4-9 CRYPTREC活動

4-9 CRYPTREC Activities

黒川貴司　金森祥子
KUROKAWA Takashi and KANAMORI Sachiko

要旨

本稿では2006年度から2010年度にセキュリティ基盤グループが主に担当したCRYPTREC活動を紹介する。主に、暗号アルゴリズムの危殆化と移行、特に、RSA1024ビット及びSHA-1に関することと電子政府推奨暗号リストの改訂に焦点を合わせる。

In this paper, we show the activity of CRYPTREC between fiscal year 2006 and fiscal year 2010 in the security fundamentals group. We focus on compromise and migration of cryptographic algorithms, especially RSA1024 bit and SHA-1, and the revision of the e-Government Recommended Ciphers List.

[キーワード]
暗号アルゴリズム，安全性評価，電子政府推奨暗号リスト，危殆化，ライフサイクル
Cryptographic algorithm, Security evaluation, e-Government Recommended Ciphers List, Compromise, Life cycle

1 まえがき

人間の誕生から死までの一生を成長過程ごとに分けて1つの周期とみなすことをライフサイクルという。この概念の類似に、製品ライフサイクルというものがある。たとえば、製品の販売数に着目すれば、製品が市場に投入されてしばらくの時期を導入期、製品が市場で受け入れられる時期を成長期、製品が市場において購入者にほぼ行き渡るまでの時期を成熟期、製品の売り上げが減少していく時期を衰退期として、4つの過程に分けて製品の寿命というものを考えることができる。また、情報通信に係るシステム開発についていえば、ライフサイクルを企画プロセス、要求定義プロセス、開発プロセス、運用プロセス、保守プロセスの5つの過程に分けることができる。

ある問題の解を計算機に出力させるための実行手順を記述したアルゴリズムというものは、その正当性が数学的に証明されているという意味でいわば恒久的なものなので、一見するとその意味ではライフサイクルという概念を適用するのは相応しくないように思える。一方で、その一種である暗号アルゴリズムには、安全性の強弱を決定するセキュリティパラメータというものが付随し、安全性の確保という観点から寿命が存在するため、ライフサイクルという概念を自然に適用し得る。ゆえに、暗号アルゴリズムの安全性を図るという行為は、そのライフサイクルのどの段階に位置するかを判断する上で必要不可欠なものと考えられるのである。

2 CRYPTRECとは

CRYPTRECとはCryptography Research and Evaluation Committeesの略であり、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である。

2000年度に通商産業省（現経済産業省）から電子政府情報セキュリティ技術開発事業の一環として調査事業を委託された情報処理振興事業協会（現情報処理推進機構）が、電子政府で利用可能な暗号技術を安全性及び実装性など、技術的な面から評価することを目的とした暗号技術評価

委員会を組織し、同委員会の事務局を務めたのがはじまりである。2001年度からは旧通信・放送機構（その後、通信総合研究所と統合され、情報通信研究機構となった）が同委員会の共同事務局として参加した。また、同委員会に加え、総務省大臣官房技術総括審議官及び経済産業省商務情報政策局長が、暗号技術の普及による情報セキュリティ政策の推進を図る観点から専門家による意見などを両省の施策の検討に資することを目的として、暗号技術検討会を設置した。なお、2008年度からは総務省大臣官房技術総括審議官が総務省大臣官房総括審議官に、2010年度からは総務省大臣官房総括審議官が総務省政策統括官に変更になっている。

3 CRYPTREC設立の背景

通信ネットワーク上での電子商取引などを実現していくためには情報通信技術の安全性及び信頼性の確保が不可欠である。インターネットが世界的規模で急速に普及するにつれて、分散型サービス不能（DDoS）攻撃、コンピューターウイルス、不正アクセスやなりすましなどの脅威が懸念されていることから、暗号技術の導入が技術的な予防策の一手段として取られる。つまり、暗号技術が情報の秘匿に加えて、情報の真正性や完全性などを保証するための技術としても用いられてきている。

従来、貿易管理上、暗号技術は情報の秘匿のための武器としての取り扱いを受けてきたが、インターネットの商用利用が拡大してきていることから、署名や認証などの用途で用いられる暗号技術については、規制が緩和されてきている。また、アメリカ合衆国の国立標準技術研究所（National Institute of Standards and Technology, NIST）が新たな政府標準暗号（Advanced Encryption Standard, AES）を選定するためのプロジェクト（1997年から2000年まで）を行い、国際標準化においては、暗号アルゴリズムの登録制度ISO 9979に代わるものとして、暗号アルゴリズムの標準化ISO/IEC 18033が開始されるなど、2000年前後の時期は標準化の機運が非常に高まっていた頃であった。

国内の政策においては、2000年度末に内閣官房のIT戦略本部によって「e-Japan重点計画」が決定され、「客観的にその安全性が評価され、実装性に優れた暗号技術を採用するため、2002年度までに、国際標準化機構（ISO）、国際電気通信連合（ITU）などにおける暗号技術の国際標準化の状況を踏まえ、専門家による検討会開催などを通じて電子政府利用などに資する暗号技術の評価及び標準化を行う。」という文言として挙げられている。

4 CRYPTRECの体制

4.1 2008年度までの体制

2000年度及び2001年度の暗号技術公募と2000年度から2002年度までの暗号技術評価の結果、電子政府における調達のための推奨すべき暗号リスト（電子政府推奨暗号リスト、現リスト（図1））を策定し、2003年2月に公表したが、2003年度以降も電子政府推奨暗号に選定された各暗号の安全性等についての情報収集や評価を行い、必要に応じて修正情報の周知やリストからの削除などの電子政府推奨暗号リストの変更を行うなどの、安全性及び信頼性を確保するための活動を引き続き推進していく必要があるため、4.1.1および4.1.2に述べるような組織改編を行っている（図2）。

4.1.1 暗号技術監視委員会

暗号技術監視委員会は、暗号技術検討会の下に設置され、電子政府推奨暗号の監視、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする調査・検討を行っている。また、具体的な調査・検討に際して暗号技術監視委員会を支援することを目的に、同委員会の下に暗号技術調査ワーキンググループを適宜設置し、検討を行っている。暗号技術監視委員会は情報通信研究機構及び情報処理推進機構の委員会として開催され、総務省、経済産業省、警察庁、外務省、防衛省等がオブザーバとして参加している（図3）。

4.1.2 暗号モジュール委員会

暗号モジュール委員会は暗号技術検討会の下に設置され、ISO/IEC等の国際標準の動向を注視しつつ、将来的に政府調達基準等として利用されることを視野に入れながら、電子政府推奨暗号に準拠した暗号モジュールに対するセキュリティ要件及び試験要件の策定に向けた検討を行っている。

電子政府推奨暗号リスト

平成１５年２月２０日
総　　務　　省
経　済　産　業　省

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5(注1)
	鍵共有	DH
		ECDH
		PSEC-KEM(注2)
共通鍵暗号	64ビットブロック暗号(注3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(注4)
	128ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4(注5)
その他	ハッシュ関数	RIPEMD-160(注6)
		SHA-1(注6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系(注7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

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【著者注:平成17年10月12日付けで、SP800-67に変更された。】
2)デファク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。

図1　電子政府推奨暗号リスト(現リスト)

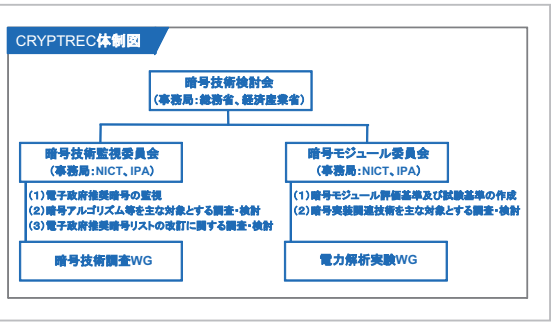

図2　旧CRYPTREC体制図

また、同セキュリティ要件及び試験要件の検討に資するため、暗号実装関連技術に関して、サイドチャネル攻撃及び耐タンパー性に関する調査・検討を行っている。暗号モジュール委員会は情報通信研究機構及び情報処理推進機構の委員会として開催され、総務省、経済産業省、警察庁、外務省、防衛省等がオブザーバとして参加している。

4.2　2009年度からの体制

電子政府推奨暗号リストの改訂に向けて、これまでの主な活動である電子政府推奨暗号の安全性及び信頼性確保のための調査・検討に加えて、暗号技術の運用を主な対象とする調査・検討を進めるために、4.2.1～4.2.3に述べるような組織改

図３ 委員会開催風景

編を行った(図４)。

4.2.1 暗号方式委員会

暗号方式委員会は、2008年度まで開催していた暗号技術監視委員会を引き継ぐ形で、2009年度から組織された。従来、暗号技術監視委員会が担っていた作業に加えて、電子政府推奨暗号リストの改訂に向けた暗号技術の安全性評価及び将来電子政府での利用が見込まれる暗号技術の調査・検討を行うことになった。

4.2.2 暗号実装委員会

暗号実装委員会は、2008年度まで開催していた暗号モジュール委員会を引き継ぐ形で、2009年度から組織された。従来、暗号モジュール委員会が担っていた作業に加えて、電子政府推奨暗号リストの改訂に向けた実装性評価に関する調査・検討を行うことになった。

4.2.3 暗号運用委員会

暗号運用委員会は、新しい電子政府推奨暗号リスト(次期リスト)を策定・運用していくにあたって必要となる暗号技術の運用を主な対象とする調査・検討を行うために、新たに設置された。具体的には、電子政府システム等で利用される電子政府推奨暗号の適切な運用について、システム設計者・運用者の観点から調査・検討を行う。特に、次期リスト策定における暗号技術に対する製品化・利用実績等の評価について評価方針や評価基準等の検討を行う。さらに、電子政府推奨暗号リストと国際標準技術等との整合性についても検討する。また、次期リスト策定における運用監視暗号リストに掲載された暗号技術の取り扱い方針について検討する。システム運用者の観点から、今後危殆化により移行が必要とされた場合、より円滑な作業を可能にするための調査・検討を行う。

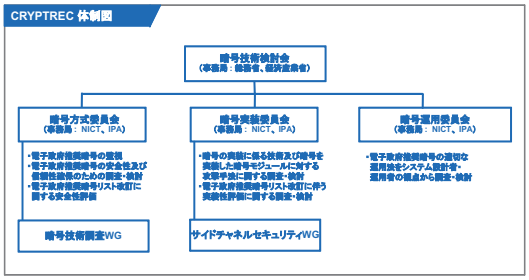

図４ 新 CRYPTREC 体制図

4.3 委員会の開催状況

2006年度から2010年度までの、委員会など各会合の開催日は表１の通りである。

5 第２期中期計画における注目すべき活動

5.1 暗号の危殆化とその移行

暗号アルゴリズムの危殆化とは、暗号アルゴリズムの安全性のレベルが低下した状況、または、その影響により暗号アルゴリズムが組み込まれているシステムなどの安全性が脅かされる状況を指す。一般的には、暗号アルゴリズムが破られたとか、解読されたとか言うが、暗号アルゴリズムに対する解析方法は数多くあり、どの程度暗号アルゴリズムが破られたのか、解読されたのかが説明

表1　第2期中期計画における委員会開催日一覧

平成18年度

暗号技術監視委員会	第1回	平成18年7月24日
	第2回	平成19年3月9日
暗号技術調査WG（公開鍵）	第1回	平成18年8月4日
	第2回	平成18年9月7日
	第3回	平成18年12月27日
	第4回	平成19年2月5日
	第5回	平成19年2月5日
	第6回	平成19年3月7日
暗号技術調査WG（リストガイド）		
暗号技術調査WG（IDベース）		
暗号モジュール委員会	第1回	平成18年7月26日
	第2回	平成18年12月15日
	第3回	平成19年3月15日
電力解析実験WG	第1回	平成18年12月27日
	第2回	平成19年3月2日

平成19年度

暗号技術監視委員会	第1回	平成19年6月5日
	第2回	平成19年11月13日
	第3回	平成20年3月3日
暗号技術調査WG（公開鍵）	第1回	平成19年5月16日
	第2回	平成19年12月18日
	第3回	平成20年2月8日
	第4回	平成20年2月22日
暗号技術調査WG（リストガイド）	第1回	平成19年8月7日
	第2回	平成19年10月17日
	第3回	平成20年1月16日
	第4回	平成20年2月25日
暗号技術調査WG（IDベース）	第1回	平成19年8月7日
	第2回	平成19年10月17日
	第3回	平成20年1月16日
	第4回	平成20年2月25日
暗号モジュール委員会	第1回	平成19年6月6日
	第2回	平成19年7月25日
	第3回	平成19年9月28日
	第4回	平成20年2月15日
電力解析実験WG	第1回	平成19年6月27日
	第2回	平成19年10月5日
	第3回	平成19年12月21日
	第4回	平成20年2月6日

平成20年度

暗号技術監視委員会	第1回	平成20年7月28日
	第2回	平成20年10月28日
	第3回	平成20年12月19日
	第4回	平成21年3月4日
暗号技術調査WG（リストガイド）	第1回	平成20年9月2日
	第2回	平成20年11月28日
	第3回	平成21年1月9日
	第4回	平成21年3月3日
暗号技術調査WG（IDベース）	第1回	平成20年9月11日
	第2回	平成20年11月20日
	第3回	平成20年12月18日
	第4回	平成21年2月17日
暗号モジュール委員会	第1回	平成20年8月1日
	第2回	平成20年10月31日
	第3回	平成20年12月15日
	第4回	平成21年2月20日
電力解析実験WG	第1回	平成20年9月3日
	第2回	平成20年10月3日
	第3回	平成20年11月26日
	第4回	平成21年2月4日

平成21年度

暗号方式委員会	第1回	平成21年8月5日
	第2回	平成22年2月18日
	第3回（合同）	平成22年3月2日～3日
暗号技術調査WG（リストガイド）	第1回	平成21年9月1日
	第2回	平成21年10月22日
	第3回	平成22年2月4日
	第4回（合同）	平成22年3月2日～3日
暗号実装委員会	第1回	平成21年8月5日
	第2回	平成21年10月2日
	第3回	平成22年2月24日
	第4回（合同）	平成22年3月2日～3日
サイドチャネルセキュリティWG	第1回	平成21年9月2日
	第2回	平成22年2月5日
	第3回（合同）	平成22年3月2日～3日
暗号運用委員会	第1回	平成21年10月23日
	第2回	平成22年2月22日
	第3回（合同）	平成23年3月2日

平成22年度

暗号方式委員会	第1回	平成22年7月20日
	第2回	平成23年2月10日
	第3回（合同）	平成23年3月2日
暗号技術調査WG（リストガイド）	第1回	平成22年9月27日
	第2回	平成22年12月2日
	第3回	平成23年2月4日
	第4回（合同）	平成23年3月2日
暗号実装委員会	第1回	平成22年7月23日
	第2回	平成22年9月28日
	第3回	平成23年2月4日
	第4回（合同）	平成23年3月2日
サイドチャネルセキュリティWG	第1回（合同）	平成23年3月2日
暗号運用委員会	第1回	平成22年9月14日
	第2回	平成22年11月4日
	第3回	平成23年1月20日
	第4回	平成23年2月24日
	第5回（合同）	平成23年3月2日

されないと詳しいことは分からない。

そこで、暗号アルゴリズムの安全性評価の状態を以下の4つに分類する。

- 状態1：暗号アルゴリズムの欠陥を利用した有効な攻撃方法が知られていない。
- 状態2：暗号アルゴリズムの欠陥を利用した攻撃方法が提案されているものの、部分的な攻撃成功にとどまっており、学術的な解読に至っていない。
- 状態3：暗号アルゴリズムの欠陥を利用した攻撃方法が提案されており、学術的に解読されている。
- 状態4：暗号アルゴリズムを利用した実際のシステムやアプリケーションにおいて現実的な脅威となる攻撃方法が示されている。

これらのうち、状態2における「部分的な攻撃成功」の状態は、公開鍵暗号の場合には、安全性の根拠となっている数学的問題の解決の糸口が発見されているものの、暗号アルゴリズムそのものの安全性が脅かされているわけではないという状態に対応し、共通鍵暗号の場合には、当該攻撃方法を適用するためには暗号アルゴリズムを構成する関数や段数を幾分変更する必要があるとか、膨大な量の平文・暗号文ペアを入手する必要がある

といった条件が存在する状態に相当する。

状態3において提案される攻撃においては、攻撃実行に必要な既知平文・暗号文ペアの数が膨大となるケースが多く、「学術的に解読された」としても鍵の更新の頻度を高める等の運用面での対応も可能であるとみられる。

また、状態4は、中規模研究所レベルの計算機環境*1によっていくつかのアプリケーションにおいて暗号アルゴリズムを攻撃可能となっており、暗号アルゴリズム単体によるセキュリティの効果が喪失している状態といえる。

暗号アルゴリズムはそもそも単体で用いられるものではなく、ソフトウェア、または、ハードウェアとして実現され、システムなどに組み込まれてはじめて使われるものである。

危殆化が問題になるのは、システムで使用しているある暗号アルゴリズムに危殆化が生じたとして、暗号アルゴリズムを交換したり、あるいは、暗号アルゴリズムのパラメータの設定を変更したりすることがはたして可能なのかということである。残念なことに、暗号アルゴリズムの変更を考慮に入れてシステム構築がなされていることが非常に少ないのが現状である。

5.1.1 RSA1024ビットの危殆化

素因数分解問題とは、2つの相異なる素数p,qの積である合成数Nが与えられたときに、Nだけからその素因数p,qを求める問題である。そして、RSA暗号は、1978年にリベスト（Rivest）、シャミア（Shamir）、エイドルマン（Adleman）の3人によって公表された公開鍵暗号の1つで、その安全性は素因数分解問題の困難性に依存している。公開されている公開鍵から秘密鍵が解かれてしまえば、暗号文の復号も、署名の偽造も可能になってしまうため、RSAモジュラスの選択において、素因数分解問題の困難性は非常に重要な位置を占めている。

1990年頃になって、ポラード（Pollard）らの数学者よって一般数体ふるい法（General Number Field Sieve, GNFS）が提案されてからは、徐々に分解される合成数のサイズが大きくなってきている。一般数体ふるい法は、非自明な関係式

$$x^2 \equiv y^2 \pmod{N}$$

を見つけて、最大公約数GCD$(x \pm y, N)$を計算することにより、Nの素因数を見つけ出すアルゴリズムで、多項式選択、関係式収集、フィルタリング、線形代数計算、平方根計算の5つのステップからなり、関係式収集及び線形代数計算の2つのステップが計算量の大半を占める。現在知られている解法アルゴリズムの中では最速であるが、最適化のためのパラメータ設定が複雑なのが1つの特徴となっている。

CRYPTRECでは、2006年度において、暗号技術監視委員会の下に、公開鍵暗号ワーキンググループを設置し、素因数分解問題の困難性の計算量などについて調査・検討を行い、その調査結果を公表した。その結果を図に表わすと図5のようになる。

5.1.2 SHA-1の危殆化

一般にハッシュ関数Hの安全性は大きく分けて、以下の3つがある。

(1) 衝突発見困難性－ハッシュ値が一致する、すなわち、$H(M_1) = H(M_2)$となるようなメッセージM_1とM_2を探索することが困難なこと。

(2) 第2原像計算困難性－ある既知のメッセージMとそれに対するハッシュ値が与えられたときに、ハッシュ値が一致する、すなわち、$H(M) = H(M')$となるような別のメッセージM'を探索することが困難なこと。

(3) 原像計算困難性－ある未知のメッセージMに対するハッシュ値が与えられたときに、ハッシュ値が一致する、すなわち、$H(M) = H(M')$となるようなメッセージM'を探索することが困難なこと。

ところが、MD5の衝突発見手法に関する研究の進展によって、レンストラ（Arjen Lenstra）らの研究チームは、ハッシュ関数MD5に関して、偽造したX.509証明書を商用のCA（Certification Authority）に実際に署名させることにより、中間CA証明書の偽造に成功するまでに至っている（図6）。

ここで重要なことは、上述の(1)～(3)とは異なり、新たに、

(4) Chosen-Prefix衝突発見困難性－既知のメッ

*1 Blaze et al. [1996]における“Corporate Department”の規模である30万ドルの資金によって準備される計算機環境を想定している。

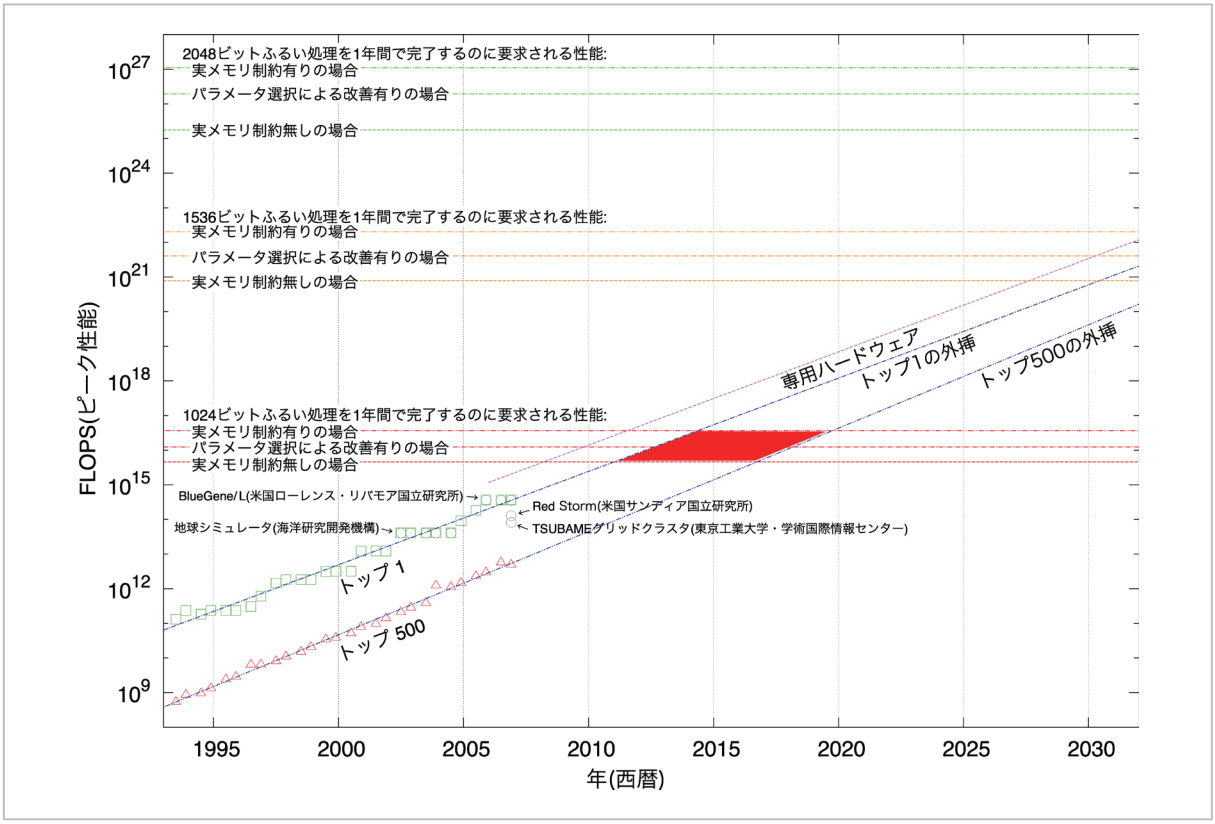

図5　1年間で関係式収集ステップを完了するのに要求されるコンピュータの処理性能予測

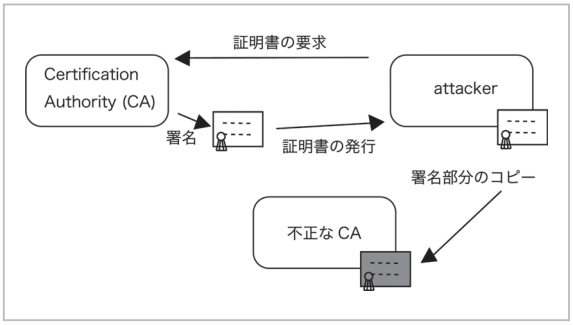

図6　中間 CA 証明書の偽造の様子

セージ P_1 と P_2 が与えられたときに、ハッシュ値が一致する、すなわち、$H(P_1 \| S_1) = H(P_2 \| S_2)$ となるようなメッセージ S_1 と S_2 を計算することが困難なこと。

という探索アルゴリズムが提案されていることである。第2原像計算困難性を有していたとしても、この探索アルゴリズムのため、より現実の状況に沿った上で MD5 を使用した X.509 証明書の偽造が可能になっている。

SHA-1 は米国の NIST によって 1995 年に制定された、ブロック長が 512 ビット、ハッシュ長が 160 ビットのハッシュ関数である。提案されてから 10 年近くの間、深刻な問題点は見つかっていなかったが、MD5 の衝突発見と同じ、ワン（Xiaoyun Wang）らによって 2005 年に衝突探索アルゴリズムが提案されている。ワンらが提案した 2005 年頃の評価では、衝突発見に関する計算量は 2^{63} ～ 2^{69} の範囲である。素因数分解問題の場合と同じ形式で、危殆化の様子を図に表わすと図7のようになる。なお、SHA-1 に関してはまだ Chosen-Prefix 衝突発見困難性の脆弱性が見つかっていない。

5.1.3　暗号の移行

暗号技術を利用した情報通信システムのライフサイクルがサイクルたるためには、システム更改時などにおいて暗号の移行が考慮されていなければならない。その際、暗号アルゴリズムの変更をどのように実施していくかの検討を行うため、暗号アルゴリズムの移行指針とそのロードマップについて検討することが非常に重要である。

5.1.2 の通り、CRYPTREC が 2005 年度に公表した、SHA-1 の衝突発見困難性に関する評価結果及び 2006 年度に公表した、RSA1024 ビット

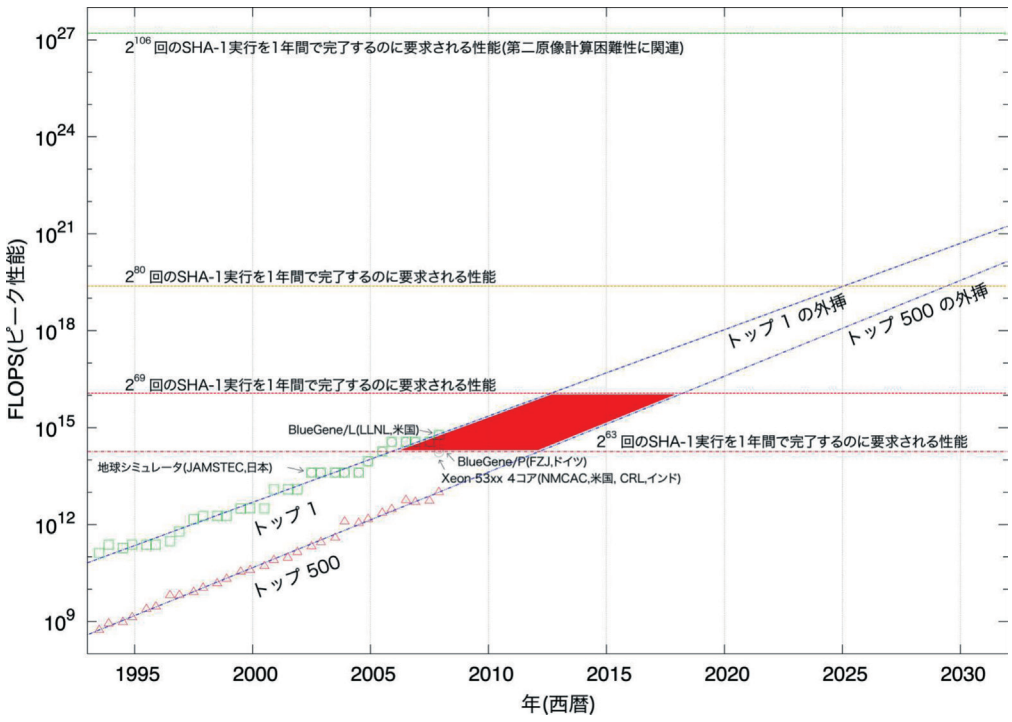

図7 SHA-1 に対する攻撃に関する計算量の予測

が有する素因数分解の困難性に関する評価結果を受けて、2008 年度に、政府機関の情報システムに関する情報セキュリティ対策を立案・遂行する機関である、内閣官房情報セキュリティセンター(National Information Security Center, NISC)は、政府機関の情報システムにおいて使用されている SHA-1 及び RSA1024 ビットに係る移行指針を策定した(図 8)。そこでは、政府認証基盤(Government Public Key Infrastructure, GPKI)などの、各府省庁の電子政府システムおいて、システム更改などのライフサイクルに合わせて、今後 SHA-256 及び RSA2048 ビットが選択可能なようにシステム設計をする旨、政府統一的な対応策が講じられている。

暗号の移行に要する期間は、システム更改時期に合わせるといっても、すぐに予算の手当てがな

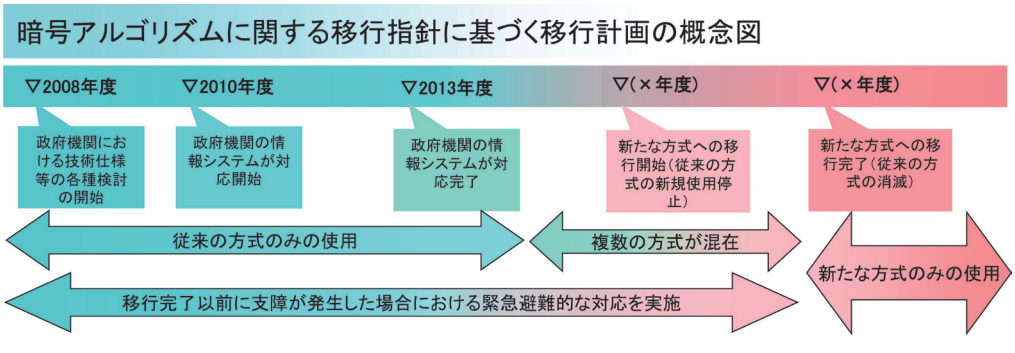

図8 暗号アルゴリズムの移行指針に基づく移行計画の概念図

引用:NISC「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係わる移行指針」の決定について

されて数年で済むようなものはほとんどなく、5～10年といった長いスパンで考えなければならない。従って、暗号技術に求められる安全性というのは最低でも15～20年は必要であろう。

5.2 JCMVPからの要望への対応

情報処理推進機構の暗号モジュール試験及び認証制度（JCMVP）の事務局から、電子政府推奨暗号リストに記載の暗号技術とJCMVPにおいて承認されたセキュリティ機能との間において、いくつかの仕様上の差異があるので、JCMVPが承認した仕様もCRYPTRECで認めるよう要望書が届いた。その要望を認めるためには、仕様書の参照先の変更（追加を含む）または仕様書の変更の妥当性を検証する必要があった。2007年度は、暗号技術検討会の了承を得た後、暗号技術監視委員会の下に設置されていた公開鍵暗号ワーキンググループにて、次の各項目の安全性について調査・検討を行った。

- DH及びECDHに係る鍵導出関数（Key Derivation Function、KDF関数）
- ECDSA及びECDHに係る楕円曲線ドメインパラメータの生成・検証
- ISO化に伴い生じた仕様変更に係るPSEC-KEM

CRYPTRECでは、基本的に電子政府向けに情報発信することを念頭において活動してきたため、JCMVPに限らず、府省庁以外の組織、特に、民間向けに情報発信する際にどの点が重要になるかについての情報が不足しているので、この点については今後の課題である。

5.3 電子政府推奨暗号リストの改訂

客観的な評価により安全性及び実装性に優れると判断される暗号技術をリストアップすることを目的に、2000年度に暗号技術の公募・評価活動を開始し、2002年度末に電子政府推奨暗号リスト（現リスト）を発表し、その後、2003年度から監視活動及び安全性評価を継続して行ってきた。暗号技術に対する解析・攻撃技術の高度化や、新たな暗号技術の開発が進展している状況にあることに加えて、現リストには、策定時点において今後10年間は安心して利用できるという観点で選定された暗号が掲載されているので、2012年度、現リストを改訂することが必要となっている（図9）。

5.3.1 電子政府推奨暗号リスト改訂のための骨子案

電子政府推奨暗号の改訂のため、2008年度に「電子政府推奨暗号リスト改訂のための骨子案」としてパブリックコメントを行い、一般からの意見を募った。

骨子案では、暗号の開発から危殆化までを模した、暗号のライフサイクルの観点から、現リストの構成を見直して、下記の(1)～(3)の各リスト及び(4)リストガイドをまとめて「CRYPTREC暗号リスト（仮称）」（次期リスト）として公開することとした。

(1) 電子政府推奨暗号リスト
(2) 推奨候補暗号リスト
(3) 運用監視暗号リスト
(4) リストガイド

CRYPTRECにより安全性が確認された暗号技術は、(1)～(3)の3つのリストのいずれかに登録される。各リストへの登録は、WTO政府調達協定との整合性に配慮しつつ、安全性や市場動向により決定される。登録の見直しは一定の間隔で行う。現リストに掲載されている暗号技術については、安全性の再評価を行った上で2013年の次期リスト運用開始前に推奨候補暗号リストへ登録されていたものとして扱う。2013年の次期リスト運用開始時には、新たに応募された技術と共に製品化の状況・技術の利用状況により電子政府推奨暗号リストへ登録するかの決定を行う。

次期リストにおける各（部分）リストの役割は以下の通りである。

(1) 電子政府推奨暗号リスト

CRYPTRECにより安全性が確認され、かつ市場において利用実績が十分である技術リスト。電子政府構築（政府調達）の際には当該技術を推奨する（現リストと同等の位置づけ）。ここに登録される技術は国際標準化機関等により、標準化されていることが望ましい。

(2) 推奨候補暗号リスト

CRYPTRECにより安全性が確認されているが、市場において利用実績が十分でない普及段階にある暗号技術が登録されているリスト。今後、利用が期待される新規技術等はここに分類される。電子政府構築（政府調達）の際には当該

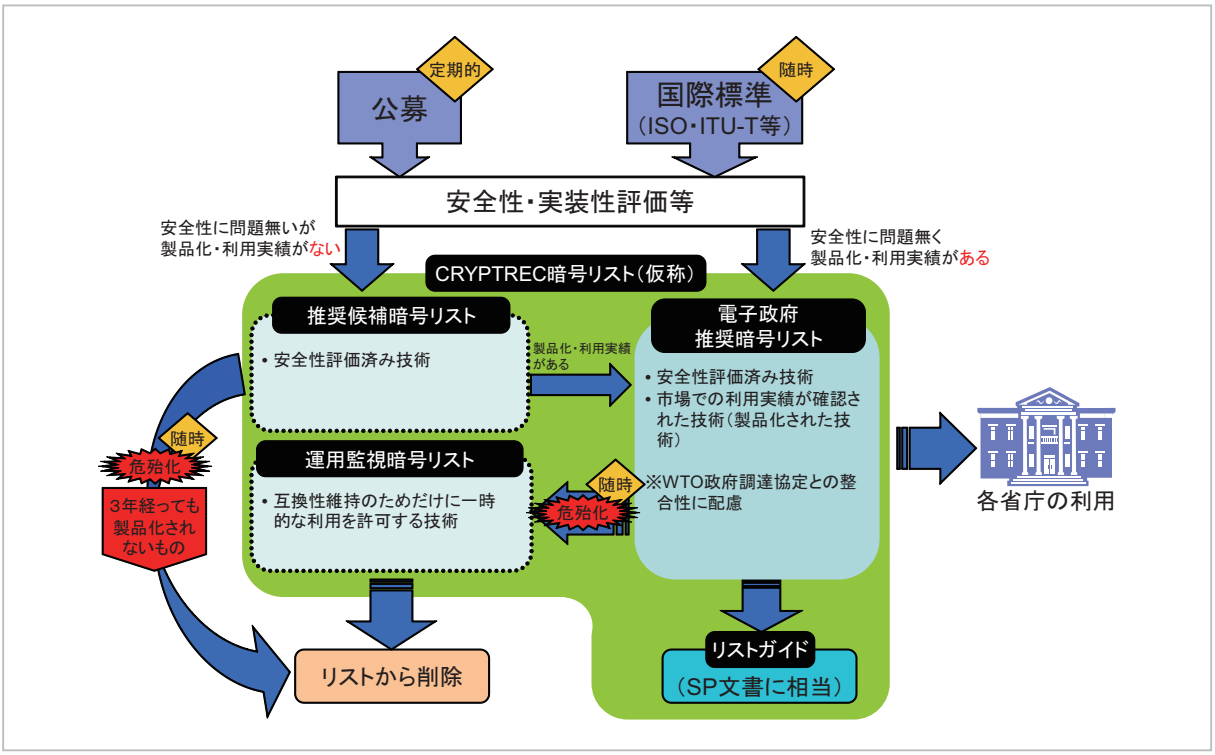

図9 リスト改訂概念図

引用：2008年パブリックコメント「電子政府推奨暗号リストの改訂に関する骨子(案)」

技術を調達しても良い。一定期間ごとに普及の度合いの調査を行い、利用実績が十分であると認められれば電子政府推奨暗号リストに登録される。また、利用実績が十分であると認められなかった場合にはここから削除される。そして、実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術は随時削除される。

(3) 運用監視暗号リスト

電子政府推奨暗号リストに登録されていたが、実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなったもののうち、互換性維持のために継続利用を容認するもののリスト。暗号解読のリスクと、電子政府システムにおける移行コスト等を勘案して、定期的に掲載継続の可否を判断する。CRYPTRECとして新規調達を推奨しない。

(4) リストガイド

電子政府で利用されている、あるいは利用する可能性のある技術について、その技術概要と、推奨する利用方法を記述する。また、次期リストに記載された技術の中で、安全性を維持するため正しいパラメータの設定が要求される技術における具体的なパラメータ設定方法の記述を行う。さらに、将来必要になると予想されるセキュリティ技術については、その開発状況や利用可能性について記載する。リストガイドは、システム運用者や設計者の利用や、システム利用者への啓発を目的とする。

暗号技術公募の基本方針

公募を行う際の基本方針は以下の通りとした。

(1) 公募対象のカテゴリは、下記の(1a)～(1c)のいずれかの条件を満たすものとする。

(1a) 現リストに含まれていないが、電子政府システムの構築において安全性及び実装性の高い技術仕様の推奨が必要とされている暗号技術カテゴリであること。

(1b) 安全性及び実装性で、現リストに記載されている暗号アルゴリズムよりも優位な点を持ち、国際学会で注目されている新技術が提案されている暗号技術カテゴリであること。

(1c) 普及・標準化が見込まれる暗号技術カテゴリであること。

(2) 応募可能な暗号技術は、下記の(2a)～(2e)

のすべての条件を満たすものとする。

(2a) 十分な安全性を有する暗号技術であること。ただし、現リストに掲載されている暗号技術と同カテゴリに属する暗号技術については、それらの暗号技術よりも、安全性もしくは実装性において優れた暗号技術であること。

(2b) 個別のシステムやアプリケーションの仕様に依存しない、汎用的な暗号技術であること。

(2c) 当該技術を利用した製品が販売済みであるか又は、販売の予定があること。

(2d) 安全性評価及び、実装性能評価に足る技術仕様が公表されていること。

(2e) 暗号技術に関する基本特許については、製造、販売、使用に対して、無償 (Royalty Free) 又は、妥当かつ非差別的 (Reasonable And Non-Discriminatory) な条件で、暗号技術の実施許諾権が与えられること。

5.3.2 電子政府推奨暗号リスト改訂のための暗号技術公募 (2009 年度)

公募の概要

安全性及び実装性で、現リストに記載されている暗号アルゴリズムよりも優位な点を持ち、国際学会で注目されている新技術が提案されている暗号技術カテゴリであること、及び、現リストに掲載されている暗号技術と同カテゴリに属する暗号技術については、それらの暗号技術よりも、安全性もしくは実装性において優れた暗号技術であることを指針とした。暗号技術評価の実施にあたっては、暗号技術評価に実績のある国内及び国外の専門家に委託した評価や学会及び論文誌等で発表された評価を踏まえ、各暗号技術の安全性及び実装性等の特徴を整理する予定である。

公募の対象

2009 年度公募対象の暗号技術の種別は、以下のとおり (表 2) である。ただし、主な留意事項としては、

- 応募される暗号技術は、2010 年 9 月末までに、査読付きの国際会議、又は、査読付きの国際論文誌で発表されているか、あるいは、採録が決定されているもの。
- 評価する際に知的財産の利用が無償で行えるもの。
- 公募する暗号技術、又はそれを実装した製品が、電子政府等の利用に際し、次期リスト策定後 3 年以内までに調達可能なもの。

等を挙げていた。

公募期間

2009 年 10 月 1 日～ 2010 年 2 月 4 日 17 時

応募暗号技術

2009 年度において、表 3 のとおり 6 件の暗号技術について応募があった。

表 2 2009 年度公募対象の暗号技術の種別

暗号技術の種別	仕様の概要
ブロック暗号	平文及び暗号文ブロックサイズが 128 ビットであり、鍵長が 128 ビット、192 ビット又は 256 ビットであるブロック暗号で、現リストに掲載されている暗号技術と同等以上の特長 (安全性又は実装性) を持つもの。
暗号利用モード	秘匿に関する 128 ビットブロック暗号及び 64 ビットブロック暗号を対象にした利用モード。
メッセージ認証コード	鍵長が 128 ビットである 128 ビットブロック暗号及び 64 ビットブロック暗号を利用したメッセージ認証コード。
ストリーム暗号	鍵長が 128 ビット以上であり、平文をビット単位もしくはバイト単位で暗号化するストリーム暗号。
エンティティ認証	電子政府推奨暗号リストに掲載された共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードの組み合わせによって実現されるエンティティ認証、あるいは、安全性を計算量的な困難さに帰着できるエンティティ認証を公募します。エンティティ認証を構成する要素技術は、現リストに掲載されている暗号技術を用いることを原則とします。要素技術として、現リストに掲載されていない共通鍵暗号、メッセージ認証コードを用いる場合は、これらの要素技術を同時に応募する必要があります。また、上記以外の要素技術を用いたエンティティ認証技術の応募も可能。

表3 2009年度応募暗号技術一覧

暗号種別	暗号技術名	応募者
128ビットブロック暗号	CLEFIA	ソニー株式会社
	HyRAL	株式会社ローレルインテリジェントシステムズ
ストリーム暗号	Enocoro-128v2	株式会社日立製作所
	KCipher-2	KDDI株式会社
メッセージ認証コード	PC-MAC-AES	日本電気株式会社
エンティティ認証	無限ワンタイムパスワード認証方式（Infinite One-Time Password）	日本ユニシス株式会社

※暗号利用モードについては応募なし。

事務局選出暗号技術

CRYPTRECにおけるリストガイド策定時の検討結果などを参考に、国際標準化等の実績がある以下の暗号技術について、CRYPTREC事務局より選出した。

表4 2009年度事務局選出暗号技術一覧

暗号種別	暗号技術名	評価仕様
メッセージ認証コード（リストガイド策定時の検討等により選定）	CBC-MAC	ISO/IEC 9797-1
	CMAC	NIST SP 800-38B
	HMAC	NIST FIPS 198-1
暗号利用モード（リストガイド策定時の検討等により選定）	CBCモード	NIST SP 800-38A
	CFBモード	NIST SP 800-38A
	OFBモード	NIST SP 800-38A
	CTRモード	NIST SP 800-38A
	GCMモード	NIST SP 800-38C
	CCMモード	NIST SP 800-38C
エンティティ認証（標準策定状況により選定）	共通鍵暗号利用による認証プロトコル	ISO/IEC 9798-2、対称暗号化アルゴリズムを使用する機構
	電子署名利用による認証プロトコル	ISO/IEC 9798-3、デジタル署名技術を使用する機構
	検査関数(MAC)による認証プロトコル	ISO/IEC 9798-4、暗号検査機能を使用する機構

※128ビットブロック暗号及びストリーム暗号については選出なし。

応募暗号の評価スケジュール

2012年度の電子政府推奨暗号リストの改訂に向けた応募暗号の評価スケジュールをまとめると図10の通りとなる。2010年度にかけては、主に応募された暗号技術の評価を実施した。また、2011年度には、応募された暗号技術の評価を継続するほか、現リストに登録されている暗号技術の再評価も行う。暗号方式委員会及び暗号実装委員会が、評価結果に基づき、「CRYPTREC暗号リスト（仮称）」（次期リスト）への記載の可否について判定し、暗号技術検討会に答申する。答申された内容については、暗号技術検討会での検討を経た後、最終的に総務省及び経済産業省において決定される。決定については、2012年度実施を予定している。

応募暗号の評価項目

安全性評価項目と実装性評価項目の2つに大別される。

(1) 安全性評価項目

既知の一般的な攻撃法に対する耐性を評価する。また、その暗号に特化した攻撃法や、ヒューリスティックな安全性の根拠も評価の対象とすることがある。

(2) 実装性評価項目

提出資料に基づいて、実現可能性の確認を行う。性能の評価に関して、ソフトウェア実装では、標準的なプラットフォーム上での性能（処理速度、メモリ使用量等）を評価する。また、ハードウェア実装（エンティティ認証を除く）では、使用するプロセス（FPGA*2、ASIC*3等）別に性能（処理速度、使用セル数又はゲート数等）を評価する。また、一部の暗号技術に対しては、サイドチャネル攻撃に対する対策実現の確認も行う。

*2 FPGA：Field Programmable Gate Array
*3 ASIC：Application Specific Integrated Circuit

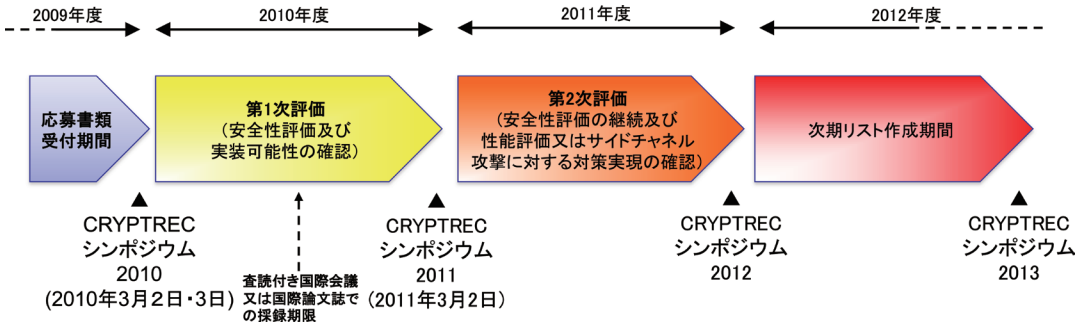

図10 評価スケジュール

引用：電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009年度）

5.3.3 第1次評価の進捗状況（2010年度）

応募暗号技術

表5 応募暗号技術の第1次評価結果

暗号種別	暗号技術名	提案者	評価継続の要否
128ビットブロック暗号	CLEFIA	ソニー株式会社	引き続き第2次評価を行う。
	HyRAL	株式会社ローレルインテリジェントシステムズ	128ビット鍵長から255ビット鍵長においては、現在のところ問題点は見つかっていないが、256ビット鍵長の場合、極小的な数であるが等価鍵の発見及び現実的な計算量での導出法が示された。よって、現リストに掲載されている暗号技術と同等以上の特長を持たないと判断し、第1次評価までで評価終了とし、次期リストには掲載しない。
ストリーム暗号	Enocoro-128v2	株式会社日立製作所	引き続き第2次評価を行う。
	KCipher-2	KDDI株式会社	引き続き第2次評価を行う。
メッセージ認証コード	PC-MAC-AES	日本電気株式会社	引き続き第2次評価を行う。

※暗号利用モードについては応募なし。
※エンティティ認証に応募された無限ワンタイムパスワード認証方式については、2010年9月末までに、査読付きの国際会議又は査読付きの国際論文誌で発表されなかったことにより、応募資格を喪失した。

事務局選出暗号技術

表6 応募暗号技術の第1次評価結果

暗号種別	暗号技術名	評価仕様	評価継続の要否
メッセージ認証コード	CBC-MAC	ISO/IEC 9797-1	今後、注意すべき利用方法や利用方法に関する注釈等について検討した上で、次期リストに掲載する。
	CMAC	NIST SP 800-38B	
	HMAC	NIST FIPS 198-1	
暗号利用モード	CBC モード	NIST SP 800-38A	
	CFB モード	NIST SP 800-38A	
	OFB モード	NIST SP 800-38A	
	CTR モード	NIST SP 800-38A	
	GCM モード	NIST SP 800-38C	
	CCM モード	NIST SP 800-38C	
エンティティ認証	共通鍵暗号利用による認証プロトコル	ISO/IEC 9798-2、対称暗号化アルゴリズムを使用する機構	一部のタイプに脆弱性を発見したので、それらについては利用しないよう注釈を付けた上で、次期リストに掲載する。ただし、脆弱性の発見されたタイプに関しては、修正方法が存在するので、ISO/IECに対して修正を求め、修正が完了し次第、注釈に関して再検討を行う。
	電子署名利用による認証プロトコル	ISO/IEC 9798-3、デジタル署名技術を使用する機構	
	検査関数（MAC）による認証プロトコル	ISO/IEC 9798-4、暗号検査機能を使用する機構	

※128ビットブロック暗号及びストリーム暗号については選出なし。

6 今後の課題

安全性評価については、共通鍵暗号に対する鍵関連攻撃など、鍵拡大関数部分に対する安全性評価や現リストの暗号技術に関する再評価に関する検討が必要になっている。

また、実装性評価については、性能評価に関し、現リスト策定時の経験があるものの、今回は評価対象の数が大幅に増えること、サイドチャネル攻撃に関して、電力解析など今回はじめて実施することが多いことから、実作業において困難が予想される。

7 むすび

情報通信技術に限らず、科学技術を社会に展開（deploy）する際において、安全性について考慮することは重要なことである。情報通信技術に関していえば、その安全性が失われたとしても、直接、人の生命や身体に危険が生じることはないかもしれないが、一度信頼を失ってしまった場合の金銭的な損失は、規模が大きくなればなるほど大きくなるであろう。暗号技術が危殆化した場合、移行にかかるコストと金銭的な損失を天秤にかけて、いつ、どのような方法で移行するのが妥当なのかを最終決定するのは評価機関であるCRYPTRECではなく、情報通信システムを運用・管理している組織や会社に他ならない。

今までCRYPTRECでは主に暗号技術の安全性及び実装性の評価を検討の対象にしてきたが、2010年度から暗号運用委員会を設置して、電子政府システム等で利用される電子政府推奨暗号の適切な運用について、システム設計者・運用者の観点から調査・検討を開始しはじめた。直ちに知見が集積してくるわけではないが、今後、年月をかけて検討していくことで、システム設計者・運用者向けにもより有用な情報提供ができるよう努力していきたい。

謝辞

この場を借りて、今までCRYPTREC活動に参加し、暗号アルゴリズムの安全性評価や実装性評価の検討にご協力していただいたすべての方々に

感謝いたします。

参考文献

1 独立行政法人情報通信研究機構・独立行政法人情報処理推進機構，“CRYPTREC Report 2005,” 独立行政法人情報通信研究機構・独立行政法人情報処理推進機構，2006年3月.
2 独立行政法人情報通信研究機構・独立行政法人情報処理推進機構，“CRYPTREC Report 2006,” 独立行政法人情報通信研究機構・独立行政法人情報処理推進機構，2007年3月.
3 独立行政法人情報通信研究機構・独立行政法人情報処理推進機構，“CRYPTREC Report 2007,” 独立行政法人情報通信研究機構・独立行政法人情報処理推進機構，2008年3月.
4 独立行政法人情報通信研究機構・独立行政法人情報処理推進機構，“CRYPTREC Report 2008,” 独立行政法人情報通信研究機構・独立行政法人情報処理推進機構，2009年3月.
5 独立行政法人情報通信研究機構・独立行政法人情報処理推進機構，“CRYPTREC Report 2009,” 独立行政法人情報通信研究機構・独立行政法人情報処理推進機構，2010年3月.
6 独立行政法人情報通信研究機構・独立行政法人情報処理推進機構，“CRYPTREC Report 2010,” 独立行政法人情報通信研究機構・独立行政法人情報処理推進機構，2011年3月.
7 総務省・法務省・経済産業省，“電子署名及び認証業務に関する法律の施行状況に係る検討会報告書,” 2008年3月，http://www.soumu.go.jp/menu_news/s-news/2008/080530_4.html
8 内閣官房情報セキュリティセンター，“政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針,” 内閣官房情報セキュリティセンター，2008年4月，http://www.nisc.go.jp/active/general/res_niscrypt.html
9 黒川貴司，“暗号アルゴリズムの危殆化,” JPNIC News letter, No. 44, JPNIC, pp. 64–68，2010年3月.
10 宇根正志，黒川貴司，鈴木雅貴，田中秀磨，“暗号ユーザーが暗号アルゴリズムの安全性評価結果をどう活用するか,”『金融研究』第29巻第2号，日本銀行金融研究所，pp. 201–228，2010年4月.
11 Matt Blaze, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, and Michael Wiener,“Minimal Key Length for Symmetric Ciphers to Provide Adequate Commercial Security,”A Report by an Ad Hoc Group of Cryptographers and Computer Scientists, January 1996.
12 Marc Stevens, Arjen Lenstra, and Benne de Weger,“Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities,”Eurocrypt 2007, LNCS 4515, International Association for Cryptology Research, pp. 1–22, 2007.

（平成23年6月15日 採録）

黒川貴司（くろかわたかし）
ネットワークセキュリティ研究所
セキュリティ基盤研究室技術員

金森祥子（かなもりさちこ）
ネットワークセキュリティ研究所
セキュリティ基盤研究室技術員