報通信ネットワークの安全性および信頼性の確保」の実施施策の1つとして，総務省および経済産業省が主管となった「暗号技術の標準化の推進」が明記された．具体的には，電子政府での利用に資するかを判断するための暗号技術評価および電子政府推奨暗号リス

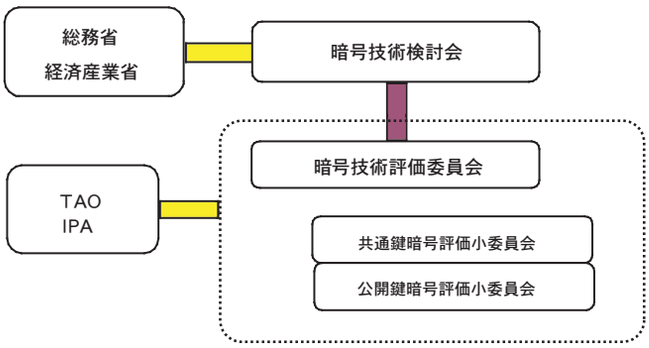

図 -1　2001/2002 年度の CRYPTREC 体制

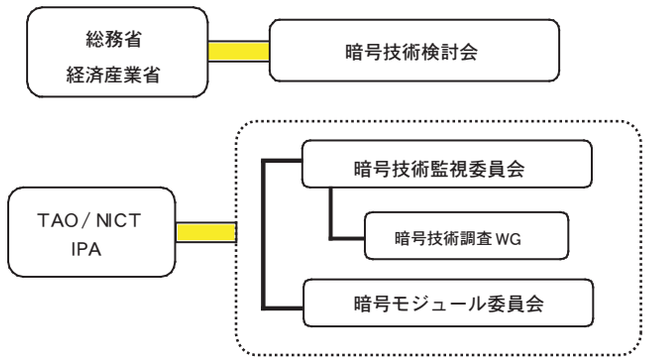

図 -2　2003/2004 年度の CRYPTREC 体制

トを作成する方針が挙げられた．

この活動を実質的に執り行う機関として，通商産業省と情報処理振興事業協会（IPA）は，今井秀樹東京大学生産技術研究所教授を委員長，辻井重男元中央大学教授を顧問とする暗号技術評価委員会CRYPTREC（Cryptography Research & Evaluation Committees）を2000年5月に発足させた．この委員会は，大学や暗号開発ベンダに所属する日本有数の暗号研究者ら有識者による委員と7省庁からのオブザーバで構成された．さらに，下部小委員会として，共通鍵暗号評価小委員会（委員長：金子敏信東京理科大学教授）と公開鍵暗号評価小委員会（委員長：松本勉横浜国立大学教授）が設置された．

2001年度からは，総務省と経済産業省との共管に変わるとともに，政策的な課題を含めて暗号技術の評価・検討を行う場として暗号技術検討会が新設された．また，暗号技術評価委員会の事務局も通信・放送機構（TAO）とIPAの共同事務局となった（**図-1**）．

実際の評価では，電子政府システムで必要とされる暗号技術を公募した後，公開鍵暗号技術を公開鍵暗号評価小委員会が，共通鍵暗号技術・ハッシュ関数・擬似乱数生成系を共通鍵暗号評価小委員会がそれぞれ担当して，国内外の主要な暗号研究者に依頼した安全性評価報告と国内外での学会発表論文などをベースに第一次判定を行った．その後，暗号技術評価委員会が両小委員会の報告を参考に審議を行い，技術的観点からの第二次判定（技術的最終評価）を行った後，暗号技術検討会が政策面など非技術的要素も加味した上で最終判定を下すという構造であった．

2回の公募を通じて応募された暗号技術52個のほか，CRYPTRECが必要と判断した暗号技術14個を含む，総計66個の暗号技術，ならびにSSL/TLSについての安全性評価を実施した．その結果，電子政府システムでの利用に資するかどうかの観点から安全性に特に問題がないと判断された暗号技術31個を電子政府推奨暗号リストに掲載することとし，2003年2月に最終確定した[2)]．

この電子政府推奨暗号リストは，「電子政府の情報セキュリティ確保のためのアクションプラン」（2001年10月情報セキュリティ対策推進会議決定）および「各府省の情報システム調達における暗号の利用方針」（2003年2月行政情報システム関係課長連絡会議了承）に基づき，電子政府システム調達における暗号技術選択の際に利用されている．

2003年度からは，電子政府推奨暗号リストに載った暗号技術に安全性上の問題が生じていないかどうかを監視するための暗号技術監視委員会（今井秀樹委員長）および暗号技術調査ワーキンググループ，ならびに安全な暗号モジュールを実現・評価するための調査検討を行う暗号モジュール委員会（松本勉委員長）に改組され，現在も活動は継続している（**図-2**）．なお，TAOは2004年度に情報通信研究機構（NICT）に変わった．

CRYPTRECによる安全性や実装性能に対する評価結果は，毎年度末に発行される暗号技術評価報告書などに掲載されている[3)]．

欧州推薦暗号技術

欧州連合では，その傘下の欧州委員会が策定した第5次情報社会技術研究開発プログラムの一環として，NESSIE（New European Schemes for Signature, Integrity, and Encryption）プロジェクトを2000年にスタートさせた．その目的は，暗号技術での欧州企業の国際競争力強化・研究開発力維持に役立つ暗号技術推薦リスト（NESSIE Portfolio）を作成し，さまざまな標準化団体などで使用してもらうことによって標準化への合意形成を図ることであった．

体制として，運営資金のみを欧州連合が拠出し，実際

の運営は，欧州の大学に所属している暗号研究者らによる技術運営チームとセキュリティ関連企業で構成されるインダストリボードが連携して担当した．

NESSIEプロジェクトの最大の特徴は，欧州製セキュリティ関連製品の国際競争力向上に役立てようという「欧州のための」プロジェクトという側面を明確にしていた点である．たとえば，欧州製品の国際競争力がもともと高いICカードでの実装性能を特に重要視していることを最初から明らかにしており，高度な暗号機能付きICカードを欧州製品の国際競争力強化につなげようとする意図の表れとも読み取れる．このような視点を評価基準に加えることで，欧州産業界の意向が反映されているといえよう．

このプロジェクトでは，公開鍵暗号や共通鍵暗号，ハッシュ関数など全部で7カテゴリ，合計39個の応募暗号技術を受け付けた．

技術運営チームが作成した評価報告書やNESSIE会議などでの評価報告などを利用して，安全性と実装性能，さらに知的財産権の取り扱いなどを総合的に判断した結果，応募暗号技術からは12個，その他の標準的な暗号技術から5個の総計17個の暗号技術を最終選抜し，2003年2月に開催された第4回NESSIE会議の席上で発表した[4]．

NESSIEプロジェクト自体は，2003年3月の最終報告書の取りまとめをもって終了した．ここでの成果は，欧州での暗号技術推薦リストとして，ISO/IECやIETFなどの標準化団体／標準化活動に提供され，国際標準化への推進を図ることになっている．

ISO/IEC国際標準暗号

現在，ISO/IECでは，暗号方式の登録制度（ISO/IEC 9979）は存在するものの，ISO/IEC国際標準暗号は策定していない．つまり，事実上の世界標準暗号であるTriple DESやRSAさえもISO/IEC国際標準暗号ではない．

しかし，ISO/IEC JTC 1/SC 27では，従来方針を変更し，ISO/IEC国際標準暗号を初めて策定する作業を2000年に開始した．2005年末を目途に，公開鍵暗号と共通鍵暗号（ブロック暗号・ストリーム暗号）について，カテゴリごとに，安全性評価が客観的に行われた少数の暗号アルゴリズムをISO/IEC 18033国際標準暗号として選定していく予定である．

このため，米国をはじめとする政府標準暗号のほか，世界中の多数の暗号研究者が評価に関与したNESSIEプロジェクトおよびCRYPTRECプロジェクトの成果が標準化作業に大きな影響を与えており，これらのプロジェクトで共通に選定された暗号技術を中心に現在審議が進められている．

また，ISO/IEC国際標準暗号が策定されることを合わせて，それらの暗号の利用方法となる，暗号利用モードやデータカプセル化メカニズム（DEM: Data Encapsulation Mechanism）の策定なども進められている．

暗号モジュール評価に関する標準化動向

今後の課題として，学術的に安全な暗号を使うことはもちろんのことだが，その暗号を正しく安全に実装することも重要になってきている．

米国政府は，FIPS規格のアルゴリズムやガイドラインなどが正しく安全に実装されているかを検査するため，暗号モジュールに関する認証プログラムCMVP（Cryptographic Module Validation Program）を1994年から開始した．現在は，FIPS 140-2として，カナダ政府機関と共同で運用している．

ISO/IEC JTC 1/SC 27では，FIPS 140-2をモデルとした暗号モジュールに関する検査・評価体制についての検討を開始した．当面は，暗号モジュールのセキュリティ要件だけを取りまとめるISO/IEC 19790が先行するかたちとなる．その際のISO/IEC承認アルゴリズムとして，ISO/IEC 9796, 14888, 15946（ディジタル署名），ISO/IEC 10118（ハッシュ関数），ISO/IEC 18033（暗号処理）をはじめとするISO/IEC国際標準暗号技術が指定される見込みである．

日本としても，ISO/IEC 19790の審議に対応していくため，CRYPTRECの暗号モジュール委員会で，暗号モジュールに関する検査・評価体制の検討を始めている．

参考文献
1）NIST: Cryptographic Toolkit, http://csrc.nist.gov/CryptoToolkit/
2）総務省，経済産業省：電子政府推奨暗号リスト，http://www.soumu.go.jp/joho_tsusin/security/cryptrec.html
3）IPAセキュリティセンタ：CRYPTREC, http://www.ipa.go.jp/security/enc/CRYPTREC/index.html
4）NESSIE: NESSIE Portfolio of Recommended Cryptographic Primitives, http://www.cosic.esat.kuleuven.ac.be/nessie/

（平成16年9月30日受付）