IMES DISCUSSION PAPER SERIES

ISO/TC68における金融分野向け
推奨暗号アルゴリズムの検討状況

田村裕子（たむらゆうこ）

Discussion Paper No. 2008-J-21

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2008-J-21
2008 年 11 月

ISO/TC68における金融分野向け推奨暗号アルゴリズムの検討状況

田村裕子（たむらゆうこ）*

要　　旨

金融分野では、重要なデータの機密性、一貫性の確保や金融取引時に実行される認証に暗号アルゴリズムが利用されており、2-key トリプル DES、鍵長を 1,024 ビットとする RSA、SHA-1 が主流になっているとみられている。しかし、これらの暗号アルゴリズムは、今後中・長期にわたって十分な安全性を確保することが難しいとの評価が暗号研究者の間で一般的となっており、米国立標準技術研究所（NIST）は 2011 年以降これらの暗号アルゴリズムを米国連邦政府の情報システムにおいて使用しない方針を発表している。

こうしたなか、金融サービスの国際標準化を担当する ISO/TC68 は、既存の暗号アルゴリズムの移行に関する検討を行い、金融分野における推奨対応策をスタンディング・ドキュメントとして取り纏めた。例えば、2-key トリプル DES に関しては、実装環境に応じて使用推奨期間に幅を持たせて規定するなど独自の対応策を示している。

今後、わが国の金融機関が、暗号アルゴリズムの移行、および、新規採用について検討していくうえでは、個々のアプリケーションに応じてリスク分析を行ったうえで、暗号アルゴリズムの取扱いに関する具体的な対応を独自に決定していく必要がある。その際、ISO/TC68 による検討結果等を参考にすることが考えられることから、本稿では、ISO/TC68 によるスタンディング・ドキュメント等を紹介するとともに、今後各金融機関が検討を進めていくにあたっての論点を整理する。

キーワード:暗号アルゴリズムの移行、スタンディング・ドキュメント、
トリプル DES、ISO/TC68、SHA-1、RSA
JEL classification：L86、L96、Z00

* 日本銀行金融研究所（E-mail: yuuko.tamura@boj.or.jp）

本稿を作成するに当たっては、独立行政法人情報処理推進機構 セキュリティセンター 暗号グループの山岸篤弘グループリーダーから有益なコメントをいただいた。ここに記して感謝したい。本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

目　次

1. はじめに

金融分野では、重要なデータの機密性や一貫性を確保するために暗号アルゴリズムが利用されており、こうしたアプリケーションの例としては、キャッシュカード取引における IC カード認証、PIN 認証や銀行のホスト・コンピュータと営業店端末間の伝送データの保護等が挙げられる。

わが国の金融分野における暗号アルゴリズムの利用については、金融機関が情報システムに適切な安全対策を講じる際に依拠する基準となっている金融情報システムセンター（FISC）の安全対策基準（FISC［2006］）において、「重要なデータについては暗号化の対策を講ずることが望ましい」とされている[1]。ただし、各金融機関が具体的にどのような暗号アルゴリズムを利用しているかについては、安全性の観点から公開されていないケースが多い。金融分野における情報セキュリティ技術の国際標準や海外の各種ガイドラインを参照すると、2-keyトリプルDES、公開鍵長を 1,024 ビットとするRSA（以下、1,024 ビットRSA と呼ぶ）、SHA-1 が主流になっているとみられる（宇根・神田［2006］）。

しかし、これらの暗号アルゴリズムは、今後のコンピュータのコスト・パフォーマンス向上や暗号解読技術の進展を前提とすると、今後中・長期にわたって十分な安全性を確保することが難しいとの見方が暗号研究者の中で一般的となっている。特に、米国立標準技術研究所（NIST：National Institute of Standards and Technology）は、基本的にはこれらの暗号アルゴリズムを 2011 年以降米国連邦政府機関の情報システムで使用しない方針を各種ガイドラインで示した（NIST［2005a,b］）。NIST は米国連邦政府用暗号アルゴリズムの評価・認定機関としての役割を担っており、NIST による認定を受けた米国連邦政府標準暗号は金融分野をはじめとする幅広い分野において利用されてきた経緯がある。

こうしたことから、金融分野においては、現行の暗号アルゴリズムを今後どのように移行していくかが重要な問題となっており、本問題への対応のあり方について検討が進められている。金融サービスを対象とする国際標準化機構（ISO）の専門委員会である ISO/TC68 では、暗号アルゴリズムの移行に関する検討が 2005 年以降行われており、2007 年 11 月には ISO/TC68 としての推奨対応策がスタンディング・ドキュメント（SD：standing document）として取り纏められた（ISO［2007］）。本内容は概ね NIST による方針と整合的なものとなってい

[1] 2007 年度の FISC の調査によれば、ホスト・コンピュータと営業店端末間の伝送データの漏洩防止対策として暗号化を実施している金融機関は 55.9%であるほか、今後暗号化を予定している金融機関は 13.8%となっている。さらに、暗号化を実施している金融機関のうち、電子政府推奨暗号リスト等の公的機関による評価・認定を受けたアルゴリズムを採用している金融機関は 79.2%と報告されている（FISC［2008］）。

るが、2-key トリプル DES については、暗号アルゴリズムの移行にかかるコストも考慮した検討の結果、一定の状況下では 2030 年末まで使用可能とされた。現在は、本 SD を技術報告書（TR：technical report）とするための審議が行われており、2009 年 7 月の発行が予定されている。

一方、わが国の政府においても、CRYPTREC（Cryptography Research and Evaluation Committees）による電子政府推奨暗号リストは 2013 年を目途に改訂されることとなっているほか（総務省・経済産業省［2008］）、内閣官房情報セキュリティセンター（NISC：National Information Security Center）は政府機関の情報システムにおける 1,024 ビット RSA と SHA-1 の移行指針案（NISC［2008］）を 2008 年 2 月に発表するなど、暗号アルゴリズム移行に向けた取組みが進められている。

暗号アルゴリズムの移行に関する問題は、現時点で暗号アルゴリズムを利用している金融機関に関係することに加えて、今後新規に暗号アルゴリズムの採用を検討する際にも将来的な暗号アルゴリズム移行に備えたシステム設計や手続のあり方等、考慮すべき論点を含んでいる。わが国の金融機関においても、ISO/TC68 等の対応を参考にしつつ、個々のアプリケーションに応じてリスク分析を行い、必要な対応のあり方について自ら検討していくことが求められる。

本稿では、今後各金融機関が暗号アルゴリズムの移行等に関する検討を進めていくにあたって参考となる情報を提供することを目的として、ISO/TC68 による推奨対応策の概要、および、わが国の電子政府等の動向について紹介する。また、暗号アルゴリズムと移行に関する論点や今後の検討課題を整理する。

本稿の構成は以下のとおりである。まず、2 節において、暗号アルゴリズムの移行に関する問題と米国連邦政府の情報システムにおける移行方針について説明する。3 節では、ISO/TC68 が金融分野における推奨対応策として取り纏めたスタンディング・ドキュメントの内容を紹介する。4 節では、関連する業界の動きとして、クレジットカード（EMV 仕様）と EV SSL 証明書における暗号アルゴリズムの取扱いについて紹介し、5 節では、わが国の電子政府等における暗号アルゴリズムの取扱いを紹介する。6 節では、各金融機関が今後暗号アルゴリズムの移行を進めるにあたって検討すべき課題を整理し、7 節で本節を締め括る。

2. 米国連邦政府における暗号アルゴリズムの取扱い

（1）背景

暗号アルゴリズムは、コンピュータのコスト・パフォーマンスの向上や暗号解読技術によって、安全性が時間の経過とともに低下するという性質を持つ。暗号アルゴリズムを利用する際は、利便性を考慮しつつ、将来の安全性低下を見積もったうえで、一定の使用期間において十分な安全性を確保できると見込まれる暗号アルゴリズムを選択する必要がある。そして、当該使用期間を越える場合には、より安全性の高い暗号アルゴリズムに移行することが必要となる。

こうした暗号アルゴリズム移行の問題は、現在海外を中心に金融分野において主流とみられる 2-keyトリプルDES、1,024 ビットRSA、SHA-1 についても当てはまる[2]。これらの暗号アルゴリズムは、今後のコンピュータのコスト・パフォーマンスの向上を前提とすると、十分な安全性を中・長期にわたって確保することが困難となってきているとの見方が暗号研究者等の間で一般的となっている。これらの暗号アルゴリズムを米国連邦政府標準暗号として認定しているNISTは、暗号アルゴリズムの認定を見直し、基本的に 2011 年以降は米国連邦政府の情報システムにおいて使用しない方針を 2005 年以降各種のガイドラインにおいて示してきた（NIST［2005a, b］）。

（2）NIST によるガイドライン

米国では、連邦政府内で使用される情報セキュリティ技術の評価・認定に関する権限がNISTに付与されている。NISTは、FIPS[3]やSP[4]において米国連邦政府内で使用する暗号アルゴリズムを認定するとともに、暗号アルゴリズムや鍵長

---

[2] わが国の金融分野においては、「日本のユーザは、CRYPTREC の定める電子政府推奨暗号リストにおいて、鍵長の下限が 128 ビットと定められたことから、2-key トリプル DES がリストから除外され、主要なシステムでトリプル DES を使う場合、2-key ではなく 3-key を選択する強い誘因が働いた」との見方もある（岩下［2007］）。

[3] FIPS（Federal Information Processing Standard）は、「機密ではない（unclassified）が取扱いに注意を要する（sensitive）情報」（例えば、プライバシーに関連する情報）を取り扱う米国連邦政府内（国防関係を除く）のシステムにおいて採用される情報技術を規定するものである。FIPS に準拠しないセキュリティ製品群は連邦政府システムの仕様要件を満たしていないことになり、調達そのものが事実上不可能になる。このため、FIPS に認定された暗号技術は強制力のある米国連邦政府標準暗号と呼ばれる。

[4] SP（Special Publication）は、一般的な推奨技術情報、あるいは、FIPS の付随情報として必要に応じて公開されるものである。基本的には、FIPS ほどの強制力はなく、採用するかどうかはそれぞれの状況に応じて個別に判断されるものとなっている。ただし、FIPS の付随情報である場合には、当該 FIPS では決まっていない仕様部分やガイドライン等が追加明示されていることが多く、事実上の強制規定として取り扱われることがある。

を今後どのように移行するかの見通しをガイドラインとして示している。FIPSで認定されている主な米国連邦政府標準暗号としては、共通鍵暗号AES（FIPS 197)、デジタル署名方式（FIPS 186-2）[5]、ハッシュ関数（FIPS 180-3）[6]がある。トリプルDESについては、2005 年にトリプルDESを認定していたFIPS 46-3 が廃止され、SP 800-67 に記述される扱いとなっている。さらに、暗号アルゴリズムの鍵管理に関するガイドラインとしてSP 800-57（NIST［2007b］）とSP 800-78-1（NIST［2007c］）が公開されており、これらの中で暗号アルゴリズムとその鍵長に関する使用推奨期間が述べられている。NIST［2007a, b］は 2005 年に発表されたガイドラインの改訂版である。

イ．情報システム一般における鍵管理に関するガイドライン

（イ）暗号アルゴリズムの等価安全性

SP 800-57 では、暗号アルゴリズムの実装に必要となる各種暗号鍵の種類やその利用方法、「暗号アルゴリズムの等価安全性」に基づく暗号アルゴリズムの使用推奨期間等が詳細に記述されている。

暗号アルゴリズムの等価安全性とは、異なる種類の暗号アルゴリズムの安全性を比較するための評価方法であり、攻撃に必要な計算量が同程度である暗号アルゴリズムは安全性が等価であると評価するものである。攻撃に必要な計算量が 2^nである暗号アルゴリズムの安全性は「nビット安全性（n-bits of security)」と呼ばれる。こうした評価は、共通鍵暗号については秘密鍵探索の計算量、公開鍵暗号については暗号アルゴリズムの安全性が依拠する問題（素因数分解問題等）を解く計算量、ハッシュ関数についてはハッシュ関数を利用した用途（デジタル署名等）への攻撃に必要な計算量[7]をベースとしている。

（ロ）暗号アルゴリズムの使用推奨期間

等価安全性に基づく使用推奨期間については、2010 年末まで使用する暗号アルゴリズムについては少なくとも 80 ビット安全性が必要であり、2030 年末までであれば少なくとも 112 ビット安全性が、2031 年以降であれば少なくとも 128 ビット安全性が必要とされている。

---

[5] FIPS 186-2 では、RSA、DSA、ECDSA が認定されている。また、2006 年には FIPS 186-2 の改訂版となる FIPS 186-3 のドラフトが発表されている。本ドラフトでは、FIPS 186-2 で認定されている鍵長に加えて、より安全性の高い鍵長がパラメータとして追加されたほか、デジタル署名に利用するハッシュ関数と鍵長の関係についても明記された。

[6] FIPS 180-3 では、SHA-1、SHA-224、SHA-256、SHA-384、SHA-512 が認定されている。

[7] ハッシュ関数の用途に関するガイドライン SP 800-107（ドラフト）では、ハッシュ関数の n ビット安全性を、ハッシュ関数に求められる原像計算困難性、第 2 原像計算困難性、衝突計算困難性の 3 つの性質（本節（2）イ．（ロ）参照）についてそれぞれ定義している。

共通鍵暗号についてはトリプルDESとAESについて、それぞれ鍵長ごとに使用推奨期間が示されている（**表 1**参照）。2-keyトリプルDESについては、Oorshot and Wiener［1990］の評価をベースに、2^{40} 個の平文・暗号文ペアを攻撃者が入手するケースを想定して 80 ビット安全性を有すると評価されており、2011 年以降使用しない方針となっている。

公開鍵暗号については、以下の安全性が依拠する問題（素因数分解問題、離散対数問題、楕円離散対数問題）ごとに記述されており、特に、1,024 ビットRSAについては 2011 年以降使用しない方針となっている（**表 1**参照）。

- 素因数分解問題（factoring problem）：N から N=p･q となる素数 p、q を求める問題。
- 離散対数問題（discrete logarithm problem）：有限群 G について、g, y∈G から $y=g^x$ となる x を求める問題。
- 楕円離散対数問題（elliptic curve discrete logarithm problem）：有限体上の楕円曲線 E について、E 上のある特定の 2 点 G、Y から Y=xG となる x を求める問題。

nビット安全性	暗号アルゴリズム				使用推奨期間
	共通鍵暗号	公開鍵暗号とその鍵長			
		素因数分解問題ベース［RSA 等］（N=p･q）	離散対数問題ベース［DSA 等］（$y=g^x$）	楕円曲線離散対数問題ベース［ECDSA 等］（Y=xG）	
		N のビット長	（y のビット長、x のビット長）	Y のビット長	
80 ビット安全性	2-key トリプル DES	1,024	（1,024、160）	160～223	～2010 年末
112 ビット安全性	3-key トリプル DES	2,048	（2,048、224）	224～255	～2030 年末
128 ビット安全性	AES-128	3,072	（3,072、256）	256～383	2030 年超
192 ビット安全性	AES-192	7,680	（7,680、384）	384～511	
256 ビット安全性	AES-256	15,360	（15,360、512）	512～	

（備考）SP 800-57 におけるテーブル 2、4 を参照して作成。

表 1：SP 800-57 に記述されている暗号アルゴリズムの使用推奨期間

また、FIPS 180-3 で規定されている 5 つのハッシュ関数については、ハッシュ関数の用途に分けてそのnビット安全性と使用推奨期間が記述されている（**表 2**

参照)。ハッシュ関数Hに求められる性質は以下の原像計算困難性、第 2 原像計算困難性、衝突計算困難性である。

- 原像計算困難性：与えられたハッシュ値 y に対して、y=H(x)を満たす入力値（原像）x を求めることが困難であること。
- 第 2 原像計算困難性：与えられた入力値 x に対して、H(x)=H(x')を満たす別の入力値（第 2 原像）x' (≠x)を求めることが困難であること。
- 衝突計算困難性：H(x)=H(x')となる入力値の組（x, x'）を求めることが困難であること。こうした（x, x'）は衝突ペアと呼ばれる。

暗号学的に安全なハッシュ関数とは、ハッシュ値のサイズをhビットとしたとき、原像を求めるのに必要な計算量が 2^h、第 2 原像を求めるのに必要な計算量が 2^h、衝突ペアを求めるのに必要な計算量が $2^{h/2}$ となるハッシュ関数をいう[8]。

NISTは、デジタル署名に利用するケースでは、ハッシュ関数の衝突計算困難性がデジタル署名の安全性に影響を与えるとしたうえで、2011 年以降のSHA-1の使用を推奨しない扱いとしている。また、HMAC[9]、鍵生成関数、擬似乱数生成といった用途であれば、第 2 原像計算困難性や原像計算困難性が安全性に影響を与えることから、いずれのハッシュ関数も 2031 年以降でも使用可能との方針が示されている。さらに、SHA-1 については、新しい情報システムを構築する際に、デジタル署名の生成に用いられるハッシュ関数として採用することを推奨しない旨が記載されている。

n ビット安全性	ハッシュ関数とその用途		使用推奨期間
	デジタル署名	HMAC、鍵生成関数、擬似乱数生成	
80 ビット安全性	SHA-1	-----	～2010 年末
112 ビット安全性	SHA-224	-----	～2030 年末
128 ビット安全性	SHA-256	SHA-1	2030 年超
192 ビット安全性	SHA-384	SHA-224	
256 ビット安全性	SHA-512	SHA-256、SHA-384、SHA-512	

（備考）SP 800-57 におけるテーブル 3 を参照して作成。

表 2：SP 800-57 に記述されているハッシュ関数の使用推奨期間

[8] SP 800-107 のドラフトでは、FIPS 180-3 で認定されている 5 つのハッシュ関数の n ビット安全性を示している。このうち、SHA-1、SHA-224、SHA-256、SHA-512 については、ハッシュ関数の入力となるメッセージのビット長によって第 2 原像の計算に必要な計算量が異なることが示されている。

[9] HMAC（keyed-hash message authentication code）は、ハッシュ関数を使用して MAC を生成する方式である。

ロ．本人確認システムにおける鍵管理に関するガイドライン

SP 800-78-1 は、米国連邦政府の職員や関係者が連邦政府機関の施設や情報システム等にアクセスする際に、連邦政府機関によって発行された証明書や関連情報を用いて実施する本人確認方式（PIV：Personal Identity Verification）[10]で使用される暗号アルゴリズムおよびその使用推奨期間を記述するものである。

（イ）カードに搭載されるアプリケーションで利用する暗号アルゴリズム

SP 800-78-1 には、PIVカードに搭載される、①個人識別、②PIVカード認証、③デジタル署名、④鍵配送の 4 つのアプリケーションで利用される暗号アルゴリズムとその使用推奨期間が示されている（**表 3**参照）。SP 800-57 が示す使用推奨期間は、データの復号や検証に暗号アルゴリズムを利用する期間を含むものであるのに対し、本ガイドラインで示されている使用推奨期間は、PIVカードがデータの生成に暗号アルゴリズムを使用する期間であることに注意が必要である。なお、個人識別の機能を搭載する（個人識別用の鍵をカードに格納する）ことは必須であるが、その他はオプションの扱いとなっている。

アプリケーション	暗号アルゴリズムとその鍵長	使用推奨期間
個人識別	RSA（1,024 ビット）	～2013 年末
	RSA（2,048 ビット）、ECDSA（256 ビット）	2013 年超
PIV カード認証	2-key トリプル DES	～2010 年末
	RSA（1,024 ビット）	～2013 年末
	3-key トリプル DES、AES（128、192、256 ビット） RSA（2,048 ビット）、ECDSA（256 ビット）	2013 年超
デジタル署名	RSA（1,024 ビット）	～2008 年末
	RSA（2,048 ビット）、ECDSA（256、384 ビット）	2008 年超
鍵配送	RSA（1,024 ビット）	～2008 年末
	RSA（2,048 ビット）、 ECDH または ECC MQV（256、384 ビット）	2008 年超

（備考）SP 800-78-1（NIST［2007c］）におけるテーブル 3.1 を参照して作成。楕円曲線暗号については、FIPS 186-2 で規定される楕円曲線（P-256、P-384）を利用するものとして記述されている。

表 3：SP 800-78-1 に記述されている暗号アルゴリズムの使用推奨期間

このうち、共通鍵暗号を利用するアプリケーションはPIVカード認証のみであり、利用可能な暗号アルゴリズムとして、2-keyトリプルDES、3-keyトリプルDES、

[10] PIV システムの概要は FIPS 201 において記述されており、連邦政府の職員等に IC カード（PIV カード）を配付し、その PIV カードや PIN 等によって本人確認を行うシステムの構成が記述されている。

AESを挙げるとともに、2-keyトリプルDESについてはその使用推奨期間を 2010 年末までとしている。また、個人識別とPIVカード認証で利用する公開鍵暗号についてはRSAとECDSAが挙げられており、これらのうち 1,024 ビットRSAの使用推奨期間は 2013 年末までとされている[11]。また、デジタル署名と鍵配送については、いずれも 1,024 ビットRSAの利用は 2008 年末までしか推奨されていない。

1,024 ビット RSA の使用推奨期間がアプリケーションによって異なる理由については、個人認証や PIV カード認証では RSA で生成したデータを一時的に利用するのに対し、デジタル署名と鍵配送では生成したデータを比較的長期間保管するケースが多いためと説明されている。

推奨する RSA の指数公開鍵 e の大きさについても記述されており、公開鍵長が 1,024 ビットであるときは、$2^{16}+1 \le e \le 2^{864}-1$、また、2,048 ビットであるときは $2^{16}+1 \le e \le 2^{1824}-1$ とされている。

（ロ）デジタル署名に利用されるハッシュ関数やパディング方法

さらに、PIVカード内に格納される公開鍵証明書やバイオメトリクス認証に利用する情報（指紋等）にはデジタル署名が付与されることとなっており、その際に利用するデジタル署名については、**表 3**で示したものとは別に、利用する公開鍵暗号、ハッシュ関数、パディング方法の組合せ、および、使用推奨期間が記述されている。

利用する公開鍵暗号としては、鍵長を 2,048、3,072、4,096 ビットのいずれかとする RSA、鍵長を 256、384 のいずれかとする ECDSA が挙げられている。ハッシュ関数としては SHA-1、SHA-256、SHA-384 が挙げられており、RSA で利用するパディング方法としては PKCS#1 v1.5 と PSS が挙げられている。

RSA を利用するケースでは、2009 年末までは互換性を最大限確保するために PKCS#1 v1.5 で SHA-1 を利用すべきであるとしている。そのうえで、2010 年中は SHA-1 から SHA-256 への移行期間として両方を併用することが推奨されているほか、SHA-256 を利用する場合のパディング方法は PKCS#1 v1.5 と PSS のいずれかが使用可能とされている。さらに、2011 年以降はハッシュ関数として SHA-256 のみの使用が推奨されている。また、ECDSA の利用については、特に使用推奨期間は記述されていないが、鍵長 256 ビットの ECDSA については SHA-256、384 ビットの ECDSA については SHA-384 の利用が推奨されている。

[11] SP 800-78（NIST［2005b］）では、個人識別用と PIV カード認証用として 1,024 ビット RSA を利用する場合には、その使用推奨期間は 2010 年末までと設定されていたのに対し、SP 800-78-1 では使用推奨期間が 2013 年末まで延長される扱いとなった。

ハ．SHA-3 ファミリーのコンペティション

NIST は、SHA-1 の安全性評価を下方修正する研究成果（Wang, Yao, and Yao［2005］）を受けて、2005 年と 2006 年に現行のハッシュ関数の安全性を評価することを目的としたワークショップを開催した。本ワークショップでの議論の結果、NIST は SHA-1 から SHA-2 ファミリー（SHA-224、SHA-256、SHA-384、SHA-512）への移行を推奨したうえで、SHA-2 ファミリーの次のハッシュ関数である SHA-3 ファミリーをコンペティションによって開発することを決定した（NIST［2007a］）。現時点で発表されているスケジュールによれば、SHA-3 ファミリーは、公募・選考により 2012 年に米国政府標準暗号として発表される予定となっている。

（3）NSA によるガイドライン

米国連邦政府における国防関係のシステムと情報については、米国家安全保障局（NSA：National Security Agency）が、「機密（classified）」および「機密ではない（unclassified）が取扱いに注意を要する」情報を取扱う際に利用する暗号アルゴリズムをSuite B Cryptography[12]として規定している（NSA［2005］）。

Suite B は、共通鍵暗号、デジタル署名、鍵配送、ハッシュ関数のセットであり、FIPS として規定されている暗号アルゴリズムの中から選択したサブセットとなっている。具体的には、共通鍵暗号は鍵長を 128 ビットあるいは 256 ビットとする AES（FIPS 197）、デジタル署名は鍵長を 256 ビットあるいは 384 ビットを利用する ECDSA（FIPS 186-2）、鍵配送は鍵長を 256 ビットあるいは 384 ビットとする ECDH と ECMQV（Draft SP 800-56）、ハッシュ関数は SHA-256 と SHA-384（FIPS 180-3）が規定されている。

Suite Bの公開鍵暗号（デジタル署名、鍵配送）にRSAやDSAではなく楕円曲線暗号を採用した理由について、NSAは明示していないが[13]、1,024 ビット以上に鍵長を伸ばしつつ使い続けた場合には、署名生成や検証にかかる時間が相対的に長くなってしまうなどのデメリットがあるためではないかとの見方もある。こうした楕円曲線暗号の利用を促進するために、NSAはカナダのサーティコム社[14]から楕円曲線暗号に関する特許 26 件のライセンスを取得したと報告している。

---

[12] Suite A Cryptography は機密（sensitive）情報の保護に利用される暗号アルゴリズムを規定するものであり、公開されていない。

[13] NSA［2005］は、RSA と DSA を “classical public key technology” と呼んでいる。

[14] サーティコム（Certicom）社は、楕円曲線暗号を搭載する製品・システムの研究開発を行っており、楕円曲線暗号に関する 350 件以上の特許と出願中特許を有している（Certicom［2008］）。

3. ISO/TC68 における暗号アルゴリズムの移行に関する検討状況

（1）ISO/TC68 における対応

ISO/TC68 における暗号アルゴリズムの移行に関する検討は、2005 年 6 月に開催されたISO/TC68 総会における日本からの問題提起に端を発している（日本銀行金融研究所［2005a］）。同年 9 月に開催されたISO/TC68/SC2[15]の総会では、日本から提出されたUne and Kanda［2007］の要旨に基づき議論が行われ、その結果、SC2 配下に金融分野で利用される暗号アルゴリズムの安全性について検討するためのスタディ・グループを組成し、暗号アルゴリズムの移行に関する推奨対応策を取り纏めることとなった（日本銀行金融研究所［2005b］）。

スタディ・グループの最終的な検討結果は、2006 年 9 月の ISO/TC68/SC2 の総会において承認されたうえで、本検討結果をもとに TC68 で適用可能な暗号アルゴリズム一覧を提供するスタンディング・ドキュメント（SD）を作成することとなった（日本銀行金融研究所［2006b］）。2007 年 11 月の TC68/SC2 の総会では、SD の内容が承認され、各国に回付されることが決議されている（日本銀行金融研究所［2007］）。さらに、2008 年 5 月には、本 SD を技術報告書（TR：Technical Report）とするための新規業務項目提案に対する投票を行うことが決定され、順調に審議が進めば 2009 年 7 月には TR が発行される予定である。

（2）スタンディング・ドキュメントの概要

ISO/TC68/SC2 で取り纏められた SD は、汎業界向けの情報セキュリティ技術の標準化を担当する ISO/IEC JTC1/SC27 傘下の国際標準において規定されている暗号アルゴリズムの使用推奨期間を記述している。本 SD は、①暗号アルゴリズムの等価安全性、②ブロック暗号、③ストリーム暗号、④ハッシュ関数、⑤メッセージ認証子、⑥公開鍵暗号という構成になっており、以下では本構成に沿ってその概要を紹介する。

イ．暗号アルゴリズムの等価安全性

まず、SD では、NIST によって提唱されている「暗号アルゴリズムの等価安全性」（NIST［2007b］）を引用したうえで、暗号アルゴリズムの安全性に基づきその使用推奨期間を記述している。

NISTは、暗号アルゴリズムを 80 ビット安全性、112 ビット安全性、128 ビット安全性以上の 3 つに分類して使用推奨期間を規定しているが、本SDでは、そ

[15] SC2 は、ISO/TC68 傘下のセキュリティを担当する分科委員会（SC：sub-committee）である。

れらに加えて96ビット安全性をもつ暗号アルゴリズムの使用推奨期間も示している。具体的には、80 ビット安全性の暗号アルゴリズムは 2010 年末まで、96ビット安全性の暗号アルゴリズムは2020年末まで、112 ビット安全性の暗号アルゴリズムは2030年末までとしているほか、128 ビット安全性の暗号アルゴリズムは2030年以降も利用可能としている（**表 4**参照）。

暗号アルゴリズムの n ビット安全性	使用推奨期間
80 ビット安全性	～2010 年末
96 ビット安全性	～2020 年末
112 ビット安全性	～2030 年末
128 ビット安全性	2030 年超

（備考）SD のテーブル 1 を参照して作成。

表 4：暗号アルゴリズムの安全性と使用推奨期間

ロ．ブロック暗号

（イ）ブロック暗号とその使用推奨期間

ブロック暗号については、ISO/IEC 18033-3 において規定されている 6 つの暗号アルゴリズム（トリプルDES、MISTY1、CAST-128、AES、Camellia、SEED）について、それぞれ使用推奨期間が記述されている。トリプルDES以外の暗号アルゴリズムについては、現時点において鍵の全数探索より効率的な攻撃が提案されていないとの評価に基づき、鍵長をnビットとするブロック暗号はnビット安全性を有すると評価したうえで**表 4**に基づいて使用推奨期間を記述している（**表 5**参照）。

2-keyトリプルDESについては、鍵の全数探索に必要な計算量が 2^{112} であることと、同一の鍵のもとで生成された平文と暗号文のペアを 2^t個入手した攻撃者が 2^{120-t}の計算量で鍵を求めることができるという研究成果（Oorschot and Wiener［1990］）から、鍵の推測に必要な計算量は $2^{\min(112,\ 120-t)}$であり[16]、その安全性を「min(112, 120−t) ビット安全性」と評価している。

こうした評価結果に基づいて、本SDでは、鍵を頻繁に更新するといった方法によって攻撃者が入手可能な平文・暗号文のペア数を制限することができる場合には、2-keyトリプルDESの使用可能期間を延ばすことができるとしている。具体的には、攻撃者が入手可能であると想定される平文・暗号文のペア数が 2^8 程度のケースでは2030年末まで、2^{24} 程度のケースでは2020年末まで、2^{40} 程度

[16] “min”は最小値を表す数学記号であり、“min(112, 120−t)”とは、112 と 120−t の小さい方の値を意味する。

のケースでは2010年末までの使用が推奨されている（**表 5**参照）。

また、3-key トリプル DES の安全性については、2^{57-s} のメモリと 2^{112+s} の計算量（$1 \leq s \leq 56$）で鍵の推測が可能であるとの評価結果（Menezes, Oorschot, and Vanstone［1997］）に基づき、その安全性を 112 ビット安全性と評価している。

暗号アルゴリズム	鍵長	n ビット安全性	使用推奨期間	攻撃者が入手可能な平文・暗号文のペアの数
2-key トリプル DES	128 ビット	80 ビット安全性	～2010 年末	2^8 程度
		96 ビット安全性	～2020 年末	2^{24} 程度
		112 ビット安全性	～2030 年末	2^{40} 程度
3-key トリプル DES	192 ビット			条件なし
MISTY 、 CAST-128 、 AES、Camellia、SEED	128 ビット	128 ビット安全性	2030 年超	
AES、Camellia	192 ビット	192 ビット安全性		
AES、Camellia	256 ビット	256 ビット安全性		

（備考）SD のテーブル 1、2、3 を参照して作成。

表 5：ブロック暗号とその安全性評価に基づく使用推奨期間

また、ブロック長を n ビットとするブロック暗号では、暗号文一致攻撃によって $2^{n/2}$ 個の平文・暗号文を入手することで平文に関する部分的な情報が高い確率で入手可能になることから、同じ鍵を $2^{n/2}$ 回以上利用しないことを推奨している。そのうえで、ブロック長が 64 ビットであっても、鍵を頻繁に更新することでこうした攻撃を防ぐことができると述べている。

暗号アルゴリズムの移行については、費用や時間が非常にかかる問題であることから、こうしたコストを削減するための検討を十分行う必要があるとしている。特に、ブロック長を 64 ビットとするトリプル DES からブロック長を 128 ビットとする AES へ移行することを考えた場合、現時点での多くの金融取引用のネットワーク・システムは 128 ビットのデータの処理に対応できていないという問題があることから、移行期間における相互運用性も考慮して検討を行うことが重要であると記述されている。さらに、10～15 年かけて移行するという計画であれば非現実的ではないとしたうえで、10 年間の保管が必要なデータの暗号化に2030年末までを使用推奨期間とする暗号アルゴリズムを利用する場合には、2010 年から 2020 年末までに移行を完了させ、その後 2030 年末までは旧暗号アルゴリズムを利用して生成されたデータの保管期間とすることが推奨されている。

（ロ）スタディ・グループにおける議論

NIST が 2-key トリプル DES を 80 ビット安全性と評価したうえでその使用を 2011 年以降推奨しないという方針を示したのに対し、本 SD ではある一定の条件のもとでは 2-key トリプル DES を 2030 年末まで使用可能としている。

2-key トリプル DES の使用推奨期間については、当初スタディ・グループにおいても意見が分かれた（岩下［2007］）。スタディ・グループでの議論の叩き台として議長から提出された SD のドラフトは、概ね NIST による方針と整合的であったが、2-key トリプル DES については条件付で 2030 年までの利用を推奨すると記述されていた。これに対して、①2-key トリプル DES の安全性評価が、最新の暗号解読技術を適用したものではなく、やや古い 1990 年の論文に基づいて行われていること、②米国、日本、欧州のいずれの公的機関や暗号プロジェクトも、推奨暗号アルゴリズムから 2-key トリプルを明示的に外しており、暗号研究者の見解を尊重すべきであること、③ISO/IEC JTC1/SC27 が策定した ISO/IEC 18033-3 の脚注においても、「NIST は 2009 年までしか 2-key トリプル DES を推奨していない」と記述しており、これと矛盾する点が反対意見として挙げられた。

ただし、2-key トリプル DES の鍵を解読する攻撃に必要な計算量は、同一の鍵のもとで生成された平文・暗号文のペアを攻撃者がどのくらい入手できるかに依存していることから、想定する攻撃者が入手できる平文・暗号文のペア数が制限されるケースでは 2-key トリプル DES を利用し続けることが可能ではないかとのコメントが多く寄せられた。2-key トリプル DES の利用継続が強く主張された背景としては、金融分野においてすでに 2-key トリプル DES を利用した製品・システムが広く普及しており、理論的には可能であるが現実的には難しいと想定される攻撃への対策に追加コストをかけることがビジネス的に難しいと判断されたことが挙げられる。その結果、TC68/SC2 が今後継続的に 2-key トリプル DES の安全性評価研究の動向をフォローしていくとともに、SD には 2-key トリプル DES の使用条件を明確にしたうえで使用推奨期間が記述されることなった。

ハ. ストリーム暗号

ストリーム暗号については、ISO/IEC 18033-4 において専用ストリーム暗号とブロック暗号に基づくストリーム暗号が規定されている。ブロック暗号に基づくストリーム暗号は、ブロック暗号を擬似乱数生成器として利用し、生成された擬似乱数を鍵ストリームとして利用するストリーム暗号であり、本 SD ではブロック暗号に基づくストリーム暗号を推奨するとのみ記述されている。

ニ．ハッシュ関数

ハッシュ関数については、ISO/IEC 10118-2 で規定されているブロック暗号に基づくハッシュ関数と ISO/IEC 10118-3 で規定されている専用ハッシュ関数についてそれぞれ使用推奨期間が記述されている。本 SD では衝突ペアの探索にかかる計算量をベースに n ビット安全性を記述している。

（イ）ブロック暗号に基づくハッシュ関数

ブロック暗号に基づくハッシュ関数の安全性は、利用するブロック暗号の安全性とハッシュ値の長さに依存する。つまり、m ビット安全性をもつブロック暗号に基づくハッシュ関数の安全性は、そのハッシュ値のサイズが h ビットであれば「min (h/2, m) ビット安全性」と表される。

本 SD では、ブロック暗号に基づいたハッシュ関数を利用する必要がないのであれば専用ハッシュ関数の利用を推奨するとしたうえで、ブロック暗号に基づいてハッシュ関数を利用することが必要な場合には AES を利用すべきであるとしている。

また、ハッシュ値のサイズについては、ハッシュ値の伸長を伴う移行は、ハッシュ値のサイズが同じ別のハッシュ関数への移行よりシステムの変更項目が多くなるとしたうえで、今後の移行にも柔軟に対応できるよう、ハッシュ関数の変更のみならず、ハッシュ値のサイズの変更が必要である点に留意してデータ・フォーマットの設計を行うべきであるとしている。

（ロ）専用ハッシュ関数

専用ハッシュ関数については、ISO/IEC 10118-3 において規定されている 8 つの暗号アルゴリズムが記述されており、アプリケーションがハッシュ関数のどの性質に安全性を依拠するかによってその使用推奨期間が記述される形となっている（**表 6**参照）[17,18]。

---

[17] SD では、アプリケーションの安全性が依拠するハッシュ関数の性質として、衝突計算困難性と第 2 原像計算困難性のみが挙げられており、原像計算困難性について示されていない。

[18] 一部のハッシュ関数においては、衝突ペアを利用したアプリケーションへの攻撃方法がいくつか提案されている。例えば、ハッシュ関数 MD5 を利用したパスワード認証方式 APOP では 2^{23} の計算量で 13 文字までのパスワードが解読できたと報告されているほか、理論的には 61 文字までのパスワードが解読可能であると報告されている（Sasaki *et al.*［2008］）。そのほか、ITU-T X.509 で規定される公開鍵証明書については、MD5 を利用した場合、2^{52} の計算量で異なる公開鍵と名前に対する公開鍵証明書の偽造が可能であることが示されている（Stevens, Lenstra, and Weger［2007］）。

ハッシュ関数	ハッシュ値のサイズ	n ビット安全性	使用推奨期間	
			衝突計算困難性が求められるケース	第2原像計算困難性が求められるケース
RIPEMD-128	128 ビット	60 ビット安全性以下のレベル	推奨しない	～2020 年末
RIPEMD-160	160 ビット	80 ビット安全性	～2020 年末	～2030 年末
SHA-1		63 ビット安全性	～2010 年末	
SHA-224	224 ビット	112 ビット安全性	～2030 年末	2030 年超
SHA-256	256 ビット	128 ビット安全性		
SHA-384	384 ビット	192 ビット安全性	2030 年超	
SHA-512	512 ビット	256 ビット安全性		
WHIRLPOOL				

（備考）SD のテーブル 4 を参照して作成。

表 6：ハッシュ関数とその安全性評価に基づく使用推奨期間

2005 年以降、SHA-1 の安全性評価に関する研究成果が多く発表された。この結果として衝突ペアの探索が 2^{63} の計算量で可能であることが示され、現時点で SHA-1 は 63 ビット安全性と評価されている。本 SD では、63 ビット安全性をもつ SHA-1 の使用推奨期間を 2010 年末までとしたうえで、衝突計算困難性が求められるアプリケーションにおいて SHA-1 を利用している場合には、より安全であると評価されている別のハッシュ関数への移行について早急に検討すべきであるとの見解が示されている。仮に、2010 年までに移行が完了しなかった場合においても、別の機構を組み込むことによって危殆化の影響を軽減する措置が求められると述べている。

NIST による SP 800-57 では、デジタル署名とは別に、HMAC、鍵生成関数、擬似乱数生成のアプリケーションに分類して使用推奨期間が示されていたが、SD ではそうした具体的なアプリケーションは明示せず、衝突計算困難性と第 2 原像計算困難性のどちらの性質に安全性を依拠するかによって使用推奨期間を分類している。さらに、SD では想定するアプリケーションの安全性がハッシュ関数のどの性質に依拠するかが明らかでない場合には、衝突計算困難性に依拠するアプリケーションと同じ使用推奨期間とすることとされている。

ホ. メッセージ認証子

メッセージ認証子については、ISO/IEC 9797-1 と ISO/IEC 9797-2 においてそれぞれブロック暗号を利用した MAC アルゴリズムとハッシュ関数を利用した MAC アルゴリズムが標準化されている。

MAC アルゴリズム全般については、ランダムに MAC を偽造して検証者に送

信するという攻撃を想定して、偽造された MAC の検証を許容する回数を設定しておく必要がある。そのため、本 SD では、1 つの鍵を利用した MAC の検証のうち、1 回の検証において偽造された MAC を誤って認証してしまうことを許容する確率を p としたとき、$2^m \geq i/p$ となるように MAC のビット長 m、および、偽造された MAC の検証累積回数 i を設定するよう記述されている。

ブロック暗号を使用した MAC アルゴリズムについては、同じ鍵で生成した MAC を複数集めることによって鍵を効率的に探索する攻撃に関する研究結果（Mitchell［2002］）に基づいて、同一の鍵で生成する MAC の個数を、128 ビットブロック暗号を利用する MAC と 64 ビットブロック暗号を利用する MAC について、それぞれ、2^{48} 個以下、2^{21} 個以下としている。

ハッシュ関数を利用した MAC については、ハッシュ関数の衝突ペアや第 2 原像を利用して鍵を効率的に探索する攻撃手法が提案されていることから、MAC アルゴリズムの使用推奨期間は利用するハッシュ関数の使用推奨期間にあわせることとされている。

へ．公開鍵暗号

公開鍵暗号については、ISO/IEC 9796-2 とISO/IEC 9796-3 においてメッセージ復元型デジタル署名、ISO/IEC 14888-2 とISO/IEC 14888-3 においてメッセージ添付型デジタル署名、ISO/IEC 18033-2 において守秘目的の公開鍵暗号が規定されている。SDでは、これらの標準において規定されている暗号アルゴリズムの使用推奨期間が、安全性を依拠する問題ごとに記述されている（**表 7**参照）。

公開鍵暗号とその鍵長			使用推奨期間
素因数分解問題ベース［RSA 等］（N=p･q）	離散対数問題ベース［DSA 等］（$y=g^x$）	楕円離散対数問題ベース［ECDSA 等］（Y=xG）	
N のビット数	（y のビット数、x のビット数）	Y のビット数	
1,024	（1,024、160）	160～191	～2010 年末
1,536	（1,536、192）	192～223	～2020 年末
2,048	（2,048、224）	224～255	～2030 年末
3,072	（3,072、256）	256	2030 年超

（備考）SD のテーブル 5 を参照して作成。

表 7：公開鍵暗号とその安全性評価に基づく使用推奨期間

RSAについては、暗号化を高速に処理できるよう、一般に指数公開鍵eは小さく設定されるが、e=3 のケースについては既に攻撃法が提案されていることから、2^{16}+1 以上の値を設定することが推奨されている[19]。

また、ISO/IEC 18033-2 で規定されるハイブリッド暗号は、共通鍵暗号で利用する秘密鍵の鍵配送を公開鍵暗号で行う方式であり、共通鍵暗号と公開鍵暗号の特長を活かした方式であるとともに、証明可能安全性を有する点が特徴である。公開鍵暗号を利用して鍵配送を行う機構は KEM（key encapsulation mechanism）と呼ばれ、共通鍵暗号を利用して暗号化・復号処理を行う機構は DEM（data encapsulation mechanism）と呼ばれる。ハイブリッド暗号の使用推奨期間は利用する公開鍵暗号に依存するとされているが、KEM に 2-key トリプル DES を利用する場合には、アプリケーションに応じて使用推奨期間が異なることに留意が必要であると述べられている。

（3）ISO/IEC JTC1/SC27 への検討依頼

本節 (2) で紹介したとおり、本 SD では、ある一定の条件のもとであれば 2-key トリプル DES を 2030 年末まで使用可能と記述されている。一方、ISO/IEC JTC1/SC27 傘下の標準である ISO/IEC 18033-3 では、脚注において「NIST は 2009 年までしか 2-key トリプル DES を推奨していない」と記述されていた。このため、ISO/TC68/SC2 は、同じ ISO 標準の中で矛盾が生じているとの見解から、「脚注を削除する、あるいは、2-key トリプル DES に関するより詳細な文書を付加する」のいずれかの対応について ISO/IEC JTC1/SC27 に検討を依頼した（岩下［2007］）。

これに対し、SC27 は 2007 年 5 月の総会において、脚注を削除するとともに、暗号アルゴリズムの安全性に関する事例をスタンディング・ドキュメントとして記述することを決議した。さらに 2008 年 4 月のSC27/WG2 会合[20]では、2007 年 10 月に作成されたスタンディング・ドキュメントのドラフト（ISO and IEC［2007］）について審議し、修正版をSC27 のサイトで公開することを決議している。

SC27 によるスタンディング・ドキュメントのドラフトには、そもそもブロック長を n ビットとするブロック暗号については、$2^{n/2}$ 個の平文・暗号文ペアを入手した攻撃者に平文解読の手掛かりを与えてしまうことになるため、2-key トリプル DES では同じ鍵を 2^{32} 回以上利用すべきではないとしたうえで、2-key トリ

[19] 適切に鍵を生成しない場合に短時間で素因数分解が可能になるケースとしては、SD で記述された公開鍵のサイズのほか、合成数を構成する素数の大きさや指数秘密鍵の構成に関する研究成果が発表されている。

[20] WG2 は、SC27 傘下の暗号アルゴリズムおよびプロトコルを担当する分科委員会である。

プル DES の安全性が大量の平文・暗号文のペアを入手することの難しさのみで評価されるわけではないが、同じ鍵で大量のデータを暗号化しないようにするといったシステム設計が望ましいと記述されている。

4. 金融分野に関連する業界の動向

（1）EMVCo による対応

EMVCo では、IC カードを用いたカード取引に関する仕様書として EMV 仕様（EMVCo［2008a］）を策定しており、EMV 仕様は金融分野におけるデファクト・スタンダードとして利用されている。EMV 仕様では、IC カードと端末間における取引に利用される暗号アルゴリズムやデータ・フォーマット等が記述されており、オフライン取引におけるカード認証で利用する暗号アルゴリズムとしては RSA が推奨されている。

オフラインでカード認証を行う方式としては SDA（static data authentication）と DDA（dynamic data authentication）の 2 種類が準備されているが、いずれの方式においても、CA の公開鍵証明書、カード発行者の公開鍵証明書、IC カードの公開鍵証明書を利用する形態となっている。

公開鍵のサイズ	使用推奨期間
1,024 ビット	～2012 年末
1,152 ビット	～2015 年末
1,408 ビット	～2018 年末
1,984 ビット	

表 8：EMVCo による CA の RSA の鍵長とその使用期間

EMVCoでは、これらのうちCAの公開鍵のサイズの見直しを毎年実施している。最新の見直しでは、1,024 ビットRSAを金融取引に関するシステムで利用することは推奨しないが、レガシー系のシステムについては 2012 年末まで利用できるとされている[21]。また、1,152 ビットRSAについては、2015 年末まで利用可能とされているほか、1,408 ビットと 1,984 ビットのRSAについては、10 年先の予測は困難であるという見解のもと、少なくとも 2018 年までは安全であることが見込まれるという扱いとなっている（**表 8**参照、EMVCo［2008a］）。

さらに、EMVCo は、1,984 ビット RSA の次の暗号アルゴリズムに関する検討を始めている。これは、1,984 ビット RSA に対する NIST のお墨付きが 2025～2030 年の間に失効する予定であることを受け、インフラの移行に 12～15 年かかることを想定して検討が開始されたものである。

TC68 によるSDでは、1,024 ビットRSAの次の暗号アルゴリズムとして 2,048

[21] 1,024 ビット RSA の使用期間については、2002 年時点では 2008 年末、2006 年時点では 2009 年末、2007 年時点では 2010 年末までとされていた。

ビットRSAが挙げられているが、ICカードにRSAを搭載するケースでは、利便性を確保しつつ鍵長の長いRSAを実装することは難しいといわれている。こうしたことから、EMVCoは、2007 年 6 月に “New Cryptography Draft”（EMVCo［2007d］）を発表し、1,984 ビットRSAの次の暗号アルゴリズムへの移行方針として以下の 3 つを挙げた[22]。

① RSA を利用し続ける。CA と発行者の鍵長を長くするが、IC カードの鍵長は現状の長さを維持する。
② RSA を利用し続ける。CA、発行者、IC カードの鍵長をそれぞれ長くする。
③ RSA を楕円曲線暗号に置き換える。

①の案を記述するドラフト（EMVCo［2007a］）では、CA の鍵長の上限を 3,960 ビット、発行者の鍵長の上限を 3,952 ビット、IC カードの鍵長の上限を 1,984 ビットとしている。また、ハッシュ関数については、1,984 ビット以上の鍵長をもつ RSA を利用する場合のハッシュ関数として、SHA-256、および、SHA-512 が規定されている。

②のドラフト（EMVCo［2007b］）では、CA の鍵長の上限を 4,016 ビット、発行者と IC カードの鍵長の上限を 4,008 ビットとしている。また、ハッシュ関数については、SHA-1、SHA-256、SHA-512 が規定されている。

③のドラフト（EMVCo［2007c］）では、公開鍵長を 256 ビット、512 ビットとする楕円曲線暗号を推奨している。また、ハッシュ関数については、公開鍵長が 256 ビットの楕円曲線暗号を利用する場合には SHA-256、512 ビットの楕円曲線暗号を利用する場合には SHA-512 を利用することが記述されている。

本ドラフトに対するコメントは 2007 年 10 月まで募集され、現在は寄せられたコメントをもとに検討が行われている。

（2）CABF の対応

インターネット・バンキングでは、近年、フィッシング詐欺が多く発生していることから、EV SSL 証明書の利用が勧められている（中山［2007］）。EV SSL 証明書は米国の CA/Browser Forum（CABF）が仕様を策定した SSL 証明書の一種であり、EV SSL 証明書の発行に際して実在証明にかかる審査基準が厳しく設定されている。また、EV SSL 証明書対応のブラウザで EV SSL 証明書が導入されたサイトにアクセスすると、これまでの南京錠マークに加え、アドレス・バーが緑色に変化するとともにバー上にウェブサイトを運営する組織と証明書の発

[22] EMVCo［2008a］では、CA、発行者、IC カードのいずれの鍵長の上限も 1,984 ビット、利用するハッシュ関数は SHA-1 とされている。

行認証局が明示されるため、利用者による確認が容易になっているという特徴がある。

EV SSL証明書の発行に利用する暗号アルゴリズムについては、ガイドライン（CABF［2008］）のAppendix Aにおいて、ルートCA、下位CA、加入者の公開鍵証明書の生成に利用する暗号アルゴリズムが規定されている（**表 9**参照）。

<table>
<tr><th rowspan="2">公開鍵証明書の生成者</th><th colspan="3">暗号アルゴリズムとその鍵長</th><th rowspan="2">使用期間</th></tr>
<tr><th>RSA</th><th>楕円曲線暗号</th><th>ハッシュ関数</th></tr>
<tr><td>ルート CA</td><td>---</td><td rowspan="3">-----</td><td>MD5*</td><td rowspan="3">～2010 年末</td></tr>
<tr><td>下位 CA</td><td rowspan="2">1,024 ビット</td><td rowspan="2">-----</td></tr>
<tr><td>加入者</td></tr>
<tr><td>ルート CA</td><td rowspan="3">2,048 ビット</td><td rowspan="3">256 ビット</td><td rowspan="3">SHA-1**、
SHA-256、
SHA-384、
SHA-512</td><td rowspan="3">2010 年超</td></tr>
<tr><td>下位 CA</td></tr>
<tr><td>加入者</td></tr>
</table>

（備考）* MD5 は原則として推奨されない。
** 2011 年以降の SHA-1 の使用は、大半のブラウザが SHA-256 をサポートするまでとする。

表 9：EV SSL 証明書の作成に利用する暗号アルゴリズムとその使用期間

まず、公開鍵暗号については 1,024 ビットの RSA の使用が下位 CA と加入者証明書については 2010 年末までとされており、このうち、加入者証明書については、1,024 ビット RSA を利用して発行された証明書は 2010 年末で失効させなければならないと明記されている。さらに、ハッシュ関数については 2011 年以降 SHA-256、SHA-384、SHA-512 の使用を推奨する扱いとなっており、SHA-1 は互換性確保を目的とした利用に限定されている。

本ガイドラインの制定前の議論では、証明書の発行に利用する暗号アルゴリズムを 2,048 ビットRSAに統一すべきとの意見も出たが、わが国で発売されている一部の携帯端末は 1,024 ビットRSAにしか対応していないことを理由に、1,024 ビットRSAの使用期間が 2010 年末まで延長された。しかしながら、「日本で発売された一部の携帯はRSA1,024 のみに対応している」のが実情であり、「ルート証明書の入れ替えでは解決せず、新しい機種に買い換えてもらう必要がある」が、「平均的な耐用年数から考えても、ほとんどの携帯端末が買い換えられるまでには長い期間がかかる」とみられている（秋山［2008］）。こうしたことから、日本電子認証協議会[23]は、「2010 年問題対策WG」を設置し、本問題への対応を検討している。

[23] 日本電子認証協議会（JCAF：Japan Certification Authority Forum）は、日本国内の主要な電子認証関連事業者によって設立されたものであり、米国の取組みに呼応してわが国における EV SSL 証明書の普及、インターネット上での企業認証基盤サービスとしての定着を目的とした活動を行っている。

5. わが国の電子政府等における暗号アルゴリズムの取扱い

（1）CRYPTREC による対応

イ．電子政府推奨暗号リスト

CRYPTREC は、わが国の電子政府で利用可能な暗号アルゴリズムのリストである電子政府推奨暗号リストを 2003 年に発表している（総務省・経済産業省［2003］）。電子政府推奨暗号リストは、電子政府における調達のための推奨すべき暗号のリストとして利用されるものであるが、客観的な第三者の安全性評価を受けた暗号アルゴリズムとして、民間の業界においても参照されることが多い。金融分野においても FISC の安全対策基準（FISC［2006］）において、暗号アルゴリズムの例として電子政府推奨暗号リストが紹介されている。

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みると、共通鍵暗号については 3-key トリプル DES が含まれているが、FIPS 46-3 として規定されていること、および、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を考慮して当面の使用を認めるとの注釈が付けられている。

ハッシュ関数には SHA-1 が含まれているが、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とされている

さらに、CRYPTREC では電子政府推奨暗号リストガイドを策定し、複数の暗号アルゴリズムを組み合わせて利用するセキュリティ技術について、推奨する暗号アルゴリズムの鍵長等を記述している。素因数分解問題に基づく公開鍵暗号については鍵長を 2,048 ビット以上とすることを推奨しているほか、ブロック暗号についてはブロック長を 128 ビットとすることを推奨している（情報通信研究機構・情報処理推進機構［2008］）。

ロ．電子政府推奨暗号リストの改訂案

現行の電子政府推奨暗号リストは、2003 年の策定時点において今後 10 年間安心して利用できるという観点で選定されたものである。そのため、CRYPTREC は暗号技術に対する解析や攻撃技術の高度や新しい暗号技術の開発の進展を考量して 2013 年に向けたリストの改訂案を発表した（総務省・経済産業省［2008］）。

本案では、「電子政府推奨暗号リスト（仮称）」、「推奨暗号候補リスト（仮称）」、「互換性維持暗号リスト（仮称）」、「リストガイド」の 4 つを策定したうえで、これらをまとめて「CRYPTREC 暗号リスト（仮称）」として公開されることが予定されている。今回の改訂案では、今後も継続して発生し得る暗号アルゴリズムの移行問題への対応として、より安全性の高い暗号アルゴリズムの移行が求

められる暗号アルゴリズムを「互換性維持暗号リスト（仮称)」として管理することが提案されている。各リスト、および、リストガイドの役割は以下のように分類されている。

- 電子政府推奨暗号リスト（仮称）: 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暗号アルゴリズムを掲載する。電子政府構築の際に推奨する暗号アルゴリズムとして位置付けられる。
- 推奨暗号候補リスト（仮称）: 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な十分でない普及段階にある暗号アルゴリズムを掲載する。電子政府構築の際に利用してもよい暗号アルゴリズムとして位置付けられる。
- 互換性維持暗号リスト（仮称）: 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暗号アルゴリズムを掲載する。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が判断される。CRYPTREC として新規調達を推奨しない暗号アルゴリズムとして位置付けられる。
- 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アルゴリズムの中で、具体的なパラメータ設定方法の記述を行う。

現時点でのスケジュールでは、2012 年度第 3 四半期までに次期リスト（案）を策定し、第 4 四半期に次期リストの発表を行い、2013 年度から運用を開始することが予定されている。

（2）NISC によるガイドライン

NISC は、2008 年 2 月、わが国の政府機関の情報システムで利用する暗号アルゴリズムについて、SHA-1 と 1,024 ビット RSA をより安全な暗号アルゴリズムへ移行するための指針案を発表した（NISC［2008］)。

本指針案では、政府認証基盤と商業登記認証局の情報システムの設計要件として、政府が発行する公開鍵証明書の生成・検証に利用する暗号アルゴリズムを複数の中から選択できる構成としたうえで特定の時期に切替え可能とすることが示されており、暗号アルゴリズムには 2,048 ビット RSA と SHA-1 の組合せ、および、2,048 ビット RSA と SHA-256 の組合せを含むこととされている。

現時点で発表されているスケジュールでは、2008 年度中に必要となる対応について検討を行い、2013 年度までに各情報システムに暗号アルゴリズムの移行

を可能とする設計を組み込むこととなっている。暗号アルゴリズムを実際に切り替える時期については各府省庁が検討する扱いとされている。

また、政府認証基盤に関連する情報システム以外については、1,024 ビット RSA、SHA-1 に対して現実的な脅威となる攻撃方法が示された時点で速やかに別の暗号アルゴリズムに変更するといった対応措置を可能とすることが設計要件として記述されている。こうした対応の例としては、暗号モジュールを交換できるようにコンポーネント化して構成する、複数の暗号アルゴリズムを選択可能とすることが挙げられている。

6. 暗号アルゴリズムの移行に関する対応のあり方

ISO/TC68 による暗号アルゴリズムの移行に関する推奨対応策は、あくまで金融向けのアプリケーション一般について記述したものであり、各金融機関が実際に検討を行うにあたっては、対象となるアプリケーションの事情を考慮して独自に検討することが必要である。本節では、今後わが国の金融機関がそうした検討を行う際の論点や課題について考察を行う。

（1）移行の方法

イ．移行のタイム・スケジュールの検討

（イ）現行の暗号アルゴリズムの移行期限

ISO/TC68 による SD は、金融分野における一般的なアプリケーションを想定したうえで、80 ビット安全性の暗号アルゴリズムについては 2010 年末までに移行することを推奨している。このため、暗号アルゴリズムの移行について個々のアプリケーションを前提に検討を行ううえでは、SD による移行期限をそのまま適用してよいか否かに関して検討が必要である。具体的な手順として、例えば、暗号アルゴリズムが解読された場合、想定するアプリケーションにおいてどのような脅威が顕現化するかを明らかにしたうえで、脅威の顕現化による影響が大きいと想定されるシステムから順番に、現時点での当該アルゴリズムの安全性低下の見通しを考慮しつつ優先的に移行期限を決定していくという方法が考えられる。

そのほか、SD にはデータの保管期間を考慮した移行スケジュールに関する留意点が記述されている。このように、保管期間中に暗号化データの復号や検証を行うケースでは、設定した移行期限から保管期間の分だけ遡った時点において暗号化やデジタル署名の生成を中止する必要がある。例えば、NIST では、PIV カードに搭載される 4 つのアプリケーションについて、暗号アルゴリズムを利用するデータを中・長期的に利用するか否かという観点からそれぞれ暗号アルゴリズムを利用したデータの生成を中止するタイミングを示している。

（ロ）暗号アルゴリズムの移行にかかる期間

ISO/TC68 による SD では、ハッシュ関数とブロック暗号の移行にかかる期間をそれぞれ 6 年程度、10～15 年程度としており、相対的にハッシュ関数よりブロック暗号の移行の方が時間を要するケースを想定している。さらに、ブロック暗号についてはブロック長が異なる暗号アルゴリズムへの移行の方が時間を要するほか、ハッシュ関数についてもハッシュ値のサイズが異なる暗号アルゴ

リズムへの移行の方が時間を要すると記述されている。

暗号アルゴリズムの移行を開始する時期を決定するには、移行にどの程度の期間が必要となるかを見積もったうえで移行スケジュールを検討することが求められる。SD の記述に基づくと、一般には移行に数年～十数年かかることを想定する必要があると考えられるが、移行期間は対象となるシステムの規模等に依存すると想定されることから、個々のシステムごとに移行期間の見積もりを行うことが求められる。

また、ISO/TC68 による SD には公開鍵暗号の移行期間に関する記述はないが、EMVCo においては IC カード認証に利用する公開鍵暗号の移行について、発行されているすべての IC カードの移行が完了するまでの期間を 12～15 年と見積もっている。

ロ．相互運用されているアプリケーションにおける対応

金融機関間で相互運用されているアプリケーションにおいては、移行を完了したシステムの安全性を確保しつつ全体としての移行を進めることが考えられる。つまり、暗号アルゴリズムの移行期間中は旧アルゴリズムと新アルゴリズムが共存することが想定されるが、新アルゴリズムに対応したシステムの安全性が他の対応が遅れているシステムの影響を受けないようなシステムの移行を実行するのが望ましい。

こうした方針としては、国際クレジットカード・ブランドが示したクレジットカードの取引システムにおける IC カード対応の事例が参考になろう。クレジットカード・システムを IC カード対応させるためには、世界中で発行されているクレジットカードを IC カードに移行させるとともに、世界中のカード発行機関のホスト・システム、ネットワーク、加盟店端末を IC カード対応させる必要がある。しかし、これらすべてを一斉に IC カード対応させることは現実的ではないことから、国際クレジットカード・ブランドでは、磁気ストライプカードと IC カードが混在するシステムを前提とし、そのうえで IC カードが IC カードとして処理されないという状況を回避する移行方針を示している（田村・廣川［2007］）。

ハ．SHA-1 の移行に関する対応

複数の暗号アルゴリズムを組み合わせて利用しているケースでは、同一の等価安全性を有する暗号アルゴリズムに同じタイミングで移行させることが求められる。ただし、ハッシュ関数については、SHA-1 の安全性が 63 ビット安全性に下方修正されていることから、衝突計算困難性に安全性を依拠するアプリケーションにおいては早期に対策を講じることが望ましい。ただし、SHA-1 の

移行については、暗号の研究者間においても、以下に紹介するとおり、さまざまな意見があり（Chang and Dworkin［2005］, Hoffman and Schneier［2005］）、必ずしもコンセンサスが得られているわけではない。SHA-1 の安全性を補強可能とする手段や移行にかかるコスト等を勘案して各々の事業者が決定していく必要がある[24]。

- NIST のスケジュールどおりに SHA-3 ファミリーが 2012 年に米国連邦政府標準暗号として認定された際、SHA-1 から SHA-2 ファミリーに移行した後に、再度 SHA-2 ファミリーから SHA-3 ファミリーへ移行することはコスト等の観点から現実的ではないため、当面は SHA-1 を使用し続けるのがよい。
- SHA-2 ファミリーについては、その設計方針やセキュリティ評価結果が NIST から公開されていないため、当面は SHA-1 を使い続け、NIST による SHA-3 ファミリーの発表後に SHA-1 から SHA-3 ファミリーに移行するのがよい。
- 暗号アルゴリズムの移行には時間がかかることを考慮すれば、SHA-1 への攻撃が現実的になってから移行を開始するという対応では遅すぎる。
- SHA-1 は既に十分な安全性を今後維持できないと評価されており、速やかに SHA-256 への移行を開始すべきである。
- 仮に SHA-2 ファミリーが暗号学的に安全でない、つまり、衝突ペアの探索にかかる計算量が 2^{128} 以下となる攻撃方法が発見された場合においても、こうした計算量が現実的な脅威と評価されるには大きなギャップがあると想定されることから、まずは SHA-2 ファミリーへ移行することが望ましい。

（2）スケジュールどおりに移行できなかった場合の対応

ISO/TC68 の SD は、ハッシュ関数の衝突計算困難性に安全性を依拠するアプリケーションでは SHA-1 の使用推奨期間を 2010 年末までとする一方、多くの場合 2010 年末までに SHA-1 を移行させることは実行困難とみられるとしたうえで、早急に移行に関する検討を開始するとともに、2010 年末までに移行できなかった場合への対応も検討しておくことが望ましいとしている。このような場合だけでなく、暗号解読技術の進展等によって移行完了前に当該暗号アルゴリズムの安全性が急激に低下してしまった場合についても想定しておくことが重要である。

---

[24] 暗号アルゴリズムを選択する際の主な論点については、宇根・神田［2006］において整理されており、そうした検討結果を参考にすることができる。

SHA-1 への対応措置としては、例えば、現時点で提案されている攻撃手法が適用できないように若干の変更を追加するということが考えられる。例えば、Szydlo and Yin［2006］において SHA-1 をサブルーチンとして呼び出す関数を構成することで、攻撃への耐性を付与する方法が提案されている。具体的には、ハッシュ関数の入力データをまず 32 ビットずつに分解し、分解されたデータをある拡張関数で拡張したものを SHA-1 への入力とすることで既存の攻撃手法に対しても安全な関数が構成できると述べられている。こうした方式の利用も緊急避難的な対策として考えられよう。

また、NISC による指針案では、移行完了前に暗号アルゴリズムの安全性の低下による影響が発生する状況を想定し、そうした場合においても業務を継続できるような体制を整えておくこととされている。本指針案では公開鍵認証基盤における緊急避難的な対応として、公開鍵証明書の失効、および、再発行等が挙げられている。移行前の旧暗号アルゴリズムを使用しつつ攻撃を回避するために、公開鍵証明書の有効期間を攻撃に必要な時間より短く設定するといったアイデアを採用したものと考えられる。例えば、CRYPTREC による 1,024 ビットの素因数分解の実行可能性に関する評価では、2010～2020 年には、いわゆるスーパーコンピュータを用いれば、1 年間程度の計算時間で、1,024 ビットの合成数の素因数分解が可能となると予想している（情報通信研究機構・情報処理推進機構［2007］）。こうした予想が現実のものとなった場合、例えば、1 年未満で鍵を更新するように公開鍵証明書のポリシーを変更するといった対応も考えられる。

（3）旧暗号アルゴリズムによるデータを長期保管する際の対応

ISO/TC68 による SD では、旧暗号アルゴリズムで生成したデジタル署名であっても、当該アルゴリズムの使用期限前に新暗号アルゴリズムで再署名する、あるいは、タイムスタンプを付与するといった方法があると述べられている。

デジタル署名については、その保管期間を考慮して暗号アルゴリズムを移行することが望ましいが、長期保管が必要なケースでは、SD が提示するような方法を採用することも考えられる。デジタル署名の長期利用については田村ほか［2005］において検討されているほか、長期署名プロファイルが JIS として制定されており（日本工業標準調査会［2008a, b］）、こうした技術を利用してデータの保管の検討を行うことも一案として考えられる。

（4）次の暗号アルゴリズム移行を考慮した対応

ISO/TC68 による SD の推奨対応策を長期的にみれば、2020 年、2030 年の時点でそれぞれ 96 ビット安全性、112 ビット安全性の暗号アルゴリズムをさらに安

全性の高いものに移行することとされている。このように、今回、移行の検討が求められている 80 ビット安全性をもつ暗号アルゴリズムの対応が完了した後も、将来的には同様の検討が求められることとなる。そのため、システムを設計するうえで将来的に変更が必要となる部分をコンポーネント化しておき、必要に応じて暗号モジュールを交換できるようにしておくことで柔軟な対応を可能にするということが考えられる。実際、NISC による指針においても、こうした対応例が記述されている。

暗号モジュールを利用するうえでは、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、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について確認することが必要である。仮に、暗号モジュールにセキュリティ上の何らかの欠陥があった場合、情報システム全体のセキュリティが確保できなくなるおそれがある。そのため、暗号モジュールの安全性を確認する必要がある。暗号モジュールが仕様書通りに実装されているか否かを確認する手段としては、米国・カナダ、および、わが国において運営されている暗号モジュール試験・認証制度を活用することが考えられる。

米国・カナダで運営されている CMVP（Cryptographic Module Validation Program）は、暗号モジュールが満たすべきセキュリティ要件を規定した FIPS 140-2（NIST［2001］）に基づく制度であり、FIPS として規定されたアルゴリズムと NIST による推奨アルゴリズムからなる「承認暗号アルゴリズム」を搭載した暗号モジュールを試験対象としている。本制度は 1995 年から運営されており、認証を取得した暗号モジュールは現時点で 1,000 件以上となっている。CMVP による認証の取得は米国連邦政府の調達基準となっていることから、認証を取得した暗号モジュールの中には 2011 年以降も利用可能な暗号アルゴリズムを搭載した暗号モジュールが多い。なお、わが国で運営されている JCMVP（Japan Cryptographic Module Validation Program）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試験対象とした制度であるが、運用を開始して間もないことから現時点で認証を取得した暗号モジュールはまだ数件にとどまっている。ただし、こうした暗号モジュール試験・認証制度を活用するにあたっては、その内容や限界を正しく認識しておく必要がある（田村・宇根［2008］）。

（5）暗号アルゴリズムの安全性評価に関する研究動向のフォロー

今回移行の対象となっている 2-key トリプル DES、1,024 ビット RSA、SHA-1 は、今後安全性が下方修正される可能性がある。こうした暗号アルゴリズムの安全性評価については、まず、学会で研究成果が発表されるケースが多いため、暗号アルゴリズムの移行に柔軟に対応していくには、今後も学会での研究動向

を注視しておく必要がある。特に注目される最近の研究動向として、以下のとおり暗号アルゴリズムの解読専用ハードウエアとハッシュ関数に関する主な研究が挙げられる。

イ．専用ハードウエアに関する研究

共通鍵暗号については、約 1 万ドル[25]で製造されたCOPACOBANAと呼ばれる専用ハードウエアによってDESが平均6.4日で解読可能であることが報告されている（Güneysu *et al*.［2007］）。2-keyトリプルDESについては、これまでのところ専用ハードウエアによる解読の研究成果は知られていない。

公開鍵暗号については、1990 年代後半から素因数分解専用ハードウエアに関する研究が盛んに進められている。現時点では、1,024 ビットの合成数については3,000万ドルかければ1年で素因数分解を可能とするハードウエアデザインが提案されているほか（Geiselmann and Steinwandt［2007］、情報通信研究機構・情報処理推進機構［2007］）。実際に専用ハードウエアによって 423 ビットの合成数を素因数分解したとの報告もある（Shimoyama［2006］）。

ロ．ハッシュ関数に関する研究

ハッシュ関数の安全性評価に関する最新の研究動向としては、SHA-1 の衝突計算困難性に関する研究はもとより、第 2 原像計算困難性や原像計算困難性に研究の対象が移行しているほか、対象とするハッシュ関数の範囲も SHA-256 や SHA-512 まで拡大してきている。

衝突計算困難性については、ステップ数を 24 ステップに縮退した SHA-256 においては衝突ペアが $2^{28.5}$ の計算量で発見されたほか、24 ステップの縮退版 SHA-512 についても 2^{53} の計算量で衝突ペアが発見可能との見積りが示されている（Indesteege *et al*.［2008］）。

第 2 原像計算困難性については、入力値が 2^{64} 程度と大きなケースでの SHA-1 については 2^{109} の計算量で探索可能の見積もりがあるほか（Andreeva *et al*.［2008］）、45 ステップの縮退版 SHA-1 については 2^{159} の計算量で探索可能との見積もりが発表されている（Cannière and Rechberger［2008］）。原像計算困難性について、SHA-1 の縮退版（34 ステップ）と SHA-256 における計算量がそれぞれ $2^{153.5}$ と 2^{249} と評価されている（Sasaki and Aoki［2008］）。

現在、学会では、次世代暗号アルゴリズムである AES、楕円曲線暗号、SHA-2 ファミリー等の安全性評価に関する研究が盛んに行われている。今後こうした

[25] 1990 年代後半に製造された DES の解読専用ハードウエアである Deep Crack は約 25 万ドルかかったといわれている（Güneysu *et al*.［2007］）。

研究成果によって、仮に、現時点で安全であると評価されている暗号アルゴリズムでの評価が下方修正された場合、NIST や CRYPTREC といった公的な暗号評価機関によって警鐘が鳴らされることとなる。ただし、こうした警鐘を受けて対応を開始すると、実際の安全性評価の下方修正から対応開始までには多少のタイムラグが生じることとなる。

今回の移行対象となっている暗号アルゴリズムは、基本的にはコンピュータ・パフォーマンスの向上によって解読に必要な計算が現実的な域に入りつつあるということを示すものであり、検討には時間的猶予が与えられたと考えることができる。ただし、一瞬にして暗号アルゴリズムが危殆化するといった状況が発生する可能性は否定できない。そうした場合には、ユーザにも早急な対応が求められることになるため、現在安全とされている暗号アルゴリズムについても継続的に研究動向をフォローすることが重要である。

7. おわりに

ISO/TC68 では、2005 年以降、暗号アルゴリズムの移行に関する検討が進められ、今般、ISO/TC68 としての推奨対応策が取り纏められた。ただし、ISO/TC68 における推奨対応策は、金融分野における一般的なアプリケーションを想定したものであることから、各金融機関が暗号アルゴリズムの移行を進める、あるいは、今後新規に暗号アルゴリズムの利用を検討していくうえでは、本推奨対応策を参考に個々のアプリケーションに応じてリスク分析を行い、必要な対応を行うことが重要である。

金融業界は、1990 年代にも DES からトリプル DES への移行問題を経験している。当時の移行は、ブロック長が同じ暗号アルゴリズムであったほか、基本的には各金融機関内、あるいは、金融業界内でのクローズド・システムにおける移行が問題となった。これに対し、今回は、トリプル DES から AES といったブロック長が異なる暗号アルゴリズムへの変更が推奨されているほか、公開鍵暗号やハッシュ関数も検討の対象となっている。さらに、インターネット・バンキングをはじめとしてオープンなネットワークを利用した金融サービスにおける暗号アルゴリズムの取扱いについても検討対象となっており、顧客への対応の呼掛けやネットワーク事業者等との調整が必要となる場面も想定される。そのため、各金融機関には十分な検討が求められるとともに、今般の暗号アルゴリズムの移行問題を契機として、暗号アルゴリズムの危殆化や世代交代に柔軟に対応できる体制を整備していくことが重要である。

以　上

参考文献

秋山卓司、『暗号アルゴリズム 2010 年問題　事例：電子証明書の国際標準化の動きと日本の携帯』、JNSA PKI 相互運用技術 WG 主催セミナー PKI Day 2008 パネルディスカッション講演資料、2008 年（http://www.jnsa.org/seminar/2008/0703/）

岩下直行、「次世代暗号技術への移行に関するユーザ側の取り組みについてー金融情報システムにおける暗号技術の国際標準化を巡る議論を中心に」、『連続セミナー2007 情報セキュリティ 2.0ー自由と統制の時代の情報セキュリティーー第 6 回次世代暗号技術への移行に向けた課題と対応』、情報処理学会、2007 年

宇根正志・神田雅透、「暗号アルゴリズムにおける 2010 年問題について」、『金融研究』第 25 巻別冊第 1 号、日本銀行金融研究所、2006 年、31～72 頁

金融情報システムセンター（FISC）、『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』、金融情報システムセンター、2006 年

――――――、「平成 19 年度金融機関等のコンピュータシステムに関する安全対策実施状況調査報告書」、『金融情報システム』平成 20 年 9 月増刊 65 号、金融情報システムセンター、2008 年

情報通信研究機構（NICT）・情報処理推進機構（IPA）、『電子政府推奨暗号の利用方法に関するガイドブック』、NICT・IPA、2008 年

――――――・――――――、『CRYPTREC Report 2006』、NICT・IPA、2007 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（http://www.cryptrec.jp/images/cryptrec_01.pdf）

――――――・――――――、『電子政府推奨暗号リストの改訂に関する骨子（案）』、総務省・経済産業省、2008 年

内閣官房情報セキュリティセンター（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 に係る移行指針（案）』、NISC、2008 年

田村裕子・宇根正志、「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」、『金融研究』第 27 巻別冊第 1 号、日本銀行金融研究所、2008 年、79～114 頁

――――――・――――――・岩下直行・松本 勉・松浦幹太・佐々木良一、「デジタル署名の長期利用について」、『金融研究』第 24 巻別冊第 1 号、日本銀行金融研究所、2005 年、121～176 頁

――――――・廣川勝久、「リテール・バンキング・システムの IC カード対応に

関する現状とその課題」、『金融研究』第 26 巻別冊第 1 号、日本銀行金融研究所、2007 年、101～128 頁
中山靖司、「インターネット・バンキングの安全性を巡る現状と課題－2007 年」、『日銀レビュー・シリーズ』、日本銀行、2007 年
日本銀行金融研究所、「金融情報技術の国際標準化について」、『日本銀行調査季報』秋（10 月）号、日本銀行、2006 年 a
――――――、『ISO/TC68/SC2-6-7 国内検討委員会議事録（平成 17 年 8 月 30 日付）』、日本銀行金融研究所、2005 年 a
――――――、『ISO/TC68/SC2-6-7 国内検討委員会議事録（平成 17 年 10 月 25 日付）』、日本銀行金融研究所、2005 年 b
――――――、『ISO/TC68/SC2-6-7 国内検討委員会議事録（平成 18 年 10 月 25 日付）』、日本銀行金融研究所、2006 年 b
――――――、『ISO/TC68/SC2-7 国内検討委員会議事録（平成 19 年 12 月 13 日付）』、日本銀行金融研究所、2007 年
日本工業標準調査会（JISC）、『JIS X 5092：2008 CMS 利用電子署名（CAdES）の長期署名プロファイル』、日本規格協会、2008 年 a
――――――、『JIS X 5093：2008 XML 署名利用電子署名（XAdES）の長期署名プロファイル』、日本規格協会、2008 年 b
Andreeva, Elena, Charles Bouillaguet, Pierre-Alain Fouque, Jonathan J. Hoch, John Kelsey, Adi Shamir, and Sebastien Zimmer, “Second Preimage Attacks on Dithered Hash Functions,” *Proceedings of Eurocrypt 2008*, LNCS4985, Springer-Verlag, 2008, pp.270-288.
CA/Browser Forum (CABF), *Guidelines for the Issuance and Management of Extended Validation Certificate*s v1.1, CA/Browser Forum, 2008 (available in http://www.cabforum.org/documents.html).
Cannière, Christophe de, Florian Mendel, and Christian Rechberger, “On the Full Cost of Collision Search for SHA-1,” *Presentation at ECRYPT Hash Workshop*, 2007.
――――――, and Christian Rechberger, “Preimages for Reduced SHA-0 and SHA-1,” *Proceedings of CRYPTO 2008*, LNCS 5157, Springer-Verlag, 2008, pp. 179-202.
Certicom, *Certicom Intellectual Property,* Certicom, 2008（available in http://www.certicom.com/ index.php/certicom-intellectual-property）.
Chang, Chu-jen, and Morris Dworkin, *Workshop Report The First Cryptographic Hash Workshop*, NIST, 2005 （ available in http://csrc.nist.gov/groups/ST/hash/documents/ HashWshop_2005_Report.pdf）.
EMVCo, *EMV ICC Specifications for Payment Systems v4.1x RSA+ Book2*, EMVCo, 2007a.

————————, *EMV ICC Specifications for Payment Systems v4.1y RSA++ Book2*, EMVCo, 2007b.

————————, *EMV ICC Specifications for Payment Systems v4.1z ECC Book2*, EMVCo, 2007c.

————————, *EMV Integrated Circuit Card Specifications for Payment Systems Book2 Security and Key Management Version 4.2*, EMVCo, 2008a.

————————, *New Cryptography Drafts*, EMVCo, 2007d（available in http://www.emvco.com/ specifications.asp?show=94）.

————————, *Notice Bulletin No.12 EMVCo Annual RSA Key Lengths Assessment*, EMVCo, 2008b.

European Network of Excellence in Cryptology (ECRYPT), *D.SPA.21 ECRYPT Yearly Report on Algorithms and Keysizes (2006)*, 2007.

Geiselmann, Willi, and Rainer Steinwandt, "Non-wafer-Scale Sieving Hardware for the NFS: Another Attempt to Cope with 1024-Bit," *Proceedings of Eurocrypt 2007*, LNCS 4515, Springer-Verlag, 2007, pp. 466-481.

Güneysu, Tim, Christof Paar, Jan Pelzl, Gerd Pfeiffeer, Manfred Schimmler, and Christian Schleiffer, "Parallel Computing with Low-Cost FPGAs-A Framework for COPACOBANA," *Proceedings of ParaFPGA Symposioum LNI 2007*, 2007.

Hoffman, Paul, and Bruce Schneier, "Request for Comments: 4270 Attacks on Cryptographic Hashes in Internet Protocols," 2005（available in http://www.ietf/rfc/rfc4270.txt）

Indesteege, Sebastiaan, Florian Mendel, Bart Preneel, and Christian Rechberger, "Collisions and other Non-Random Properties for Step-Reduced SHA-256," *Proceedings of SAC 2008*, Springer-Verlag, 2008.

International Organization for Standardization (ISO), *Financial services – Recommendations on cryptographic algorithms and their use – Standing Document*, 2007.

————————, and International Electrotechnical Commission (IEC), *ISO/IEC JTC1/SC27 Standing Document No.12 (SD12) on the Assessment of Cryptographic Algorithms and Key-Lengths – 1st Draft*, 2007.

Menezes, Alfred J., Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applid Cryptography*, CRC Press, 1997.

Mitchell, Chris J., "A new key recovery attack on the ANSI retail MAC," 2002（available in http://www.isg.rhul.ac.uk/~cjm/ankrao.pdf）.

National Institute of Standards and Technology (NIST) "Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm

(SHA-3) Family," *Federal Register*, Vol. 72, No. 212, U.S. Government Printing Office, 2007a.

———, *NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General* , NIST, 2005a.

———, *NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General (Revised)*, NIST, 2007b.

———, *NIST Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST, 2005b.

———, *NIST Special Publication 800-78-1, Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST, 2007c.

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

National Security Agency (NSA), *Fact Sheet NSA Suite B Cryptography*, NSA, 2005.

Oorshot, Paul van, and Michael Wiener, "A Known-Plaintext Attack on Two-Key Triple Encryption," *Proceedings of EUROCRYPT'90*, LNCS 473, Springer-Verlag, 1990, pp. 138-325.

Sasaki, Yu, and Kazumaro Aoki, "Preimage Attacks on MD, HAVAL, SHA, and Others," *Presentation at CRYPTO 2008 Rump Session*, 2008.

———, Lei Wang, Kazuo Ohta, and Noburu Kunihiro, "Security of MD5 Challenge and Response: Extension of APOP Password Recovery Attack," *Proceedings of CT-RSA 2008*, LNCS 4964, Springer-Verlag, 2008, pp. 1-18.

Shimoyama, Takeshi, *Factoring c128 in 7^352+1 by using special sieving hardware*, 2006（available in http://www.loria.fr/~zimmerma/records/c128）.

Stevens, Marc, Arjen Lenstra, and Benne de Weger, "Chosen-prefix for MD5 and Colliding X.509 Certificates for Different Identities," *Proceedings of Eurocrypt 2007*, LNCS 4515, Springer-Verlag, 2007, pp.1-22.

Szydlo, Michael, and Yiqun Lisa Yin, "Collision-Resistant Usage of MD5 and SHA-1 via Message Preprocessing," *Proceedings of CT-RSA 2006*, LNCS 3860, Springer-Verlag, 2006, pp. 99-114.

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

Wang, Xiaoyun, Andrew Yao, and Frances Yao, "New Collision Search for SHA-1," *Presentation at CRYPTO 2005 Rump Session*, 2005,