日米欧の暗号技術標準化・評価プロジェクトを終えて
－ 3 プロジェクトの実績と今後への展望 －

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

あらまし　1997 年以降、暗号技術の標準化や評価を目的とした米国政府の AES プロジェクト(1997 – 2001)、欧州連合の NESSIE プロジェクト(2000 – 2003)、日本政府の CRYPTREC プロジェクト(2000 – 2003)が行われた。本稿では、これらのプロジェクトがそれぞれどのような目的をもち、どのような活動を行ってきたのかを振り返る。また、筆者を含む NTT チームがこれら 3 プロジェクトすべてに応募者として参加した体験を踏まえ、それらの成果の意義や違い、今後の展望などについて述べる。

1. はじめに

1997 年 1 月、米国商務省標準技術局 NIST (National Institute of Standards and Technology)は、後に世界中から多くの第一線の暗号研究者らが一堂に会することになる一大イベントの開始を宣言した。米国で行われた AES プロジェクト[1]である。このプロジェクトは、公募によって、当時の米国政府標準暗号 DES (Data Encryption Standard)[4]に替わる新しい 128 ビットブロック暗号 AES (Advanced Encryption Standard)[6]を策定することを目的とし、米国内はもとより世界中の暗号研究者らに参加を呼びかけたものである。

当時の暗号技術をめぐる世界的な認識では、暗号技術は「武器」であり「厳しく輸出管理すべきもの」であったから、自国政府の標準暗号を国内外の公募によって策定するなど前代未聞であった。したがって、参加者の多くは、当初 NIST の方針に対して半ば期待しつつも半信半疑であった。ところが、予想をはるかに上回る NIST の徹底したオープンな選定プロセスの遂行ぶりには世界中から賞賛の声が贈られるようになり、AES プロジェクトの開始から 4 年間以上にもわたって世界中から第一線の暗号研究者らをはじめ、多くの研究者・ベンダ・ユーザが何らかの形で関与しつづけた。

欧州では、AES プロジェクトの予想以上の成功ぶりに触発された形で、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)を作成する NESSIE プロジェクト[14]を、欧州連合 EU (European Union)の R&D プログラムの一環として、2000 年から立ち上げた。このプロジェクトでは、128 ビットブロック暗号だけでなく、共通鍵暗号・公開鍵暗号／署名・擬似乱数生成系・ハッシュ関数、MAC(メッセージ認証子)など全 10 カテゴリの暗号技術を対象に公募を行った。

他方、日本では、「ミレニアム・プロジェクト[21]」や「e-Japan 戦略[23]」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。具体的施策として、「e-Japan 重点計画[24]」などに、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及び電子政府推奨暗号リストを作成する方針が挙げられた。そのための活動として、経済産業省(当時通商産業省)などが中心となって 2000 年から開始されたのが CRYPTREC プロジェクト[19][20]である。NESSIE プロジェクトが AES プロジェクトの成功を多分に意識して行われたのに対し、CRYPTREC プロジェクトはあくまで日本独自の活動として実施された。

このように、プロジェクトごとの目的や運営方法は異なる面があるものの、ほぼ同時期に日米欧の 3 地域で暗号技術の標準化や評価を目的としたプロジェクトとして実施された。そして、これらのプロジェクトのいずれもが公募形式をとっており、各プロジェクトの指定する公募要項を満たしさえすれば、主催する国内外問わず応募が出来た。また、実

際のプロジェクトの運営に当たり、世界中の暗号研究者らが多数関与したという点についても同じである。そのため、各プロジェクトでの成果は、ISO/IEC をはじめとする、今後の暗号技術の国際標準化にも大きな影響を与えつつある。

本稿では、各プロジェクトが一通り終了し、今後はこれらの成果が利用されていく段階を迎えるに当たり、これらのプロジェクトがそれぞれどのような目的をもち、どのような活動を行ってきたのかを振り返ることにする。また、筆者を含む NTT チームがこれら 3 プロジェクトすべてに応募者として参加した体験を踏まえ、それらの成果の意義や違い、今後の展望などについて述べる。

本稿の構成は以下のとおりである:

2 章から 4 章にかけて各プロジェクトの概要を説明する。5 章では 3 プロジェクトの比較・検討を行う。6 章ではこれらの成果に対する今後の展望、特に ISO/IEC 国際標準化への影響を述べる。

2. AES プロジェクト ― 米国

2.1 なぜ AES が必要になったのか

1977 年、米国商務省国立標準局 NBS (National Bureau of Standards)は、機密ではないが取り扱いに注意を要する政府機関の情報[1](センシティブ情報; unclassified sensitive information)を暗号化する米国政府標準暗号 DES を開発し、FIPS46 (Federal Information Processing Standards 46)として公布した。DES は世界で初めてアルゴリズムを公開した暗号として現代暗号の礎を築くと同時に、策定後四半世紀の長きにわたり米国内はもとより世界中で広く使われ続けた事実上の世界標準暗号でもある。

DES の安全性に関しては、開発当初から、秘密鍵の鍵長が 56 ビットと短すぎる(当初の提案では 112 ビットであったが最終的に 56 ビットに短縮された経緯がある)、トラップドアが仕込まれているのではないか、などの指摘がくすぶり続けていたものの、1990 年代に入るまで具体的な解読法が指摘されることはなかった。しかし、1990 年になると最初の理論的な解読法となる差分解読法[10]が提案され、また 1994 年には線形解読法[11]によって最初の解読実験に成功する[12]など安全性が揺らぎ始めた。

DES の安全性に対して決定的な影響を与えたのが DES Challenge[13]である。このコンテストでは、鍵を一つ一つしらみつぶしに検査して正しい秘密鍵を見つけ出す鍵全数探索法を用いて DES を解読しようというものである。鍵全数探索法による攻撃では、対象とする鍵すべてを検査するのに必要な計算能力さえあれば必ず成功し、秘密鍵を見つけ出すことができる。つまり、それだけの計算能力を実現することができるか否かだけが暗号の安全性を左右する。

DES Challenge の結果は表 1 に示すようにすべて成功した。計算機性能の飛躍的な向上とインターネットによる分散型計算機ネットワークの普及が進んだ現在、鍵長 56 ビットの DES を破ることは十分に可能な領域に入りつつあることを示している。

こうなると、DES を使い続けるわけにはいかなくなり、新しい米国政府標準暗号が必要となった。

表 1 DES Challenge の結果

Challenge	計算能力(1 秒間の検査数)	解読時間
I (1997.1-7)	平均 1 万台の PC	約 140 日
II-1 (1998.1-2)	約 4 万台相当の PC	約 40 日
II-2 (1998.7)	約 25 万ドルの解読装置 DES Cracker (900 億個/秒超)	約 56 時間
III (1999.1)	DES Cracker と約 10 万台の PC が協力(2400 億個/秒超)	22 時間 15 分

2.2 NIST の驚くべき方針転換

1993 年の時点で、NIST は米国政府標準暗号としての DES の承認期間を FIPS46-2 の期限となる 1998 年までとする決定を一度行っている。逆に言えば、1998 年には DES に替わる新しい標準暗号が必要になった。

当時のクリントン=ゴア政権は、米国内外に高速な情報通信基盤を整備する NII (National Information Infrastructure) ／ GII (Global Information Infrastructure)構想と並び、国家安全保障の観点からキーエスクロー政策を掲げていた。これは、犯罪捜査など公共の利益があると認められれば、捜査機関等によって強制的に暗号機能を解除できる合

[1] 法律上の機密情報には該当しないものの外部への流出防止に注意を払うべき情報や、政府が保有する個人のプライバシに関わる情報なども含む。

法的暗号解読(Lawful access)を認めたものである。そのための仕組みとして EES (Escrow Encryption Standard)[5]が開発された。1994 年に FIPS185 に登録された EES には、新たな標準暗号として国家安全保障局 NSA (National Security Agency)が開発した Skipjack[7]が使われている。つまり、DES の後継暗号を Skipjack にしようと考えたのである。

ところが、米国政府は EES/Skipjack の仕様を非公開としたうえで EES の利用を強制しようとしたため、政府機関によるプライバシ侵害を主張する有識者や民間組織・プライバシ保護団体、そして国際競争力の低下を恐れる産業界などから強硬な反発を買うこととなった。これに慌てた米国政府は、EES の代用となる鍵回復方式 KRS (Key Recovery System)の提唱や EES/KRS 搭載製品の輸出規制緩和を実施するなど多くの譲歩を重ねたものの、賛同を得ることができなかった。そのため、1996 年 Skipjack の仕様を公開するなど、EES の導入を事実上断念した。

EES 導入計画が潰えると、NIST は DES の後継暗号策定に関する方針を一大転換する。「産学の賛同が得られなかった」ために標準暗号 EES の策定が事実上挫折したとの反省があったのか、一転して新しい標準暗号 AES を公募によって策定する AES プロジェクト[1]の実施を宣言した。FIPS46-2 の承認期限切れまであと 2 年に迫ってはいたが、米国内はもとより世界中の暗号研究者やユーザ、産業界、標準化機関などに最初からプロジェクトへの協力･参加を呼びかけることによって、「時間がかかっても広くコンセンサスを得ながら」標準暗号の策定を進めていく道を NIST は選んだ。

2.3 AES が決まるまで

1987 年制定のコンピュータセキュリティ法(Computer Security Act of 1987)、1996 年制定の情報技術管理改革法(Information Technology Management Reform Act of 1996)及び大統領令 13011 号(Executive Order 13011)によって、米国連邦政府システムにおける情報セキュリティに関する強力な執行権限を NIST に与えている。特に、センシティブ情報を取り扱う連邦政府システムでは、FIPS 適用除外の承認を得たものを除き、NIST が公布する FIPS を遵守しなければならないと規定されている。FIPS に登録された暗号が米国政府標準暗号と呼ばれるのはこのためである。

AES プロジェクトも上記の法的根拠に基づいた NIST の責任下で実施され、このプロジェクトで策定された AES が最終的に FIPS になることが明確にされた。つまり、このプロジェクトは、商務省や NIST といった一官庁の施策ではなく、米国政府として責任を持つ施策であることを意味した。

表 2 AES プロジェクトの日程

1997.1.2	AES プロジェクト開始を宣言	
1997.4.15	AES ワークショップ開催	
1997.9.12	AES 候補暗号公募要綱公開	
1998.6.15	公募締切	
1998.8.20–22	第 1 回 AES 候補会議開催	Round 1
	(FIPS46-2 期限切れ(1998.12))	
1999.3.22–23	第 2 回 AES 候補会議開催	
1999.4.15	第 1 次評価コメント募集締切	
1999.8.10	最終候補選抜・発表	Round 2
	(FIPS46-3 正式発効(1999.10))	
2000.4.13–14	第 3 回 AES 候補会議開催	
2000.5.15	第 2 次評価コメント募集締切	
2000.10.2	Proposed AES に Rijndael を選定	
2001.2.28	AES の FIPS 化作業開始	
2001.11.26	FIPS197 AES 正式発効	

1997 年 9 月、AES 候補暗号公募要綱が公開された。それには、応募者が準備すべき応募書類の一覧のほか、以下のようなことが記載されている。

〔仕様などに関する事項〕

- 仕様が完全に公開されていること[2]
- ブロック長 128 ビット、鍵長 128/192/256 ビットが利用できるブロック暗号であること
- Triple DES よりも安全かつ非常に効率性が改善されていること
- 世界中で特許無償で利用できること
- 設計方針や安全性自己評価を記した補助文書(supporting document)を準備・提出すること
- C ソースで作成した参照コード[3]と計測用最適化コードを提出すること

[2] 仕様書からの情報だけで第三者がその暗号を実装することができる程度に仕様が公開されていること

[3] 仕様書に対比した形で暗号化処理の手順が確認できるプログラムのこと

〔選定に関する事項〕

- 原則として「一つの」ブロック暗号を AES に決定したい
- 評価基準には、(1)安全性、(2)実装性能、(3)その他の特長、があり、この順番の優先順位で候補暗号を比較・選定する
- 応募要綱を完全に満たした候補暗号を評価対象とした第 1 次評価(Round 1)と、5 個以下の最終候補(finalists)を評価対象とした第 2 次評価(Round 2)の 2 段階で評価・選抜を実施する

1998 年 6 月までの約 9 ヶ月間の公募期間が設定され、その間に世界中から 21 件の応募があった。その後、2 ヶ月間の応募書類審査を経て、最終的に 15 件の応募が候補暗号として認定された。日本からは NTT 提案の E2 が唯一の候補暗号となった。

15 件の候補暗号は 8 月に開催された第 1 回 AES 候補会議で発表され、約 9 ヶ月にわたる第 1 次評価がスタートした。

AES プロジェクトの大きな特徴としては、評価期間を通じて NIST が一般からの意見・評価結果を広く求めつづけたことが挙げられる。そのために、ホームページ上で必要な情報を提供することはもちろん、ディスカッションフォーラムの設置、安全性や実装性能の評価結果やコメントなどの募集・公開を通じて、NIST と暗号研究者らとの間で常に情報交換できる体制を整えた。極めつけは、当時の輸出管理上は明らかに輸出禁止対象となるはずの候補暗号のソースコード一式を評価目的のための特例措置として原則輸出を許可したこと、そして優秀な評価結果を発表してもらうため NIST 主催の第 2 回 AES 候補会議を多くの暗号研究者らが集まる暗号国際会議の開催に合わせてローマに出向いて開催したことである。

このような前例にとらわれない NIST の真摯な努力に対して、世界中の多くの暗号研究者らも独自のホームページを立ち上げて AES プロジェクトをサポートしたり、多くの安全性や実装性能の評価結果を提供したりするなどして応えた。

1999 年 4 月までの第 1 次評価期間中に寄せられた論文、コメント、NIST 自身の評価結果などをもとに 5 個の最終候補を選抜し、8 月に選抜結果を発表した[2]。

そのなかで、安全性上の問題が指摘された候補を除く 10 候補に対して、NIST はすべての相互比較によって上位 5 候補暗号を選抜するのではなく、同じような特長をもつと判断した同種プロファイル(similar profile)というグループ内の相互比較で最も優れた候補暗号を選抜するという方式を採用したことを明らかにした。

AES プロジェクトの最終目標は、「一定水準以上の暗号」を求めることではなく、「最優秀の(一つの)暗号」を求めることにある。このため、同種プロファイルに含まれる候補暗号の中で最優秀でなければ AES になることは極めて困難であるので、安全性や実装性能に問題があるか否かに関わらず、二番手以降の候補暗号をこれ以上評価する必要はないと NIST は判断した。いわゆるトーナメント方式による決定方法である。

2000 年 5 月までの第 2 次評価期間では、安全性評価よりもむしろ実装性能評価のほうに関心が集まった。これは、最終候補に安全性上の問題点がそう簡単には見つかりそうもなかったためである。現に、第 2 次評価期間中に安全性に関して大きな問題点を指摘された最終候補はない。そのため、実装性能の評価結果が AES 選定に大きな影響を及ぼすと考えられ、世界中から多くの実装性能評価が寄せられた。このなかには、NSA による評価結果も含まれる。

第 3 回 AES 候補会議では、ハードウェアや IC カードでの実装性能評価と実装攻撃に対する安全性評価が注目された。

これらの評価結果に対して、NIST は対照的な判断を下している。AES 選定のために、実装性能の評価結果は積極的に利用されている一方、実装攻撃に対する安全性の評価結果はその評価基準があいまいであるとして複数のデータを掲載するに留め、NIST の判断には利用されていない。

AES プロジェクトが終わりに近づくにつれ、「AES 提案暗号(Proposed AES)としていくつの暗号技術を選定するか」という議論が再燃した。公募に当たり、NIST は、相互接続性などを考慮し、Triple DES よりも安全かつ幅広い様々なアプリケーションで非常に効率性が改善された「一つの」ブロック暗号を AES に決定したいとの原則論を掲げた。その一方で、あるアプリケーションに対して非常に優位な特性を示す暗号が複数あるのであれば例外的に複数の AES を決める可能性も排除しないとしていたためである。この点についても NIST は幅広く意見を求めた。

「複数」を支持する代表的な意見は、一つだけを選定した場合、その暗号が解読されるなどの問題がおきた場合の影響が大きくなりすぎるというものであり、あらかじめ副標準暗号や代替(バックアップ)暗号を選んでおくべきであるというものである。この場合、複数とはいっても多くは「二個」のことを意味している。一方、「一つ」を支持する代表的な意見は、複数の暗号を選定した場合には、相互接続性の問題や実装コストの上昇など主に実装・運用上のデメリットが発生すること、また副標準暗号や代替暗号を選んでおくことが安全性上の問題回避の対策になっている保証はない、というものである。ちなみに、第 3 回 AES 候補会議の参加者の多くは後者の意見を支持した。

2000 年 10 月、NIST は AES 提案暗号として Rijndael だけを選定したことを発表した。``Report on the Development of the Advanced Encryption Standard (AES)"[3]に記載された選定理由によれば、Rijndael を最終的に選定する決め手になったのは他の最終候補よりも明確に抜きん出た性能を示したハードウェアと IC カードの実装評価結果であった。また、選定個数について、当初の原則論をあえて修正してまで複数の暗号を選ぶメリットを見出せなかったとした。

2001 年 11 月、Rijndael は FIPS197 AES[6]として正式に米国政府標準暗号の一つに登録され、約 5 年にわたる AES プロジェクトが終結した。

Rijndael を AES として FIPS 化する過程で一つ議論になった点がある。

今後 20 年間という利用期間を考えたとき、Rijndael の仕様のままでは安全性が確保できないではないか、実装性能をやや落としてでも安全性を高めておくべきではないか、という指摘があった。確かに、暗号研究者のなかには、今後数年のうちに Rijndael の理論的解読法が見つかってもおかしくはないとの意見が比較的根強くある。

しかし、それらの意見に対する NIST の答えは「修正しない」であった。その理由は、今の仕様のままでも(仮に理論的解読法が見つかっても)現実的な脅威にはならないので、わざわざ実装性能を落とす必要はない、というものである。この判断は暗号研究者の観点とは違う NIST の極めて現実的な対応の反映といえる。

ところで、DES に関連して、NIST は 1998 年に承認期限切れとなった FIPS46-2 に替わり、Triple DES と DES を米国政府標準暗号に定めた FIPS46-3[4]を 1999 年に発行した。つまり、共通鍵暗号の米国政府標準暗号は、現在、Triple DES、DES、AES の三つあることになる。ただし、新規の連邦政府システムには Triple DES もしくは AES を採用するのが原則である。また、2004 年に発効予定の FIPS46-4 では DES は標準暗号から完全に承認取り消しとなることが決まっているため、現在 DES を使用している連邦政府システムでもこれから 2 年以内に Triple DES か AES に切り替えるよう警告している。

3. NESSIE プロジェクト ― 欧州

3.1 なぜ NESSIE プロジェクトを始めたか

米国政府の狙いどおり、世界中の多数の暗号研究者らが積極的に AES プロジェクトに関与し続けており、また多くの標準化機関やセキュリティ関連企業なども AES に興味を示していた。そのうえ、世界中で AES は特許無償許諾が行われることが決まっていたので、このまま順調に選定が推移すれば、AES が国際標準暗号の地位を獲得するのは時間の問題と考えられた。一方、逆の見方をすれば、暗号技術に対する欧州企業の国際競争力を低下させるかもしれない、という危機感を芽生えさせる動機付けになったのかもしれない。

EU では、欧州委員会策定の第 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[14]を 2000 年 1 月から 3 年間の予定でスタートさせた。

NESSIE プロジェクトの掲げた目的として以下の点が挙げられている。

(1) 安全かつ強力な暗号技術推薦リスト(NESSIE portfolio)を作る
(2) プロジェクトの成果を広く普及させるとともに、プロジェクトインダストリボード、第 5 期フレームワークプログラム、様々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
(3) 暗号技術での欧州企業の国際競争力を強化すると同時に、欧州の研究開発能力の優位な立場を維持する

(4) 上記の目的を達成するための具体的な対応として、最終フェーズに入っている AES プロジェクトに対して欧州の立場から寄与することや独自の公募を行うこと、評価方法や評価ツールの開発を進めること、などを行う

NESSIE プロジェクトの概要を見ると、多分に AES プロジェクトを意識していることがわかる。評価プロセスや運営方針自体が AES プロジェクトのそれと非常に似通っている点からも読み取れよう。例えば、①世界中の暗号研究者らが参画できるよう、公募の実施、NESSIE 会議の開催、ディスカッションフォーラムの設置などを行って、透明で公開された選考プロセスとそれを基にした選抜を実施すること、②公募暗号技術すべてを対象とする第 1 次評価(First Phase)と、第 1 次評価選抜暗号技術を対象とする第 2 次評価(Second Phase)の 2 段階評価・選抜を実施すること、③NESSIE プロジェクトの成果への合意形成と標準化推進を図ること、が挙げられている。

一方、大きく異なるのは、EU からは運営資金が供与されるだけで、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」が連携して担当する点である。つまり、AES プロジェクトが政府直轄プロジェクトであるのに対し、NESSIE は産学連携プロジェクトの一つということができる。しかし現実には、EU の正式なプログラムとして実施されること、インダストリボードメンバには欧州の有力なセキュリティ関連企業が名を連ねていること、ISO/IEC や IETF などでの国際標準化推進を図ること、などの理由から、欧州暗号技術のデファクトスタンダードを決めることになるプロジェクトでもある。

例えば、暗号技術推薦リストを策定するうえで考慮する評価基準として安全性と実装性能の両面があるのだが、そのなかでも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いる。このことは、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わることで、欧州産業界の意向が反映されているといえよう。

このように、ここでの成果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る。

3.2 暗号技術推薦リストが決まるまで

2000 年 3 月、NESSIE 候補暗号公募要綱が公開された。

表 3 NESSIE 公募カテゴリ

カテゴリ	要求される安全性強度
ブロック暗号	High (鍵長 256 ビット以上、ブロック長 128 ビット以上) Normal (鍵長 128 ビット以上、ブロック長 128 ビット以上) Normal-Legacy (鍵長 128 ビット以上、ブロック長 64 ビット以上)
ストリーム暗号 (同期型／自己同期型)	High (鍵長 256 ビット以上、内部メモリ 256 ビット以上) Normal(鍵長 128 ビット以上、内部メモリ 128 ビット以上)
メッセージ認証子	High (鍵長 256 ビット以上) Normal (鍵長 128 ビット以上)
ハッシュ関数 (非衝突型／一方向性型)	High (ハッシュ値 512 ビット以上(非衝突型)／256 ビット以上(一方向性型)) Normal (ハッシュ値 256 ビット以上(非衝突型)／128 ビット以上(一方向性型))
擬似乱数生成系	High (固定ブロック長 128 ビット以上、鍵長 256 ビット以上) Normal (固定ブロック長 128 ビット以上、鍵長 128 ビット以上)
公開鍵暗号方式	最良解読計算量が 2^{80} 回 Triple DES 暗号化相当以上を有すること
デジタル署名方式	最良解読計算量が 2^{80} 回 Triple DES 暗号化相当以上を有すること
公開鍵認証方式	最良解読計算量が 2^{80} 回 Triple DES 暗号化相当以上を有すること なりすまし成功確率が 2^{-32} 以下であること

その中で、応募者が準備すべき応募書類として、AES プロジェクトの時とほぼ同じレベルの仕様書と補助文書の記述、参照コード、知的財産権の取り扱い声明書などが指定された。なお、知的財産権の取り扱いについては、AES プロジェクトのように特許無償許諾を強制することはしなかったが、無償許諾が望ましいとした。

一方、公募範囲としては、公開鍵暗号から共通鍵暗号、ハッシュ関数、擬似乱数生成系まで幅広く暗号技術カテゴリを設定し、いくつかのカテゴリについては安全性強度によって複数のレベルに分けた (表 3 参照)。AES プロジェクトが 128 ビットブロック暗号だけを公募したのとは大きく異なる点である。

もう一つ異なる点は選定する暗号技術の数である。AES プロジェクトでは原則として「一つ」だけ選定するとしたのに対し、暗号技術推薦リストには原則として各カテゴリ「二、三個」ずつ選定するとした。

表 4 NESSIE プロジェクトの日程

2000.1	NESSIE プロジェクト開始を宣言	
2000.1	インダストリボードの設立	
2000.3.8	NISSIE 候補暗号公募要綱公開	
2000.9.29	公募締切	
2000.11.13–14	第 1 回 NISSIE 会議開催	1st Phase
2001.6	(第 1 次評価予備審査)	
2001.9.12–13	第 2 回 NISSIE 会議開催	
2001.9.23	最終候補選抜・発表	
2002.2	(第 2 次評価予備選定)	2nd Phase
2002.11.6–7	第 3 回 NESSIE 会議開催	
2003.2.26–27	第 4 回 NESSIE 会議開催	
2003.2.27	NESSIE Portfolio 発表	

約半年の公募期間を経た 2000 年 9 月、世界中から 7 つのカテゴリで合計 39 件の応募暗号技術を受け付けた。約 1 ヶ月の書類審査の後、応募暗号技術すべてを第 1 次評価対象とすることが決まった。

2000 年 11 月の第 1 回 NESSIE 会議で 35 件の応募暗号技術の発表が行われ、その後約 10 ヶ月間にわたり第 1 次評価が実施された。

第 1 次評価期間中、NESSIE プロジェクトの技術運営チームが作成した評価報告書やディスカッションフォーラムなどに投稿された一般からの評価報告などは随時 NESSIE のホームページ上に公開された。また、2001 年 9 月には第 2 回 NESSIE 会議が開催され、世界中の暗号研究者らによる評価報告と質疑応答が行われた。

NESSIE プロジェクトでの大きな特徴としては、ソフトウェア実装評価にも多大な労力をつぎ込んだ点である。とりわけ、ブロック暗号・ストリーム暗号・ハッシュ関数・MAC すべての暗号技術について自ら最適化したコードを作成し、多くのプラットフォーム上で実装性能の評価を実施した。これによって、同程度の最適化レベルで実装されたときの暗号ごとの実装性能が横並びで比較できるようになり、暗号技術の選定に大いに利用された。

これらの情報を基に安全性や実装性能を検討した結果、2001 年 9 月、NESSIE プロジェクトは第 1 次選抜を実施し、25 件の暗号技術を第 2 次評価対象とすることを決定した [15]。

この決定で注目すべきは、Proposed AES に Rijndael が選定されたことを反映したのか、ブロック暗号のカテゴリだけ厳しく絞込みが行われたことである。具体的には、ブロック暗号で第 2 次評価対象に選抜されたのは 17 件中 7 件だけである。しかも、AES と同じ 128 ビットブロック暗号(及び 128 ビットブロックが使える暗号)だけに限れば 10 件中わずか 3 件にすぎない。このような絞込みが行われたのは、選抜基準として「AES に対抗できる安全性と実装性能を有していること」が求められたためと推測される。つまり、安全性はもとより実装性能でも AES と同程度以上でなければ製品化できないとのインダストリボード側の論理が強く働いた可能性がある。

第 2 次評価対象になった暗号技術に対しては、AES プロジェクトと同様、若干の仕様変更(tweak)が認められており、実際に BMGL や PSEC-2、SHACAL などの暗号技術の仕様が変更された。第 2 次評価では仕様変更されたものが評価対象となった。

第 2 次評価に入ってからは、カテゴリごとに 2〜3 個の暗号技術を最終選抜して暗号技術推薦リストを策定するという方針に基づき、安全性と実装性能の両面でさらに詳細な評価が進められた。途中、第 3 回 NESSIE 会議(2002 年 11 月)などをはさみながら、安全性評価報告書やソフトウェア実装評価報告書などが数回まとめられている。

また、非技術的要素として、AES が特許無償許諾であることに対抗するためか、最終選抜の際には、特許無償許諾化を含め、知的財

産権の取り扱いをどのようにするのかという点についても重要な検討項目になった。

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 件、その他の標準的な暗号技術から 5 件の総計 17 件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(巻末表 11 参照)[16]。17 件の暗号技術のうち、ACE Encrypt、ECDSA、GPS を除く 14 件の暗号技術が特許無償許諾もしくはパブリックドメインで利用可能である。

NESSIE プロジェクトは、2003 年 3 月の最終報告書[17][18]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。

NESSIE プロジェクトの最終選抜で注目されるのは、最大の激戦区であったブロック暗号カテゴリにおいて、AES に加えて最終選抜されたのがわずか 3 件の応募暗号だけ(MISTY1, Camellia, SHACAL-2)にとどまったにも関わらず、そのうちの 2 件が日本企業の提案であったことである。「MISTY1」は三菱電機、「Camellia」は NTT と三菱電機の共同開発のブロック暗号である。しかも、MISTY1 は唯一の 64 ビットブロック暗号として、また Camellia は AES と併記された唯一の応募 128 ビットブロック暗号として選定されている。この結果の意味するところは、世界中に数多くあるブロック暗号の中でも、日本企業提案の MISTY1 と Camellia が AES と並んで別格であると欧州で認められた暗号方式として、国際的にも AES と同等に扱われる資格が得られたといえることである。

4. CRYPTREC プロジェクト ― 日本

4.1 CRYPTREC の発足

1997 年 3 月、暗号の利用に関する制度面や技術面における国際的な整合性を図る観点から各国政府が暗号政策を行う際の留意事項をまとめた OECD 暗号政策ガイドライン 8 原則[28]が採択された。これを受けて、今後政府が果たすべき役割として、中立的な立場で暗号技術を評価する機関を設置することや政府が使用する暗号技術の標準化を進めることなどを求めた報告書が複数の政府の研究会で取りまとめられた。

そうした中、日本政府は 1999 年 12 月に決定した「ミレニアム・プロジェクト[21] 」において、2003 年度までに民間から政府及び政府から民間への行政手続きをインターネットを利用してペーパーレスで行える電子政府の基盤を構築する方針を示した。そのための実施施策として、電子署名・認証法などの整備とともに、通商産業省(現経済産業省)を主管としてセキュリティ技術開発を推進することが決められた。

これに基づいて、2000 年 4 月、通商産業省は「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－[22] 」と題した具体的なアクションプランを策定した。それには 4 つのプログラムが組まれており、そのうちの一つが「電子政府における情報セキュリティ基盤技術である暗号技術の評価(プログラム 3)」である。この具体策として、

- 情報処理振興事業協会(IPA)を事務局として、電子政府において利用され得る暗号アルゴリズムの性能等を技術的・専門的見地から客観的に評価を実施するための「暗号技術評価委員会(仮称)」の設置
- 電子政府における暗号技術実装の必要性に応じ、暗号モジュールの評価などについての検討
- 暗号評価の成果を用いた政府における利用指針策定への貢献、および実施環境の整備
- ISO における暗号アルゴリズムの標準化の検討に際し、我が国としての積極的な貢献、ならびに我が国の暗号アルゴリズムの国際標準化への推進

を挙げた。

この方針を受け、IPA では、今井秀樹東京大学生産技術センタ教授を委員長、辻井重男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 Committee[4])を 2000 年 5 月に発足させた[19]。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

[4] 2001 年度以降は、Cryptography Research & Evaluation Committees の略称に変更

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。

2000 年度の CRYPTREC では、暗号技術が電子政府での利用に資するかを判断するための評価に向け、主に以下の 4 つの活動を実施した。

(1) 暗号技術の公募
(2) 評価対象の暗号技術について国内外で活躍する暗号研究者への評価依頼
(3) 評価依頼した暗号研究者からの評価報告書や学会発表、CRYPTREC へのコメントなどをもとにした評価判断
(4) 評価報告書の発行

その後､2001 年 1 月に政府は IT 基本法(高度情報通信ネットワーク社会形成基本法)を成立させた。この法律に基づいて、5 年以内に世界最先端の情報技術(IT)国家となることを目指した「e-Japan 戦略[23] 」を、また 3 月には具体的行動計画となる「e-Japan 重点計画[24] 」をそれぞれ決定した。その重点計画の「6. 高度情報通信ネットワークの安全性及び信頼性の確保」の実施施策の一つとして、総務省及び経済産業省が主管となった「暗号技術の標準化の推進」がある。この施策と通商産業省のアクションプランとの大きな違いは、電子政府システムなどに利用する暗号技術の「評価を実施」するのではなく､「標準化を推進」するに変わったことである。つまり、技術的な評価を実施するだけでなく、その評価結果を政府の施策に反映していくことが正式に決定されたことになる。

このような施策の変更に伴い、2001 年度から CRYPTREC の主管官庁が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 IPA と通信・放送機構(TAO)の共同事務局となった。

2001 年度／2002 年度の CRYPTREC での主たる目的として、

- 2000 年度の継続評価対象の暗号技術
- 2001 年度の応募暗号技術
- CRYPTREC によって評価が必要と判断された暗号技術
- 電子署名･認証法に係る指針に記載された暗号技術
- SSL/TLS に利用されている暗号技術及びそのプロトコル

について、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評価を実施し、これらの評価成果をもとに最終的に「電子政府推奨暗号リスト」を 2002 年度末までに作成することになった。

4.2 電子政府推奨暗号リストが出来るまで

CRYPTREC でも、短い期間ではあったが 2000 年 6～7 月と 2001 年 8～9 月の 2 回､電子政府システムで必要とされる暗号技術を公開鍵暗号技術、共通鍵暗号技術、ハッシュ関数、擬似乱数生成系のカテゴリに分けて公募を行った(表 5 参照)。CRYPTREC の公募要綱によれば、応募者が準備すべき応募書類として、仕様書と補助文書、参照コード(共通鍵暗号技術のみ必須)､知的財産権の取り扱い声明書など、AES プロジェクトや NESSIE プロジェクトとほぼ同じものが要求された。

表 5 CRYPTREC 公募カテゴリ

技術カテゴリ		内容
公開鍵暗号技術	守秘	守秘の機能を有する暗号スキーム (公開の通信路または記録媒体を介して正当な利用者以外には知られないように電子情報を共有する)
	認証	認証の機能を有する暗号スキーム (被認証者の正当性を検証者が確認する)
	署名	署名の機能を有する暗号スキーム (電子情報の正当性を確認する機能のことであり、署名作成者の確認機能と電子情報自体の改ざんの有無を確認する機能の両方からなる)
	鍵共有	鍵共有の機能を有する暗号スキーム (公開の通信路を用いて共通鍵暗号技術を利用する際に送信者と受信者の間で鍵情報を共有する)
共通鍵暗号技術	64 ビットブロック暗号	ブロック長 64 ビット、鍵長 128 ビット以上を利用するブロック暗号
	128 ビットブロック暗号	ブロック長 128 ビット､鍵長 128 ビット以上を利用するブロック暗号
	ストリーム暗号	鍵長 128 ビット以上を利用するストリーム暗号
ハッシュ関数		160 ビット以上のハッシュ値を発生させるハッシュ関数
擬似乱数生成系		公開鍵暗号技術で用いる乱数や共通鍵暗号技術のセッション鍵生成等の用途に適した乱数生成アルゴリズム

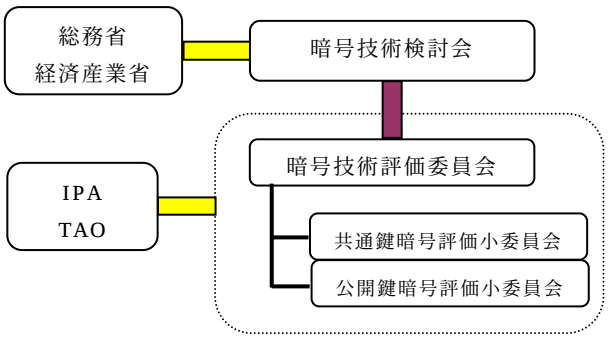

図 1 CRYPTREC 体制

その一方、運営方針などその他の点に関しては異なる点のほうが多い。

例えば、評価・選定の体制は図 1 に示すように、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評価を実施し、第一次判定を行う。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)を行う。さらに、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多階層構造になっている。

ちなみに、AES プロジェクトでは「AES 技術検討チーム」が、NESSIE プロジェクトでは「技術運営チーム」がそれぞれ評価・選定を一手に引き受けている。

評価の手順にも違いがある。CRYPTREC プロジェクトでは、応募暗号技術に対してスクリーニング評価と詳細評価を実施し、評価が必要と判断した暗号技術に対して詳細評価のみを実施することが明記された。

スクリーニング評価とは、応募書類をベースに、①安全性に明らかな問題点がないか、②第三者による実装が可能であるか、の二点を中心に評価を実施し、詳細評価対象暗号にするか否かの判断を行う。内容的には、AES プロジェクトや NESSIE プロジェクトにおける書類審査段階に近い。

詳細評価とは、電子政府で利用可能な安全性を有しているか否かの観点から以下の評価を実施する。

- 既知の攻撃法による統一的な評価
- 各暗号技術の個別の安全性評価(特有の攻撃法に対する耐性)
- パラメータや鍵の設定基準に問題がないかどうかの評価

詳細評価結果に基づいて、安全性に特に問題がないと判断された暗号技術は電子政府暗号候補として監視状態に置かれる。

また、CRYPTREC プロジェクトでもソフトウェア実装性能の評価を一部実施している。しかし、AES プロジェクトや NESSIE プロジェクトの場合とは異なり、評価の付帯情報の一つとしての位置付けであり、電子政府推奨暗号リスト選定の際に利用する評価結果ではない。

電子政府推奨暗号リストの作成において、その選定個数は「原則複数」としか明示されていなかった。そのため、技術的な側面からのさらなる絞込みは行われずに、2002 年 11 月時点で監視状態に置かれていた暗号技術は、特別な事由(おおむね非技術的要因)がない限り、電子政府推奨暗号リストに選定された。AES プロジェクトや NESSIE プロジェクトが最終選抜個数を限定した 2 段階の選抜プロセスを採用したのとは異なるアプローチであった。

表 6 CRYPTREC の日程

2000.5	暗号技術評価委員会の設置
2000.6–7	2000 年度暗号技術の公募
2000.8–10	2000 年度スクリーニング評価
2000.10 –2001.3	2000 年度詳細評価
2001.4	CRYPTREC Report 2000 の発行
2001.5	暗号技術評価報告会(2000 年度)開催
	暗号技術検討会の設置
2001.8–9	2001 年度暗号技術の公募
2001.10	応募暗号説明会開催
2001.10 –2002.3	2001 年度詳細評価(2001 年度詳細評価対象暗号) 2001 年度スクリーニング評価(2001 年度新規応募暗号)
2002.1	暗号技術評価ワークショップ開催
2002.3	CRYPTREC Report 2001 の発行
2002.4	暗号技術検討会 2001 年度報告書の発行
	暗号技術評価報告会(2001 年度)開催
2002.4 –2003.2	2002 年度詳細評価(2002 年度詳細評価対象暗号)
2002.11	電子政府推奨暗号リスト案の公開
2003.2	電子政府推奨暗号リストの決定
2003.3	CRYPTREC Report 2002 の発行
	暗号技術検討会 2002 年度報告書の発行
2003.5	暗号技術評価報告会(2002 年度)開催

もう一点異なるのは、2003 年度までに電子政府システムの基盤を構築するため、2003 年度までに「製品」としての調達可能性を要求したことである。このため、新たに開発する暗号技術を求めるというよりは、すでに製品として存在するか近々製品供給が始まるような暗号技術を事実上求めることとなった。このため、AES プロジェクトや NESSIE プロジェクトでは評価コメントを反映した仕様変更を途中で認めることによって技術的によりよい暗号技術へ修正することを認めたのに対し、CRYPTREC プロジェクトでは製品供給が始まるような暗号技術に仕様変更を認めるべきではないとの立場をとった。

2000 年度の CRYPTREC では、応募暗号技術 47 個を含む、総計 56 個の暗号技術について、スクリーニング評価と詳細評価を実施した。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最終的な評価結果の判定が行われ、安全性上の問題点などが明確に指摘されなかった 23 個の暗号技術を 2001 年度継続評価対象(監視状態の暗号技術を含む)とする決定を行った。

2001 年度は、15 個の新規応募暗号技術を受け付け、さらに評価が必要な暗号技術として 6 件の詳細評価と SSL/TLS における安全性評価を加えた。これにより、スクリーニング評価 15 件、詳細評価 29 件、SSL/TLS における安全性評価が行われた。その結果、安全性上の問題が指摘されたり、電子政府暗号候補の対象からは除外されている暗号技術を除いた総計 32 個の暗号技術を 2002 年度継続評価対象(監視状態の暗号技術を含む)とする決定を行った。

2002 年度は、新規公募を行わず、評価が必要な暗号技術 4 個を加えた総計 36 個の暗号技術について詳細評価を実施した。そして、安全性に特に問題がないと判断された暗号技術のうち、31 個を電子政府推奨暗号リスト(巻末表 11 参照)に掲載することとし、2003 年 2 月に最終確定した[25]。

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)及び「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く予定である。

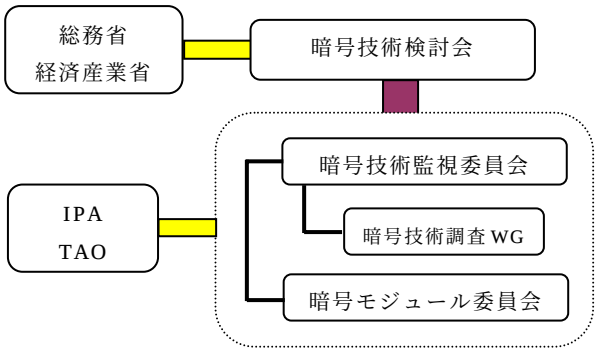

図 2 2003 年度の CRYPTREC 体制

2002 年度末をもって一区切りを迎えた CRYPTREC プロジェクトであるが、今後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、若干の体制変更を伴いながらも活動そのものは継続することになっている(図 2 参照)。

5. プロジェクトの比較

本節では、AES プロジェクト、NESSIE プロジェクト、CRYPTREC プロジェクトについて比較する。これらのプロジェクトは、応募暗号技術を中心に安全性や実装性能などを客観的に評価するという点は同じであるが、その目的や体制、運営方法など大きく異なる点も数多くある。特に注目すべき項目について表 7 にまとめる。

この比較表からもわかるように、AES プロジェクトと NESSIE プロジェクトでは、評価体制や最終成果、公募カテゴリなどについて異なるものの、その他の項目はよく似ている。

とりわけ「透明で開かれた選考プロセス(Transparent and Open Process)」を標榜し、評価・選抜の判定に用いる情報はプロジェクト運営チーム内部だけで議論するのではなく、幅広く一般参加者と議論しながら結論を導いていく姿勢をとった点は全くといっていいほど同じである。具体的には、応募者や暗号研究者、ベンダ、ユーザなどから幅広く意見を聞き、公開の場で討論を行うことができるように、Web 上にディスカッションフォーラムを設置し、国際会議と同じような規模の AES 候補会議や NESSIE 会議を評価期間中に数回開催した。また、暗号国際学会などにもプロジェクトの運営スタッフが積極的に参加し、プロジェクトへの参加を呼びかけるなど PR 活動にも余念がなかった。

こうした運営スタッフの多大な努力の甲斐あって、対外的な注目度が飛躍的に高まり、世界中の多くの研究者から安全性や実装性能に関する評価報告が多数寄せられた。そして、実際にオープンな場で選抜に利用する評価データや意見の分かれる議題について多くの議論が行われた結果、評価データの信憑性が高まり、選抜結果に対するコンセンサスを得やすくすることに多大な効果をもたらした。

選定の手順に関しては、最終的に選定する暗号技術の個数が「一つ(AES プロジェクト)」あるいは「二、三個(NESSIE プロジェクト)」と事前に明言されていたため、結果として「極めて優秀な暗号技術を選抜」するための選定プロセスが採用されている。具体的には、応募暗号技術のなかから最終選抜される可能性のあるものだけを選び出す第 1 次評価と、第 1 次評価で選ばれた暗号技術のなかから特に優秀なものを選抜する第 2 次評価の二段階選抜方式を採用した。

このため、選抜に際しては、安全性だけでなく、むしろそれ以上に実装性能についても厳しく評価している。これは、安全性には大きな差が生じないような暗号技術であっても設計方針によって実装性能は大きく異なるためである。つまり、「必要十分な学術的安全性を有していれば、より優れた実装性能をもつ暗号を選抜」することを評価プロセスの中心に据えていたことを意味する。

両プロジェクトとも、このような運営方針を採用することによって、世界中からの暗号研究者やベンダ、ユーザなどのコメントを踏まえ、安全性・実装性能の両面で優れた少数の暗号技術を選抜したことになっている。このため、政府用、産業推薦用という当初の名目上の差はあるにせよ、実際には国際的にも認められた「安全性・実装性能の両面で優れた暗号技術」を選抜した形となっており、今後の国際標準暗号への布石ともなっている。

これに対し、CRYPTREC プロジェクトの評価・運営プロセスは大きく異なっている。

そもそもの目的が、応募暗号技術を中心に、電子政府システムでの利用に資する「一定水準以上の安全性」を有しているかどうかを客観的に評価し、その基準に合格した暗号技術を電子政府推奨暗号リストに掲載することである。つまり、少数の優秀な暗号技術を選抜するのではなく「一定水準以上の安全性を有している暗号技術に合格書を出す」ことが目的となっている。このため、CRYPTREC プロジェクトでは安全性評価のほうに大きく重心が置かれた。

実際の運営では、4 つの委員会(とりわけ 2 つの小委員会)が中心となって自ら客観的な評価を行う体制であった。このため、評価期間中の委員会審議・評価概要は基本的に非公開とされた一方、年度末報告書[26][27]の形で安全性や実装性能の評価結果が公開された。また、一般から幅広く意見を聞き、公開の場で討論するための技術討論ワークショップの開催やディスカッションフォーラムの設置などは行われなかった一方、CRYPTREC 委員会が評価結果を発表する暗号技術評価報告会が開催された。

このように、対外的な注目度や民間への訴求効果を意識して透明で開かれた選考プロセスを標榜した AES プロジェクトや NESSIE プロジェクトとは異なり、CRYPTREC プロジェクトでは、あくまで高度な信頼性および安全性に支えられた電子政府システムの構築

表 7 AES プロジェクト/NESSIE プロジェクト/CRYPTREC プロジェクトの比較表

	AES プロジェクト	NESSIE プロジェクト	CRYPTREC プロジェクト
評価体制	〔主管〕NIST 〔根拠〕コンピュータセキュリティ法をはじめとする法的権限に基づき NIST が実施する。 〔体制〕NIST 内部に「AES 運営チーム」と「AES 技術検討チーム」を組織する。 NSA が技術サポートを行う。	〔支援〕欧州連合 〔根拠〕欧州委員会策定の第 5 次情報社会技術研究開発プログラムの一つとして実施する。 〔体制〕欧州の大学に属している暗号研究者による「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」を組織する。技術運営チームが実際の評価と運営を担当、インダストリボードが産業界の意向を反映する。	〔主管〕総務省・経済産業省 〔根拠〕政府決定の e-Japan 戦略、e-Japan 重点計画に基づいて実施する。 〔体制〕国内の高度な専門的知識を有する学識経験者らによる「暗号技術検討会(総合判定担当)」と「暗号技術評価委員会(技術評価担当)」を組織する。実際の評価を担当する「共通鍵暗号評価小委員会」「公開鍵暗号評価小委員会」を設置する。

	AES プロジェクト	NESSIE プロジェクト	CRYPTREC プロジェクト
活動期間	約 5 年間(1997.1 – 2001.11)	約 3 年間(2000.1 – 2003.3)	約 3 年間(2000.5 – 2003.3)
公募期間	9 ヶ月(1997.9.12 – 1998.6.15)	6 ヶ月半(2000.3.8 – 2000.9.29)	2000 年度：1 ヶ月 (2000.6.13 – 2000.7.14) 2001 年度：2 ヶ月 (2000.8.1 – 2000.9.27)
評価期間	第 1 次：1998.8.20 – 1999.4.15 第 2 次：1999.8.10 – 2000.5.15	第 1 次：2000.11.13 – 2001.9.22 第 2 次：2001.9.23 – 2003.2.26	2000 年度：2000.10 – 2001.3 2001 年度：2001.10 – 2002.3 2002 年度：2002.4 – 2003.2
最終目標	安全性と実装性能に優れた「一つ」の暗号技術を米国政府標準暗号 AES として策定	欧州企業の国際競争力強化及び研究開発力維持に有効な、安全性と実装性能に優れた推薦暗号技術をカテゴリごとに「二、三個」選抜	電子政府システムでの利用に資する、一定水準以上の安全性を有する「複数」の暗号技術をリストアップ
成果の利用	米国政府標準暗号 AES を策定。 FIPS として連邦政府システムでの利用を義務付ける(強制)。	暗号技術推薦リストを選定。 欧州産業界のデファクトスタンダード化、及び ISO/IEC 国際標準化、IETF 標準化など各種国際標準化への推進を図る(産業標準化)。	電子政府推奨暗号リストを作成。 電子政府システムにおいて可能な限り利用する(推奨)。
評価プロセス	☐ 書類審査 ☐ 第 1 次評価（5 個以下の最終候補を選抜するための評価） ☐ 第 2 次評価（Proposed AES を選抜するための評価） ☐ Proposed AES の FIPS 化作業	☐ 書類審査 ☐ 第 1 次評価（第 2 次評価対象候補を絞り込むための評価） ☐ 第 2 次評価(暗号技術推薦リストに選抜するための評価)	☐ スクリーニング評価（詳細評価を実施するか否かを判定するための評価） ☐ 詳細評価（電子政府で利用可能かどうかを判定するための評価）
一般公募型技術討論会	AES 候補会議を 3 回開催(内 1 回は応募者による発表会)	NESSIE 会議を 4 回開催(内 1 回は応募者による発表会)	なし(応募者による発表会と CRYPTREC による報告会のみ)
応募暗号技術の仕様変更	第 2 次評価に入る前に、最終候補については若干の仕様変更(tweak)を認める	第 2 次評価に入る前に、第 2 次評価対象候補については若干の仕様変更(tweak)を認める	仕様の変更は原則として認めない
知的財産権の取り扱い	世界中において、非排他的に特許無償許諾を実施	非排他的に特許無償許諾が望ましいが、必須ではない	複数の暗号技術が併記される場合には特許無償許諾を義務付けない
公募カテゴリ	128 ビットブロック暗号のみ	公開鍵暗号技術 共通鍵暗号技術 ハッシュ関数 擬似乱数生成、など	公開鍵暗号技術 共通鍵暗号技術 ハッシュ関数 擬似乱数生成
評価対象とする暗号アルゴリズム	“完全かつ適切”なものと認定された 15 個の応募暗号技術	☐ “完全かつ適切”なものと認定された 39 個の応募暗号技術(修正版を含めると 42 個) ☐ NESSIE が必要と判断した暗号技術	☐ 応募暗号技術すべて ☐ 評価が必要と CRYPTREC が判断した暗号技術
評価に利用する情報	☐ NIST や NSA による評価結果 ☐ AES 候補会議(及び連続開催された暗号国際会議)での一般発表論文ならびに質疑応答 ☐ パブリックコメント ☐ ディスカッションフォーラムでの議論 ☐ その他の有力な暗号国際会議での発表論文	☐ NESSIE による評価結果 ☐ NESSIE 会議での一般発表論文ならびに質疑応答 ☐ パブリックコメント ☐ ディスカッションフォーラムでの議論 ☐ その他の有力な暗号国際会議での発表論文	☐ 国内外の主要な暗号研究者による外部委託評価報告書 ☐ 国内研究会を含む、暗号学会での発表論文 ☐ パブリックコメント ☐ 使用実績

に貢献するための客観的な安全性評価を主体的に行うことに主眼が置かれた。

CRYPTREC プロジェクトの成果は、電子政府システムを対象にしたものとはいえ、日本有数の暗号研究者らが中心となって「学術的な安全性を有している暗号技術」を取りまとめた電子政府推奨暗号リストを初めて公式に作成したことにある。暗号技術の安全性を(暗号開発ベンダだけではなく)第三者に客観的に評価してもらう風潮が乏しかった日本において、第三者による評価の重要性を知らしめた点で画期的であった。

6. 今後の展望 – 理論から実装へ

6.1 ISO/IEC 国際標準暗号策定へ

ISO/IEC JTC1/SC27 では、従来からの方針を変更し、2000 年から ISO/IEC 国際標準暗号(ISO/IEC18033)を初めて策定する作業を開始した。ちなみに、ISO/IEC9979 は暗号方式の「登録制度」なのであって、ISO/IEC 国際標準暗号ではないことに注意されたい。事実上の世界標準暗号である DES さえも ISO/IEC 国際標準暗号ではないのである。

ISO/IEC18033 では、公開鍵暗号と共通鍵暗号(ブロック暗号・ストリーム暗号)を対象に、安全性評価が客観的に行われた、限られた数の暗号を選定する方針を打ち出している。各国の ISO/IEC 国内委員会から提案された暗号について、安全性や実装性能を比較して、2005 年頃を目途に各カテゴリ数個(二、三個)ずつの ISO/IEC18033 国際標準暗号を選定していく予定である。

このため、世界中の暗号研究者が評価に関与した AES プロジェクト、NESSIE プロジェクト、CRYPTREC プロジェクトの成果が ISO/IEC18033 標準化作業に大きな影響を与えることになると考えられており、事実これらのプロジェクトで選定された暗号技術を軸に現在審議が進んでいる(巻末表 11 参照)。逆に言えば、これらのプロジェクトで一定以上の評価を受けていない暗号が ISO/IEC18033 国際標準暗号に選定される可能性は、よほどの事由がない限り、かなり低いといえる。

6.2 暗号理論ベースから実装ベースへ

日米欧とも「学術的に安全」な標準暗号・推奨暗号を選定し終えた。この「学術的に安全」とは、攻撃者から秘密鍵が秘匿され、計算途中の結果を読み出せない、という条件の下で、現在知られている攻撃方法を用いても解読できない、ということを意味する。

ところが、暗号を実装する際に往々にしてこの「前提条件」が破られることがある。つまり、実装上の問題や不手際があると、外部からの何らかの攻撃手段によって秘密鍵が直接露呈したり、計算途中の結果がわかったりする場合がある。このようなことが起きると、暗号そのものを攻撃しなくても入手した情報を使って暗号を解読することができるようになるため、どんなに学術的に安全な暗号を使っていたとしても安全性を維持することは一般に難しくなる。

そこで、今後は、学術的に安全な暗号を使うことはもちろん、その暗号を正しく安全に実装することがより重要になってくる。

米国政府は、米国政府標準暗号を含む FIPS 規定のアルゴリズム(Approved Algorithms)やガイドライン、プロトコルなどを正しく安全に実装されているかを検査するため、暗号モジュールの実装に関する認証プログラム CMVP (Cryptographic Module Validation Program)[8]を 1994 年から開始している。現在はカナダ政府機関 CSE と共同で運用しており、FIPS140-2[9]として規定されている。

FIPS140-2 では、暗号モジュールが期待したセキュリティ機能を担保する－つまり、暗号技術が正しく動作し、かつ不正な行為を検知・防御する－ために、暗号モジュールが実現すべきセキュリティ要件を、11 個の要素カテゴリに分割し、それぞれの要素カテゴリごとに 4 段階のセキュリティレベル(Lev1 – Lev4)で規定している。このセキュリティレベルは暗号モジュールの安全性強度に直結しており、レベルが高くなるほど要求されるセキュリティ要件が厳しくなる。例えば、セキュリティレベルが高くなるほど、暗号モジュールに対する攻撃の検知や防御がより強固になり、また万が一、防御が破られる事態になったときには自動的に暗号モジュールとしての機能を喪失(自爆)させるなどの対策が組み込まれるようになる。

一般に Lev2 程度あれば商用製品としての暗号モジュールとして十分なセキュリティ機能を、Lev4 であれば軍用製品としての暗号モジュールとしても利用可能なほどの強固なセキュリティ機能を実現している。

実際の認証方法としては、暗号モジュールが必要なセキュリティレベルの対策を満足しているかを第三者検査機関が検証することによって実装の妥当性を確認し、検査に合格した暗号モジュールには NIST/CSE から FIPS140-2 認証が与えられる。

現在のところ、このような暗号モジュールの実装に関する検査・評価体制は、世界的にも FIPS140-2 しかないため、ISO/IEC JTC1/SC27 では FIPS140-2 をモデルとした暗号モジュール検査・評価体制についての検討を開始した。当面は、暗号モジュールの要求条件だけを取りまとめる ISO/IEC19790 が先行する形となる。その際の承認アルゴリズム(Approved Algorithm)として、ISO/IEC 9796, ISO/IEC10118, ISO/IEC18033 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。

日本でも、CRYPTREC プロジェクトの暗号モジュール委員会(図 2 参照)で、暗号モジュールの実装に関する検査・評価体制の検討を始めている。

6.3 「暗号が安全である」とは ― 評価基準

「暗号は安全でなければならない」ことに異論をはさむ人はいないであろう。ところが、安全かどうかの「基準」について多くのコンセンサスが得られているとは言いがたい。

確かに、暗号研究者の中では一定のコンセンサスが得られた「学術的な安全性基準」がある。例えば、公開鍵暗号であれば最強の安全性である IND-CCA2 を満たすことを証明すること、共通鍵暗号であれば鍵全数探索よりも効率的な解読法が見つからないこと、などなど。では、それらの条件を満たさない暗号は安全ではない、といえるのであろうか。

一つ目の解は、暗号研究者らがよくいうように、理想的な(期待される)安全性を下回ったのだから「その暗号は学術的に安全とはいえない」という結論である。

例えば、128 ビットブロック暗号の場合の安全性基準は表 9 のようになる。

暗号研究者は、選択平文攻撃であっても、2^{128} 以下の解読計算量で解読できる攻撃方法が見つかれば「その暗号は破れた(broken)」と報告する。その際、2^{80} 以上の解読計算量を実現できる技術は現存しない(2^{64} 以上の解読計算量でも解読に数年以上かかる)、あるいは 100Mbps のネットワークを 24 時間数ヶ月間流しつづけた伝送量に等しいだけの平文と暗号文の組合せを攻撃者は知る必要がある、といった実利用環境における実現可能性は特に考慮せず、解読計算量だけで安全性の判断が行われる。

もう一つの解は、現実の利用環境下のアプリケーションにおいて解読できないのであれば現実的な脅威とはならないのだから「その暗号は現実には安全である」という結論である。この場合は、解読計算量よりも実利用環境における実現可能性に照らし合わせて安全性の判断が行われる。

表 8 攻撃モデル

暗号文単独攻撃	(多数の)暗号文から秘密鍵などを見つけ出す
既知平文攻撃	平文とそれに対応する暗号文のペアを(一般には多数)知っているという条件下で秘密鍵などを見つけ出す
選択平文攻撃	攻撃者が解読に利用する(一般には多数の)平文を選択し、それに対応する暗号文のペアを知っているという条件下で秘密鍵などを見つけ出す
選択暗号文攻撃(公開鍵暗号の場合)	攻撃者が解読に利用する(一般には多数の)暗号文を選択し、それに対応する平文のペアを知っているという条件下で秘密鍵などを見つけ出す

表 9 128 ビットブロック暗号の基準

計算量	大まかな基準概要
2^{128}	理想的な安全性基準 計算量がこの基準を上回れば鍵全数探索による攻撃が最良の攻撃方法であることを意味し、「学術的に安全である」という
2^{80}	20 年後までに計算機探索が実際に出来る可能性があると言われている計算量
2^{64}	世界中のボランティアの協力のもと約 5 年かかって達成した計算量(RC5-64 Challenge)
2^{56}	世界中のボランティアの協力のもと約 1 日で達成した計算量(DES Challenge)
2^{40}	1 台のパソコンでも実現可能な計算量

このような「安全性」の解釈について、NIST は非常に現実的な判断を下している。具体的な例を以下に示す。

AES プロジェクトでは、MAGENTA の安全性について、「2^{64} 個の選択平文を用いた中間値一致攻撃により 2^{64} 回の暗号化処理で解

読可能である。また、2^{33} 個の既知平文を用いたときは 2^{97} 回の暗号化処理で解読可能である。したがって MAGENTA は安全ではない」と NIST は判定した。

その一方、DES については 1997 年に鍵全数探索法によって実際に解読されたにも関わらず、「2004 年までに Triple DES か AES へ移行」するよう求めるだけで米国政府標準暗号からは除外していない。つまり、鍵全数探索法による解読が成功してもなお「DES の安全性低下は一刻を争うほど致命的ではない。今後数年間はほとんどのアプリケーションで安全に利用できる」と NIST は判定した。

客観的に見れば、DES よりも MAGENTA のほうが安全であろう。それなのに反対の結論を NIST が下した理由としては、「新規の暗号を選定」するのか「運用中の暗号を維持」するのかによって、利用した安全性の判断基準が異なったとしか考えられない。

AES 選定のように新規の暗号を選択するのであれば、より安全な暗号を選ぶべきである。つまり、学術的な安全性に問題のある暗号をあえて選択する必要はなく、暗号研究者が使う「2^{128}」を安全性の判断基準としたのであろう。

一方、DES のように一度標準暗号として運用を始めた暗号については、「そのまま運用したときに発生する安全性に関するリスクと連邦政府システムの可用性を停止させることに伴うデメリットを比較したときに、前者のリスクが明確に上回るかどうか」という安全性の判断基準を使っているように思われる。つまり、暗号解読事例が発表されたとしても、実利用環境において暗号機能が喪失するような現実的な脅威が差し迫っているのでない限り、現在運用中の暗号を直ちに利用停止する必要性はなく、システム更新時などに合わせて新しい暗号に移行させれば十分である、ということである。

このような NIST の考え方は非常に重要である。つまり、情報システムの構築時にはできる限り安全な暗号技術を採用するよう心がけるべきであるが、一度運用を開始したら暗号解読法が発表されても過剰な反応をしないことである。なぜならば、十分に高い安全性を有している暗号技術をシステム構築時に採用していれば、仮に暗号解読法が発表されたとしても、直ちに(数年以内に)実利用環境における現実的な脅威となる可能性は一般に低いためである。次回のシステム更新時を目途に今後の運用期間を考慮して継続使用するか代替するかを決めればよい。

表 10 安全性の解釈

事象	解釈
最強の安全性証明付き、もしくは多角的評価の結果として理論的な解読方法が未発見	新たに暗号技術を導入する場合で相互接続性維持などの特別な理由がないのであれば、このカテゴリの暗号技術を選択すべきである。
最強の安全性証明なし、もしくは多角的評価の結果として理論的な解読方法が提案	新たに暗号技術を導入する場合でも相互接続性維持などの特別な理由があるならば、このカテゴリの暗号技術を選択してもよい。 運用中の暗号技術に対してはこの種の結果を気にする必要性はあまりない。
理論的な解読方法の実験に成功	新たな暗号技術を導入する場合、このカテゴリの暗号技術を選択することは避けるべきである。 攻撃モデルや解読計算量にも依存するが、運用中の暗号技術に対しては一般に中長期的なシステム更新に合わせて暗号技術の変更を検討すべきである。
鍵全数探索法による解読に成功	このカテゴリの暗号技術は新規に採用してはならない。 運用中の暗号技術に対しても、比較的早い時期での暗号技術の変更を実施すべきである。なお、解読計算量が小さく解読の危険性が非常に高ければ、運用の緊急停止も視野にいれる必要がある。
実装攻撃による解読に成功	実際の利用環境において、この攻撃方法での前提条件と同様の条件が整うのであれば、この種の実装方法を採用してはならない。また、採用している場合には速やかな代替実装製品への交換が必要である(安全な実装方法に代わっていれば同じ暗号技術のままでもよい)。 それ以外の場合には、このような攻撃方法があることを実装ベンダが注意しておけばよい。
第三者の安全性評価を受けていない	独自もしくは第三者の暗号専門家に依頼して安全性評価を行ったうえで導入の是非を検討すべきである。少なくとも、暗号開発ベンダ独自の安全性主張だけで安全性を判断すべきではない。

学術的な安全性の議論とは別に、より現実的な影響をもたらす可能性があるものとして、実装上の弱点を利用した攻撃(実装攻撃)

に対する安全性の議論がある。具体的には、暗号処理中の有意なデータ変動(消費電力や処理時間等)やメモリ情報(退避データや蓄積データ等)を何らかの手段で取得・分析するなどして、秘密鍵を入手したり計算途中の結果を露呈させるなど、暗号が安全に機能するための「前提条件を損なう」ような攻撃法に対する安全性である。このような攻撃法に対して脆弱性があると、実質的に暗号処理がバイパスされるなど、暗号を利用する上での現実的な脅威となりうる。

しかしながら、6.2 節でも述べたように、学術的に暗号が解読されることとは本質的に異なる。一般に、暗号が安全に機能するための前提条件を損なわないように十分な注意を払って実装すれば、あるいは前提条件を損なうような環境で利用しなければ、この種の攻撃に対しての問題点は回避できる。注意すべきはあくまで暗号の実装方法や利用環境であって、暗号そのものの安全性ではない。

7. まとめ

米国や欧州では過去にも暗号技術の評価や選定を行った実績がある。そのためか、AES プロジェクト、NESSIE プロジェクトとも壮大なプロジェクトであった割には、極めて順調な運営が行われたものと感じている。オープンな評価・選定プロセスには世界中から賞賛の声が贈られており、今後の重要な成果として利用されることは間違いない。

これに対し、日本では CRYPTREC プロジェクトが公式な暗号技術評価を実施した初めての経験であった。そうしたなかでも、このプロジェクトでの成果は、電子政府推奨暗号リストの作成に留まらず、NESSIE プロジェクトでの成果と合わせて ISO/IEC 国際標準暗号の策定に関する安全性評価結果として利用されるなど、当初の目的を十二分に達成したプロジェクトといえる。

今後は、AES プロジェクトや NESSIE プロジェクトのように、評価手法や選定基準、安全性評価結果などの情報について、一般参加者と広くオープンに議論してコンセンサスをより一層高めるという施策(例えば技術討論ワークショップの開催やディスカッションフォーラムの設置など)により、さらなるプロセスの改善も可能になるだろう。これらの施策は、委員会審議に伴う応募者間の情報格差の解消や、安全な暗号の評価・選択・利用についての社会全般の幅広い共通的なコンセンサスを追求していく意義付けをより明確することに役立つと思われる。

参考文献

[1] NIST, “Advanced Encryption Standard (AES) Development Effort,” http://csrc.nist.gov/CryptoToolkit/aes/index2.html

[2] NIST, “Status Report on the First Round of the Development of the Advanced Encryption Standard,” http://csrc.nist.gov/CryptoToolkit/aes/round1/r1report.pdf

[3] Nechvatal, Barker, Bassham, Burr, Dworkin, Foti, and Roback, “Report on the Development of the Advanced Encryption Standard (AES),” http://csrc.nist.gov/CryptToolkit/aes/round2/ r2report.pdf

[4] NIST, “Data Encryption Standard (DES); specifies the use of Triple DES,” FIPS PUB 46-3, http://csrc.nist.gov/publications/fips/index.html

[5] NIST, “Escrowed Encryption Standard (EES),” FIPS PUB 185, http://csrc.nist.gov/publications/fips/index.html

[6] NIST, “Advanced Encryption Standard (AES),” FIPS PUB 197, http://csrc.nist.gov/publications/fips/index.html

[7] NIST, “SKIPJACK and KEA Algorithms,” http://csrc.nist.gov/CryptoTookit/skipjack/skipjack.pdf

[8] NIST, “Cryptographic Module Validation (CMV) Program,” http://csrc.nist.gov/cryptval/

[9] NIST, “SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES,” FIPS PUB 140-2, http://csrc.nist.gov/cryptval/

[10] Biham and Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” *Journal of Cryptology*, Vol. 4 No. 1, pp. 3-72, 1991. (The extended abstract appeared at CRYPTO’90)

[11] Matsui, “Linear Cryptanalysis Method for DES Cipher,” *Advances in Cryptology – EUROCRYPT’93*, LNCS **765**, Springer-Verlag, 1993.

[12] Matsui, “The first experimental cryptanalysis of the Data Encryption Standard,” *Advances in Cryptology – CRYPTO’94*, LNCS **839**, Springer-Verlag, 1994.

[13] RSA Laboratories, “Cryptographic Challenges,” http://www.rsasecurity.com/rsalabs/challenges/index.html

[14] NESSIE, “New European Schemes for Signatures, Integrity, and Encryption,” https://www.cosic.esat.kuleuven.ac.be/nessie/

[15] Preneel, Rompay, Granboulan, Martinet, Murphy, Shipsey, White, Dichtl, Serf, Schafheutle, Biham, Dunkelman, Ciet, Quisquater, Sica, Knudsen, and Raddum, “NESSIE Phase I: Selection of Primitives,” https://www.cosic.esat.kuleuven.ac.be/nessie/deliverables/Decision.pdf

[16] NESSIE, “Portfolio of recommended cryptographic primitives,” https://www.cosic.esat.kleven.ac.be/nessie/deliverables/decision-final.pdf

[17] NESSIE, “NESSIE Security Report, Version 2,” https://www.cosic.esat.kleven.ac.be/nessie/deliverables/D20-v2.pdf

[18] NESSIE, “Performance of Optimized Implementations of the NESSIE Primitives, Version 2,” https://www.cosic.esat.kleven.ac.be/nessie/deliverables/D21-v2.pdf

[19] 情報処理振興事業協会セキュリティセンタ,「暗号技術評価事業について」, http://www.ipa.go.jp/security/enc/CRYPTREC/idex.html

[20] 通信・放送機構,「CRYPTREC 情報」, http://www.shiba.tao.go.jp/kenkyu/CRYPTREC/

[21] 首相官邸,「ミレニアム・プロジェクト（新しい千年紀プロジェクト）について」, http://www.kantei.go.jp/jp/mille/

[22] 通商産業省,「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－」, http://www.meti.go.jp/poicy/netsecrity/downloadfiles/esecu01j.pdf

[23] 高度情報通信ネットワーク社会推進戦略本部,「e-Japan 戦略」, http://www.kantei.go.jp/jp/singi/it2/index.html

[24] 高度情報通信ネットワーク社会推進戦略本部,「e-Japan 重点計画」, http://www.kantei.go.jp/jp/singi/it2/index.html

[25] 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/secrity/pdf/cryptrec_01.pdf

[26] CRYPTREC,「暗号技術評価報告書(2002 年度版)」, http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030401_report01.html

[27] 経済産業省、総務省,「暗号技術検討会 2002 年度報告書」, http://www.meti.go.jp/policy/ netsecurity/cryptpress2002.htm

[28] OECD, ``GUIDELINES FOR CRYPTOGRAPHY POLICY,'' 1997.

表 11 標準・推奨暗号一覧表

技術分類		米国標準暗号技術	欧州暗号技術推薦リスト	電子政府推奨暗号リスト (H.15.2.20)	ISO/IEC 国際標準暗号
公開鍵暗号技術	署名	***DSA (FIPS186-2)*** ***RSA (FIPS186-2)*** ***ECDSA (FIPS186-2)***	***RSA-PSS (primary)*** ***ECDSA (secondary)*** SFLASH (special)	***DSA*** ***ECDSA*** ***RSASSA-PKCS1-v1_5*** ***RSA-PSS***	ISO/IEC9796 ISO/IEC14888 ISO/IEC15946-2
	守秘	― ― ―	***PSEC-KEM (primary)*** RSA-KEM (secondary) ACE-KEM (special)	RSA-OAEP RSAES-PKCS1-v1_5 (注 1)	(ISO/IEC18033-2)
	鍵共有	― ― ―	― ― ―	DH ECDH ***PSEC-KEM*** (注 2)	ISO/IEC11770 ISO/IEC15946-3
	認証	FIPS196	GPS	― ― ―	ISO/IEC9798
共通鍵暗号技術	64 ビット ブロック暗号	DES (FIPS46-3) ***Triple DES (FIPS46-3)*** Skipjack (FIPS185)	***MISTY1***	CIPHERUNICORN-E (注 3) Hierocrypt-L1 (注 3) ***MISTY1*** (注 3) ***3-key Triple DES*** (注 3, 注 4)	(ISO/IEC18033-3)
	128 ビット ブロック暗号	***AES (FIPS197)***	***AES*** ***Camellia***	***AES*** ***Camellia*** CIPHERUNICORN-A Hierocrypt-3 SC2000	(ISO/IEC18033-3)
	256 ビット ブロック暗号	― ― ―	SHACAL-2	― ― ―	― ― ―
	ストリーム 暗号	― ― ―	― ― ―	MUGI MULTI-S01 128-bit RC4 (注 5)	(ISO/IEC18033-4)
その他	ハッシュ 関数	***SHA-1 (FIPS180-2)*** ***SHA-256 (FIPS180-2)*** ***SHA-384 (FIPS180-2)*** ***SHA-512 (FIPS180-2)***	Whirlpool ***SHA-256*** ***SHA-384*** ***SHA-512***	RIPEMD-160 (注 6) ***SHA-1*** (注 6) ***SHA-256*** ***SHA-384*** ***SHA-512***	ISO/IEC10118
	擬似乱数 生成系	***PRNG in FIPS 186-2 (FIPS 186-2)***	― ― ―	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1 (注 7) ***PRNG based on SHA-1 for general purpose in FIPS186-2 (+ change notice 1) Appendix3.1*** (注 7) ***PRNG based on SHA-1 for general purpose in FIPS186-2 (+ change notice 1) revised Appendix3.1*** (注 7)	― ― ―
	メッセージ 認証子	MAC (FIPS113) ***HMAC (FIPS198)***	UMAC TTMAC EMAC ***HMAC***	― ― ―	ISO/IEC9797

(注意) 米国政府標準、欧州暗号技術推薦リスト、電子政府推奨暗号リストのうち 2 つ以上の選定されている暗号技術を***太字***で示す。
(注意) (primary)：主選定暗号技術、(secondary)：副選定暗号技術を表す。(special)は汎用目的ではなく、特定の条件を満たす場合に利用可能な暗号技術を示す。
(注意) ISO/IEC18033 は現在審議中である。

【電子政府推奨暗号リストにおける注釈】
(注 1) SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。
(注 2) KEM (Key Encapsulation Mechanism) – DEM(Data Encapsulation Mechanism)構成における利用を前提とする。
(注 3) 新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することが望ましい。
(注 4) 3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。
1) FIPS46-3 として規定されていること
2) デファトスタンダードとしての位置を保っていること
(注 5) 128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。
(注 6) 新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、256 ビット以上のハッシュ関数を選択することが望ましい。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。
(注 7) 擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。