

IMES DISCUSSION PAPER SERIES

暗号アルゴリズムにおける2010年問題について

うね まさし ・ かんた まさゆき
宇根 正志 ・ 神田 雅透

Discussion Paper No. 2005-J-22

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 日本橋郵便局私書箱 30 号

日本銀行金融研究所が刊行している論文等はホームページからダウンロードできます。

<http://www.imes.boj.or.jp>

無断での転載・複製はご遠慮下さい。

備考： 日本銀行金融研究所ディスカッション・ペーパー・シリーズは、金融研究所スタッフおよび外部研究者による研究成果をとりまとめたもので、学界、研究機関等、関連する方々から幅広くコメントを頂戴することを意図している。ただし、ディスカッション・ペーパーの内容や意見は、執筆者個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではない。

暗号アルゴリズムにおける2010年問題について

うね まさし † ・ かんた まさゆき *
宇根 正志 † ・ 神田 雅透 *

要 旨

金融分野においては、金融取引に用いられる各種データの機密性や一貫性を確保する手法、あるいは、取引相手を認証する手法の要素技術として暗号アルゴリズムが活用されている。現時点では、共通鍵暗号は 2-key トリプル DES と RC4、公開鍵暗号は鍵長 1024 ビットの RSA、ハッシュ関数は 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等を前提とすると、今後 10～15 年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間で強まっている。また、従来暗号アルゴリズムの安全性について実質的に「お墨付き」を付与してきた米国立標準技術研究所 (NIST) は、より安全な次世代の暗号アルゴリズムへの移行を図るため、2-key トリプル DES や鍵長 1024 ビットの RSA や SHA-1 など現在主流とされている暗号アルゴリズムを 2011 年以降米国連邦政府機関のシステムで使用しない方針を各種ガイドラインの中で示している。

こうしたことから、暗号アルゴリズムの移行を今後どのように進めるかが重要な問題となっており、本稿ではこうした問題を総称して「暗号アルゴリズムにおける 2010 年問題」と呼ぶ。NIST が期限として定めている 2010 年までに移行を完了させるためには、本問題への対応について早急に検討を開始することが求められる。

本稿では、現在主流とされている暗号アルゴリズムの安全性評価結果について紹介したうえで、暗号アルゴリズムにおける 2010 年問題とその影響、NIST の対応状況等について説明する。さらに、今後金融分野において本問題に対処していくうえで留意すべき点について考察する。

キーワード: 暗号アルゴリズム、共通鍵暗号、公開鍵暗号、セキュリティ、
2010 年問題、ハッシュ関数、トリプル DES、RC4、RSA、SHA-1
JEL classification: L86、L96、Z00

† 日本銀行金融研究所情報技術研究センター (E-mail: masashi.une@boj.or.jp)

* NTT 情報流通プラットフォーム研究所 (E-mail: kanda.masayuki@lab.ntt.co.jp)

本稿の作成に当たっては、東京大学の今井秀樹教授、横浜国立大学の松本 勉教授から有益なコメントを頂いた。ここに記して感謝したい。本稿に示されている意見は日本銀行あるいは金融研究所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：エグゼクティブサマリーをかねて	1
2 . 現在主流となっている暗号アルゴリズム	5
(1) 国際標準やガイドライン等に記述されている暗号アルゴリズム	5
(2) IETF 標準に規定されている暗号アルゴリズム	7
3 . 主要な暗号アルゴリズムの安全性評価結果	9
(1) 共通鍵暗号	9
(2) 公開鍵暗号	13
(3) ハッシュ関数	16
4 . NIST と 2010 年問題	18
(1) 暗号アルゴリズム選定における NIST のスタンス	18
(2) ISO/TC68 における過去の対応：DES およびトリプル DES の場合	22
(3) 2010 年問題への対応とその影響	23
5 . 2010 年問題等への対応のあり方	25
(1) 各種機関・プロジェクトによって規定 / 認定 / 推奨されている暗号アルゴリズム	25
(2) 暗号アルゴリズムを選択する際の主な論点	33
(3) その他の留意点	36
(4) 中期的な検討課題	38
6 . おわりに	40
【参考文献】	41

1. はじめに：エグゼクティブサマリーをかねて

金融分野においては、各種金融取引における安全性を確保するために暗号アルゴリズムが広く利用されている。例えば、銀行の ATM とホスト・コンピュータ間で交信されるデータ（暗証番号や口座番号等）の機密性や一貫性の確保、インターネット・バンキングにおけるホストやクライアントの認証といった場面において暗号アルゴリズムが活用される。機密性を確保する手段として共通鍵暗号が用いられるほか、データの一貫性や通信相手を確認する手段として、共通鍵暗号に基づくメッセージ認証コード（MAC：message authentication code）や公開鍵暗号に基づくデジタル署名が用いられるケースが多いとみられる。

具体的にどのような暗号アルゴリズムが利用されているかに関しては、金融分野における情報セキュリティ技術の国際標準や各種ガイドラインを参照することができる。例えば、金融取引用の暗証番号（PIN：personal identification number）等の暗号化に関する国際標準 ISO 9564-2（ISO [2005a]）は、PIN 自体の暗号化のアルゴリズムとしてトリプル DES を規定しているほか、トリプル DES の鍵配送用のアルゴリズムとして RSA を規定している。公開鍵暗号の鍵管理方法に関する国際標準 ISO 11568-2（ISO [2005b]）は、ハッシュ関数として SHA-1 を含むいくつかのアルゴリズムを規定している。これらの暗号アルゴリズムの中でも、トリプル DES については 2 つの異なる鍵を用いる 2-key トリプル DES が、RSA については鍵長を 1024 ビットに設定した方式（以下、1024 ビット RSA と呼ぶ）が主流となっているとみられる。また、インターネット・バンキング等においては、SSL version 3.0/TLS version 1.0 に規定される RC4 が広く利用されているとみられている。

しかしながら、これらのアルゴリズムを今後も長期にわたって使用しつづけることは難しい情勢になってきている。例えば、米国立標準技術研究所（NIST：National Institute of Standards and Technology）は、米国連邦政府機関における 2-key トリプル DES と 1024 ビット RSA の利用を 2010 年までとする方針を各種ガイドラインにおいて示しているほか、SHA-1 についても 2010 年までに利用を中止する方針を別途発表している。また、RC4 に関しては、もともと NIST が認定あるいは推奨する暗号アルゴリズムとなっていない。

NIST による米国連邦政府標準暗号の承認といったかたちでの暗号アルゴリズムの認定は、金融分野をはじめとする幅広い分野において、公的機関による暗号アルゴリズムの安全性の「お墨付き」として機能してきた。例えば、1977 年に米国連邦政府標準暗号 FIPS 46 として認定された DES は、その後事実上の共通鍵暗号の国際標準として普及してきた経緯がある。こうした観点からみれば、

現在主流となっている暗号アルゴリズムの安全性に関する NIST のお墨付きは 2010 年で失われてしまうことを意味する。

NIST の動きの背景として、第 1 に、暗号解読技術の進展、計算機のコスト・パフォーマンスの向上、分散コンピューティング環境の整備等によって、2-key トリプル DES、1024 ビット RSA、SHA-1 をはじめとする 1990 年代中頃以前に開発された暗号アルゴリズムの安全性低下が顕著となってきた点が挙げられる。既存の安全性評価結果をベースとしたうえで、今後のコンピュータのコスト・パフォーマンスが一定条件で向上しつづけると想定した場合、これらの暗号アルゴリズムは、今後 10～15 年といった長期にわたって十分な安全性を確保することが困難になるとの見方が暗号研究者の間で強まっている。こうした見方を裏付けるものとして、例えば、2005 年には、663 ビット合成数が実際に素因数分解されたほか、最良の攻撃法と考えられていた誕生日攻撃法¹の場合よりも少ない計算量によって SHA-1 の衝突（ハッシュ値が同一となるような異なる入力値のペア）が探索可能であるとの研究成果が発表された。

第 2 の背景として、現在主流となっている暗号アルゴリズムよりも、安全性（および処理速度等）の観点で優れた暗号アルゴリズムが利用可能になりつつあるという点が挙げられる。NIST による AES の公募・選定が行われた後、欧州では暗号アルゴリズムの評価プロジェクト NESSIE（New European Schemes for Signatures, Integrity, and Encryption）による推奨暗号（以下、NESSIE 推奨暗号と呼ぶ）の公募・選定が行われたほか（NESSIE consortium [2003]）、わが国においては CRYPTREC による暗号アルゴリズムの評価と電子政府推奨暗号リストの作成が行われた（総務省・経済産業省 [2003]）。ISO においては、これらの評価結果を参照するかたちで、暗号アルゴリズムの国際標準 ISO/IEC 18033 シリーズの策定が進められており、ブロック暗号およびストリーム暗号のパート（ISO/IEC 18033-3, 4）が既に国際標準として成立している（ISO/IEC [2005a, b, c]）。このように、暗号研究者による暗号アルゴリズムの各種評価プロジェクトの結果や国際標準を参照することによって、安全性等の面で信頼できる次世代の暗号アルゴリズムが容易に選択可能になりつつある。

現在主流となっている暗号アルゴリズムに対する NIST のお墨付きが 2010 年で失われることを考慮すると、金融分野における情報システムの安全性や信頼

¹ 誕生日攻撃法は、バースデー・パラドックスに基づいたハッシュ関数の攻撃手法であり、同一の出力値となる異なる入力値ペアを探索するというものである。バースデー・パラドックスは、23 人から構成されるグループの中で少なくとも 2 人の誕生日が一致する確率が 0.5 を超えるという事実のことであり、1 年が 365 日によって構成されていることを考えると直感的な印象からはかなり少ない人数ですむことから「パラドックス」として位置づけられている。

性を維持しつづけるという観点からは、2011 年以降も長期間安全性を確保することが可能であるとの評価を得ている暗号アルゴリズムに今後移行することが求められる。一方、暗号アルゴリズムを変更するとなると、個々の金融機関における情報システムの変更が必要となることに加え、複数の金融機関における情報システム間の互換性を確保するための対応も必要となるケースが考えられる。したがって、暗号アルゴリズムの移行には、システム変更に伴って相応の費用が必要になるほか、金融業界におけるコンセンサス形成等も不可欠であり、移行のための準備期間も十分に確保しておく必要が出てくると予想される。

このように、情報システムの安全性や信頼性を損なうことなく、短期間のうちに暗号アルゴリズムの移行をスムーズに完了させるためには、どのような対応が望ましいかについて検討することが重要な課題になっている。本稿では、2010 年に向けた暗号アルゴリズムの移行に伴う問題を総称して、「暗号アルゴリズムにおける 2010 年問題」(以下、単に「2010 年問題」)と呼ぶ。

金融機関が 2010 年問題に対応しようとする際、まずは、どのような暗号アルゴリズムに移行するべきかということが問題となる。この点について、DES からトリプル DES への移行時とは異なるのは、現在 NIST 以外でも暗号アルゴリズムの評価が第三者機関によって実施されているということである。すなわち、CRYPTREC による電子政府推奨暗号や、NESSIE 推奨暗号が公表されている(本文表 5(4)参照)。また、これらを参照するかたちで ISO/IEC 18033 シリーズ(守秘目的の暗号アルゴリズムを規定する国際標準)の策定が ISO/IEC JTC1/SC27 において進められている。これらを参考にしながら、より安全性の高い暗号アルゴリズムへの移行について検討することが望まれる。

さらに中長期的な課題としては、2010 年問題のように、暗号アルゴリズムの安全性低下に伴う問題(いわゆる、暗号アルゴリズムの危殆化)に迅速かつ適切に対応できるように、暗号アルゴリズムの安全性評価の最新情報をフォローするとともに、NIST 等の動向を注視する体制を構築することが望ましいと考えられる。また、暗号アルゴリズムの変更や鍵長の伸長を円滑に行うことができるという意味での「拡張性」を有する情報システムの実現に向けた検討も望まれる。

本稿は、金融機関が 2010 年問題について検討する際に参考になる情報を提供することを目的としている。2 節では、現時点で金融分野においてどんな暗号アルゴリズムが使われているかについて、国際標準やガイドラインを中心に整理する。3 節においては、2 節で取り上げた暗号アルゴリズムに関して現時点における安全性評価結果を整理する。4 節においては、既存の暗号アルゴリズムの安全性低下に対する NIST の対応方針について説明し、2010 年問題が金融分野にどのような影響を及ぼす可能性があるかを考察する。5 節においては、どのよう

な暗号アルゴリズムを選択すべきかという観点から、ISO/IEC 18033 シリーズにおいて規定されているもの、NIST において認定あるいは推奨されているもの、CRYPTREC、NESSIE において推奨されているものを紹介したうえで、どの暗号アルゴリズムに移行するかについて検討する際の論点や、その移行を進めるうえで留意すべき点、さらには、暗号アルゴリズムの危殆化という観点から今後金融機関が対処することが望ましいと考えられる検討課題を示す。6 節では、2010 年問題への対応の重要性について再度説明したうえで本稿を締めくくる。

2. 現在主流となっている暗号アルゴリズム

最初に、金融分野においてどのような暗号アルゴリズムが使われているかを、国際標準やガイドライン等に規定されているもの、および、インターネット・バンキング等における利用という観点でインターネット標準である IETF の標準に規定されているものに分けて整理する。

(1) 国際標準やガイドライン等に記述されている暗号アルゴリズム

各金融機関のネットワークや情報システムにおいてどのような暗号アルゴリズムが利用され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。そこで、金融分野における情報セキュリティ技術の国際標準の策定・管理を担当している ISO/TC68 の国際標準やその他の各種ガイドラインを参照し、どのような暗号アルゴリズムが記述されているかを整理すると表 2(1)のとおりである。

表 2(1)をみると、共通鍵暗号においては、トリプル DES が中心となっていることがわかる。ISO 9564-1 (ISO [2002]) においては、鍵長を少なくとも 112 ビットとすることが規定されており、2-key のトリプル DES での利用が前提となっている。本標準以外では 2-key のトリプル DES に限定した記述が明記されているものは見当たらず、3-key のトリプル DES も含まれるかたちとなっている。AES に関しては、ISO/TR 17944 (金融システムにおけるセキュリティの枠組み) において推奨暗号アルゴリズムとして記述されているのみである (ISO [2002b])。

公開鍵暗号に関しては、公開鍵暗号に関連するすべての ISO/TC68 傘下の国際標準に RSA が規定されている。RSA の推奨鍵長については、ISO/TR 13569 において 1024 ビット以上を推奨する旨が記述されているのみである (ISO [1998b])。RSA 以外のアルゴリズムとしては、DSA と ECDSA が ISO/TR 17944 に推奨暗号アルゴリズムとして記述されている。DSA、ECDSA の鍵長については、ISO/TR 13569 に従うとすれば、それぞれ 1024 ビット以上、160 ビット以上となる。

ハッシュ関数については、ハッシュ関数に関するすべての ISO/TC68 国際標準に共通して SHA-1 が規定されている。ただし、公開鍵暗号を用いる鍵管理の国際標準案 ISO/DIS 11568-4 では、「ISO/IEC 10118 シリーズ (汎業界向けのハッシュ関数の国際標準) に規定されているハッシュ関数を利用すること」との規定が置かれており、SHA-1 以外のハッシュ関数も規定されている (ISO [1998a])。

その他、国際標準ではないが広く参照されている業界標準として、全銀協 IC キャッシュカード仕様 (JBA [2001])、IC カードの業界標準である EMV (version 4.1、EMVco [2004])、欧州におけるカード・リーダ/ライタの技術仕様である

表 2(1) ISO/TC68 の国際標準に規定されている暗号アルゴリズム

国際標準・ガイドライン	共通鍵暗号	公開鍵暗号	ハッシュ関数
ISO 10126-2(NP 審議中) メッセージ暗号化	DES	(記載なし)	(記載なし)
ISO 16609(MAC の要件)	・DES ・TDES	(記載なし)	(記載なし)
ISO TR 13569 ガイドライン	鍵長 80 ビット以上	鍵長 1024 ビット以上(楕円曲線暗号の場合は 160 ビット以上)	(記載なし)
ISO 11568-2 鍵管理(共通鍵暗号)	TDES	(記載なし)	(記載なし)
ISO TR 17944 セキュリティ管理の枠組み	・TDES(ANS X9.52) ・AES(FIPS 197)	・RSA(ANS X9.31) ・DSA(ANS X9.30-1) ・ECDSA(ANS X9.62) ・ISO/IEC 15946 ・ISO/IEC 9796 ・ISO/IEC 14888	ISO/IEC 10118 ・10118-2: 共通鍵暗号ベースの方式(4つ)を規定 ・10118-3: RIPEMD-(128, 160)、SHA-(1, 224, 256, 384, 512)、Whirlpool ・10118-4: MASH-1,2
ISO/DIS 11568-4 鍵管理(公開鍵暗号)	(記載なし)	・RSA(ISO/IEC 9796) ・DSA	・10118-4: MASH-1,2
ISO 9564-1, 2 PIN の暗号化	TDES(鍵長は少なくとも 112 ビット)	RSA(EMV)	(記載なし)
ISO TR 19038 TDES の利用モード	TDES	(記載なし)	(記載なし)
【参考】全銀協 IC キャッシュカード標準仕様(13年版、奨励)	・DES ・TDES(2-key の明示はないが EMV に準拠)	RSA(鍵長は 1984 ビット以下、EMV と同じ)	SHA-1
【参考】EMV version 4.1	2-key TDES	RSA(ISO/IEC 9796-2、鍵長は 1984 ビット以下)	SHA-1
【参考】FINREAD	・DES ・TDES	RSA(鍵長は 1024 ビット以上)	・SHA-1 ・MD5 ・RIPEMD-160

備考：“TDES”は「トリプルDES」を意味する。

FINREAD(CEN/ISSS [2002])をみると、上記と同様の傾向にあることがわかる。特に、EMV に関しては、共通鍵暗号として 2-key のトリプルDESが規定されている点が注目される。

これらの国際標準やガイドライン等に沿ったかたちで金融機関が暗号アルゴリズムを採用しているとすれば、金融分野においては共通鍵暗号アルゴリズムとしてトリプルDESが広く利用されていると考えることができる。

トリプルDESの暗号鍵の利用形態として 2-key と 3-key のどちらが採用されているかについては、公表されている資料からは定かでない。ただし、ISO 9564-1において、PINの暗号化に用いられる鍵のサイズを少なくとも 112 ビットにすることの規定が置かれていること、全銀協のICキャッシュカード標準仕様をはじめとして、2-key トリプルDESの利用を定めているEMVを採用しているアプリケーションも多いことを勘案すると、2-key トリプルDESを採用しているケー

すが金融分野においては比較的多いのではないかと考えられる²。

RSA についても、鍵長に関して ISO/TR 13569 に 1024 ビット以上が推奨されるとの記述がみられるだけである。ただし、RSA の暗号化・復号処理あるいは署名生成・検証処理をなるべく効率的に実施するという観点から考えると、推奨鍵長の中で最短の 1024 ビットを採用するという選択が自然であると考えられる。実際に、1024 ビット RSA を利用している事例として、SWIFT の BKE(bilateral key exchange) を挙げることができる (SWIFT [2000])。BKE は、金融機関間において決済情報を送信するネットワーク・システムである SWIFTNet において暗号化通信を行う際に MAC 生成用鍵の配送を行うシステムであり、鍵配送用の暗号アルゴリズムとして 1024 ビット RSA を利用している旨を公表している。また、EMV のセキュリティ・ガイドライン(EMVco [2005])においては、IC カードに実装する RSA の推奨鍵長が記述されており、2009 年末までの利用を想定する場合には 1024 ビットが推奨されている。なお、本ガイドラインでは、2012 年末、2014 年末、2016 年末までの利用を想定する場合の推奨鍵長も記載されており、それぞれ 1152 ビット、1408 ビット、1984 ビットに設定されている。

(2) IETF 標準に規定されている暗号アルゴリズム

金融機関は、インターネット・バンキングのサービスを提供する際に、利用者の認証(クライアント認証)や通信データの暗号化を行うために暗号アルゴリズムを利用している。こうした暗号化・認証の機能は、インターネット・エクスペアラやネットスケープ等のブラウザに標準装備されている SSL(Secure Sockets Layer)によって実現しているケースが多い。SSL は、TLS(Transport Layer Security) version 1.0 として IETF (Internet Engineering Task Force) の RFC に規定されている (Dierks and Allen [1999]、Blake-Wilson, Nystrom, Hopwood, Mikkelsen, and Wright [2003])ほか、TLS version 1.1 の Internet draft が提案されている(Dierks and Rescorla [2005]、Blake-Wilson, Nystrom, Hopwood, Mikkelsen, and Wright [2005])。

SSL version 3.0/TLS version 1.0 において利用される暗号アルゴリズムとしては、共通鍵暗号がトリプル DES、DES、RC2、RC4、IDEA、AES、Camellia、SEED、公開鍵暗号が RSA、DSA、Diffie-Hellman 鍵配送方式(以下、DH と呼ぶ) ハッシュ関数が SHA-1、MD5 となっている。これらのうち、共通鍵暗号については、トリプル DES と RC4 が利用されるケースが多いとみられている。また、公開鍵暗号については、公開鍵の鍵長として 1024 ビットを採用するケースが大勢となっているといわれている (Preneel *et al.*[2004]ほか)。

² 金融分野における 2-key トリプル DES の実装件数は多いとの見方もある (岩下[2004])。

このほか、IETF の RFC に規定されている暗号アルゴリズムとしては、共通鍵暗号では MISTY1、公開鍵暗号では楕円曲線ベースの ECDH、ECDSA などが挙げられる。

3. 主要な暗号アルゴリズムの安全性評価結果

2 節においては、金融分野の国際標準・ガイドラインに規定されている暗号アルゴリズム、および、SSL/TLS などの IETF 標準に規定されている暗号アルゴリズムを整理した。本節では、これらの暗号アルゴリズムの安全性評価結果を紹介する。

(1) 共通鍵暗号

共通鍵暗号は、ブロック暗号 (block cipher) とストリーム暗号 (stream cipher) の 2 つに分けられる。ブロック暗号は、暗号化の対象となる平文を一定のサイズに区切って (区切られたものは“ブロック”と呼ばれる) ブロックごとに順々に暗号化していくというものである。ストリーム暗号は、平文のサイズと同じサイズの擬似乱数を生成し、1 ビットずつ順々に排他的論理和を計算することによって暗号文を生成するというものである。以下では、これらの分類にしたがって、2 節で紹介したトリプル DES、DES、RC2、IDEA、MISTY1、AES、Camellia、SEED (以上、ブロック暗号) と、RC4 (ストリーム暗号) を対象とした安全性評価結果を説明する。

イ. ブロック暗号

ブロック暗号に対する攻撃法は、ショート・カット攻撃 (short cut attacks) とブルート・フォース攻撃 (brute force attacks) に分類される。ショート・カット攻撃は、攻撃対象となる暗号アルゴリズムにおけるアルゴリズム上の欠陥を手掛かりとして暗号鍵を効率よく探索するという攻撃であり、ブルート・フォース攻撃は、アルゴリズム上の欠陥を利用するのではなく、暗号鍵の候補を 1 つ 1 つ試して暗号鍵や平文に関する情報を得ようとする攻撃である。

(イ) ショート・カット攻撃

ショート・カット攻撃は暗号アルゴリズムのアルゴリズム上の欠陥を利用する攻撃であり、どのようなタイプのショート・カット攻撃が適用可能かは、各暗号アルゴリズムの構造に依存する。

ショート・カット攻撃が有効であるというのは、当該攻撃を実行するために必要となる計算量が最も初歩的な攻撃である全数探索攻撃³に必要な計算量を

³ 全数探索攻撃は、真の暗号鍵の候補となるものを 1 つ 1 つしらみつぶしに試して鍵の探索を行うという攻撃であり、ブルート・フォース攻撃の 1 種である。鍵長が n ビットの暗号の場合、全数探索攻撃によって確率 1 で真の鍵を見つけるための計算量は 2^n となる。

表 3(1) ブロック暗号におけるショート・カット攻撃に対する安全性

暗号アルゴリズム	鍵長	ブロック長	ショート・カット攻撃の適用結果
トリプル DES (2-key/3-key)	112 or 168	64	【安全】全数探索攻撃よりも少ない計算量によって暗号鍵を推定可能なショート・カット攻撃は提案されていないようである。
RC2	可変 (SSL v.3.0/TLS v.1.0 では 40)	64	【学術的に解読された】全数探索攻撃よりも少ない計算量によって暗号鍵を推定可能な攻撃(差分解読法)が既に提案された。
IDEA	128	64	【安全】全数探索攻撃よりも少ない計算量によって暗号鍵を推定可能なショート・カット攻撃は提案されていないようである。
MISTY1	128	64	
AES	128, 192, 256	128	
Camellia	128, 192, 256	128	
SEED	128	128	

備考：本表は平成 17 年 11 月 7 日現在の情報を利用して作成した。

下回る場合であり、こうした状況を「当該暗号アルゴリズムは学術的に解読された」といった表現で呼ぶケースが多い。学術的に破られた暗号アルゴリズムは実運用上直ちに安全でないと判断されることは少ないが、本来満たすべき設計基準を満たしていないという意味で当該暗号アルゴリズムの設計者に対する信頼が揺らぎ、もっと致命的な欠陥が存在するのではないかとの疑念が生まれ、利用される機会が相対的に少なくなっていくという結果をもたらす。

各暗号アルゴリズムに対してこれまでに提案されているショート・カット攻撃について整理すると、表 3(1)のとおりである。RC2 が差分解読法⁴に対して学術的に解読されてしまうことが示されている (IPA・TAO [2002]) もの、その他の暗号アルゴリズムについては解読につながる強力なショート・カット攻撃はこれまでのところ発表されていない。

(ロ) ブルート・フォース攻撃

ブルート・フォース攻撃 (全数探索攻撃以外) においても、全数探索攻撃に必要な計算量との比較によって学術的に解読されたか否かが評価される。ブルート・フォース攻撃の適用結果を整理すると、表 3(2)のとおりである。

まず、トリプル DES については、2-key の場合も 3-key の場合も全数探索攻撃よりも少ない計算量 (それぞれ 2^{57} 、 2^{112}) で暗号鍵を推定する攻撃が提案されており (Merkle and Hellman [1981])、学術的には既に解読されている。本攻撃を実行するためには 2^{56} 個の平文・暗号文のペアを入手することが必要とされており、実用上問題となる可能性は小さいとみられているものの、(鍵を求

⁴ 差分解読法 (differential cryptanalysis) は、一定の条件を持つデータ組に対して暗号アルゴリズムの処理を行ったときの出力データの差分にある種の偏りが存在することを利用して暗号鍵を効率的に推定するという攻撃の総称である。

表 3(2) ブロック暗号におけるブルート・フォース攻撃に対する安全性

暗号 アルゴリズム	鍵長	ブロック長	ブルート・フォース攻撃の適用結果
2-key トリプル DES	112	64	【学術的に解読された】全数探索攻撃よりも少ない計算量 (2^{57}) によって暗号鍵を推定可能な攻撃が提案された。攻撃を実行するためには 2^{56} 個の平文・暗号文ペアを入手・記録しておく必要があるものの、 計算量については現実的に解読可能な域に達しつつある。 【注意点】暗号文一致攻撃を 2^{32} 個程度の暗号文を入手することで実行可能。
3-key トリプル DES	168	64	【学術的に解読された】全数探索攻撃よりも少ない計算量 (2^{112}) によって暗号鍵を推定可能な攻撃が提案された。ただし、 2^{56} 個の平文・暗号文ペアを入手・記録しておく必要がある。 【注意点】暗号文一致攻撃を 2^{32} 個程度の暗号文を入手することで実行可能。
RC2	可変 (SSL v.3.0/TLS v.1.0 では 40)	64	【注意点】全数探索攻撃よりも少ない計算量によって暗号鍵を推定する方法は発表されていないものの、暗号文一致攻撃を 2^{32} 個程度の暗号文を入手することで実行可能。 【安全】全数探索攻撃よりも少ない計算量で暗号鍵を推定可能な攻撃は提案されていないようである。
IDEA	128	64	
MISTY1	128	64	
AES	128, 192, 256	128	
Camellia	128, 192, 256	128	
SEED	128	128	

備考：本表は平成 17 年 11 月 7 日現在の情報を利用して作成した。

めるための計算量が 2^{57} と見積もられている 2-key トリプル DES に関しては、「現実的な意味でも解読可能な領域に達しつつある」(CRYPTREC 暗号技術評価報告書 2001 年度版 203 頁、IPA・TAO [2002]) との評価が下されている。また、トリプル DES は、ブロック長が 64 ビットと比較的短く、暗号文一致攻撃⁵に注意する必要があるが指摘されている。64 ビットのブロック暗号に暗号文一致攻撃を適用する際に必要となるメモリ・サイズは約 32 ギガ・バイトであり、実現困難な攻撃ではなくなりつつあるとの認識が高まっている。

64 ビットのブロック暗号である RC2、IDEA、MISTY1 については、全数探索攻撃よりも少ない計算量で実行可能なブルート・フォース攻撃は発表されていない。ただし、トリプル DES と同様に、暗号文一致攻撃に対して注意する

⁵ 暗号文一致攻撃 (ciphertext matching attack) は、同一の鍵によって生成された暗号文を大量に集め、それらの中から同一の暗号文となるものを探索し、その結果を用いて対応する平文や暗号鍵を推測するという攻撃である。この暗号文一致攻撃に対する安全性は、パースデー・パラドックスに基づいて評価することができる。例えば、64 ビット・ブロック暗号の場合、1 つの鍵で暗号化を行った 2^{32} 個の暗号文 (約 32 ギガ・バイト) をランダムに集めたとすれば、少なくとも 1 組は同じ値となる暗号文 (すなわち同じ平文) を高い確率で発見できることとなる。

必要がある。

一方、128 ビットのブロック暗号である AES と Camellia、SEED に関しては、こうした懸念は今のところない。128 ビットのブロック暗号に暗号文一致攻撃を適用するためには、同じ鍵で暗号化された暗号文を少なくとも 2^{64} 個集めてくる必要があり、約 2^{28} テラ・バイトのメモリを準備することが求められる。こうした莫大な量のメモリを調達することは困難と考えられるため、暗号文一致攻撃に対しても十分な安全性を有していると考えられることができる。

ロ．ストリーム暗号

ストリーム暗号は擬似乱数を生成して 1 ビットごとに平文との排他的論理和を計算して暗号文を生成するという暗号であり、その安全性は擬似乱数生成器に大きく依存する。仮に、擬似乱数生成器に欠陥があり、暗号鍵と出力される擬似乱数との間に強い相関があったり、過去の擬似乱数から将来生成される擬似乱数を予測可能であったりする場合、攻撃者が擬似乱数を入手できる状況では暗号鍵を容易に求めたり、暗号文を容易に解読できたりすることとなる。

これまでに提案されているストリーム暗号の中で最も広く利用されているとみられているのが RC4 である。RC4 は、SSL version 3.0/TLS version 1.0 における共通鍵暗号としても採用されており、インターネット・バンキングにおけるデータの暗号化を実現する暗号アルゴリズムとして金融機関が利用するケースも多いと考えられる。

RC4 の安全性評価結果をみると、鍵長を 128 ビットに設定するとともに、SSL version 3.0/TLS version 1.0 における標準的な仕様に沿ったパラメータ設定⁶を行う限り、学術的に解読を可能にするような攻撃は現時点では発表されていないようである。ただし、無線 LAN で利用されている暗号通信プロトコルである WEP (Wired Equivalent Privacy) における RC4 の利用形態では、初期状態からの攪拌が不十分であるため、出力される擬似乱数と暗号鍵との間に強い相関が生じる場合があり、これを利用して暗号鍵の推定に成功した例もある (Fluhrer, Mantin, and Shamir [2002])⁷。このため、SSL version 3.0/TLS version 1.0 における標準的なパラメータ設定以外での利用は CRYPTREC において推奨されていない (総務省・経済産業省 [2003])。

⁶ 本パラメータは内部状態を決定する値であり、例えば本パラメータを n とすると、内部状態の数は 2^n となる。標準的なパラメータ設定では、 $n=8$ と設定される。

⁷ このような攻撃に対する WEP の安全性に関連して、WEP が既に広く利用されていることから、WEP を一部修正して安全性を高めるといった対応についても検討されている。ただし、既存の対応では十分とはいえないのではないかとの見方もある (吉田・古原・今井[2005])。

(2)公開鍵暗号

公開鍵暗号として、ここでは RSA、DSA、DH、ECDSA を取り上げ、各暗号アルゴリズムの安全性評価結果を整理する⁸。

イ．RSA（素因数分解の困難性評価）

RSA の安全性は、大きな合成数の素因数分解が困難であることに依拠している。RSA の基本的なアルゴリズムを利用した暗号化や署名生成の手法にはさまざまなバリエーションがあり、守秘方式としては PKCS#1 version 1.5 や OAEP が挙げられるほか、署名方式としては PSS や ISO/IEC 9796 シリーズが挙げられる。これらの中には、OAEP や PSS のように、攻撃者の能力についてある想定を行い、そのもとで素因数分解の困難性と等価⁹であることを示すことによって安全性の証明を行う「証明可能安全性」を有しているものもある。ただし、いずれの方式においても、仮に素因数分解問題を効率的に解くアルゴリズムが提案された場合、あるいは、高速に素因数分解を行うハードウェアが実現した場合には、解読や署名偽造が可能となってしまうことになる。

どのくらい大きな合成数（RSA の鍵長に相当）を実際に素因数分解できるかについてさまざまな研究者が計算機実験を行っており、現時点で最速といわれている一般数体ふるい法と呼ばれるアルゴリズムによって 663 ビットの合成数の素因数分解が 2005 年 5 月に成功している。

1024 ビット合成数の素因数分解の可能性について計算量とコストの観点から検討した結果をみると、ムーアの法則¹⁰をベースとして過去の素因数分解の実績値から未来の素因数分解の可能性について検討した Brent [2000]においては、一般数体ふるい法と呼ばれるアルゴリズムを用いた場合、2018 年頃には 1024 ビットの合成数は現実的に素因数分解可能な領域に入ってくる可能性があるとの結果が示されている。Lenstra and Verheul [2001]においては、共通鍵暗

⁸ なお、量子コンピュータが登場すれば、素因数分解問題等が効率よく解けるようになる可能性があることが知られている。しかし、実際に数千ビットの公開鍵を素因数分解するためには、数万のキュビット (q-bit) を実現する量子コンピュータが必要となるとの見方もあり、20~30 年というタイム・スパンで実現される可能性は極めて低いと考えられている。このため、以下の議論では、量子コンピュータによる安全性への影響を考慮しないこととした。

⁹ 素因数分解問題が解けなければその暗号アルゴリズムが解けないこと、また仮に暗号アルゴリズムが解けるのであれば素因数分解問題が解けることを意味する。

¹⁰ ムーアの法則 (Moore's law) は、「半導体の集積密度は 18~24 ヶ月で倍増する」という法則であり、ゴードン・ムーア博士が提唱したものである。本法則は、半導体の性能やそれに伴う情報技術の発展を予測する際に用いられることが多く、情報セキュリティの文脈でも登場する機会が多い。

号として十分な安全性を有しているとみられていた 1982 年時点の DES と同じ強度を達成するためには、どの程度の鍵長であれば十分かという観点で検討が行われている。その結果、1024 ビットの RSA が (1982 年時点の) DES と安全性の面で等価と考えられるのは 2002 年頃であり、2001 年の時点で 20 年間の利用を前提とするのであれば、鍵長は 2048 ビットにすべきであるとしている。Kaliski [2003]は、十分な安全性を確保している公開鍵暗号として 1024 ビット RSA の利用を推奨できるのは 2010 年までであり、2030 年までの利用を想定する場合には 2048 ビット以上の RSA を推奨するとの見解を示している。

また、NESSIE の暗号アルゴリズム評価報告書 (Preneel *et al.* [2004]) においては、計算量による試算結果が報告されている。本報告書では、512 ビットの素因数分解に必要な計算量が 56 ビット鍵長の共通鍵暗号を全数探索攻撃によって解読する際の計算量と等価であるとの仮定のもとで、公開鍵暗号において今後中期的な安全性を確保するために必要な要件 (攻撃に必要な最小計算量のオーダーが 80 ビット) を満足できる合成数のサイズを 1536 ビットと見積もっており、1024 ビットでは不十分との試算結果と解釈することができる。

これらの試算結果に従うとすれば、2010 年の時点には、1024 ビット RSA を長期的に十分な安全性を有する公開鍵暗号として利用することは困難になるものと予想される。

素因数分解を実行する専用ハードウェアについても、その設計方法とハードウェア実現のためのコストに関する検討結果が発表されている。Franke *et al.* [2005]は、現時点で最速といわれている一般数体ふるい法において最も計算量を有する「ふるい」の処理 (関係式収集処理とも呼ばれる) を実行する専用ハードウェア SHARK を提案しており、1024 ビットの素因数分解におけるふるいの処理を約 2 億ドルのコストをかければ 1 年で実行可能であるとの検討結果を発表した。また、Geiselmann *et al.* [2005]は、1024 ビットの合成数を素因数分解する際の行列計算の処理を実行する専用ハードウェアの設計方針と実現可能性について試算し、約 200 万ドルの費用をかければ約 2.4 か月で実行可能であるとしている。こうした専用ハードウェアの実現可能性に関する研究結果も、1024 ビット RSA の安全性が徐々に低下している現状を示している。

□ . DSA と DH (離散対数問題の困難性評価)

DSA は証明可能安全性を有していないものの、擬似乱数生成器の欠陥等運用上の留意点を除けば、筆者が知る限り、暗号アルゴリズム自体に致命的な問題点は現時点で発表されていない。また、DH についても同様であり、本アルゴリズム自体の安全性に着目した場合には、筆者が知る限り、離散対数問題を解く以外の効率的な解法は提案されていない。

DSA と DH の安全性は、有限体の乗法群上の離散対数問題（以下、単に離散対数問題と呼ぶ）の困難性に依拠している。現時点で離散対数問題を最も高速に解くアルゴリズムは指数計算法(index calculus)であり、そのバリエーションとしてさまざまな手法が提案されている（例えば、Coppersmith [1984]、ElGamal [1985]、Pomerance [1985]、Gordon [1993]、Schirokauer [1993]、Adleman [1994]、Schirokauer, Weber and Denny [1996]）。本アルゴリズムによる計算機実験の最近の結果としては、法のサイズ（鍵長に相当）が 607 ビットの乗法群における離散対数問題を解くことに成功したとの結果が 2002 年に報告されている（Thomé [2002]）。

指数計算法のアルゴリズムは、素因数分解に用いられる一般数体ふるい法のアルゴリズムと密接に関係していることが知られている。指数計算法によって離散対数問題を解くために必要とされる計算量のオーダーは、鍵長を一定とすれば、素因数分解問題の高速解法である一般数体ふるい法と同程度になると評価されている（例えば、Preneel *et al.* [2004]）。そのため、素因数分解問題の困難性をベースとした暗号アルゴリズムの鍵長と離散対数問題の困難性をベースとする暗号アルゴリズムの鍵長は、一般に同程度に設定されることが多い。実際、DSA や DH においては、RSA と同じく 1024 ビットの鍵長が利用される場面が多いようである。上記イ . において説明したように、2010 年の時点からみると 1024 ビットの合成数の素因数分解が長期的に困難とは言い難い状況となっている可能性が高いことから、DSA や DH に採用されている法のサイズも 2010 年に向けて見直すことが求められているといえる。

八．ECDSA（楕円曲線離散対数問題の困難性評価）

ECDSA は、有限体上で定義される楕円曲線の有理点の集合における離散対数問題（以下、楕円曲線離散対数問題と呼ぶ）の困難性に基づく暗号方式であり、DSA を楕円曲線上で実現した方式である。ECDSA は、DSA と同様に証明可能安全性を有していないものの、筆者が知る限り、本方式の安全性に関して致命的となるような攻撃が提案されていない。このことから、現時点では ECDSA の安全性を評価する場合には、楕円曲線離散対数問題の困難性と実際に使用されている鍵長との関係に着目することとなる。

ECDSA における楕円曲線離散対数問題には、離散対数問題の高速解法である指数計算法が適用困難であることが知られている。また、金融用途向けの ECDSA を規定している ANS X9.62（ISO/TR 17944 も引用している）においては、特定の楕円曲線の使用を推奨しているわけではない。しかし、楕円曲線離散対数問題では、利用される楕円曲線の種類によって解法の最速アルゴリズムが異なってくるので、通常の離散対数問題よりも高速に解を求めることを可能

とする手法(例えば、Menezes, Okamoto and Vanstone [1993]、Frey and Rück [1994]、Sato and Araki [1998])が適用可能となるような、ある特殊なタイプの楕円曲線を選択しないようにすることが求められる。

このような注意を払ったうえで鍵長をどのように設定するかが問題となるが、ISO/TR 13569 において楕円曲線暗号の鍵長(有限体の位数のサイズ)を160ビット以上に設定する旨の規定が置かれていること等から、金融分野では160ビットが選択されることになるとみられる。

楕円曲線離散対数問題がどのくらいの計算機資源と時間によって実際に解くことができるかについては、サーティコム社が主催しているコンテストにおいて検証されている。これまでに、109ビットのサイズの位数をもつ有限体上での楕円曲線離散対数問題が解けたとの結果が報告されている。

160ビットのサイズの位数をもつ有限体上での楕円曲線離散対数問題に関しては、まず Lenstra and Verheul [2001]の試算によると、解読アルゴリズムの進歩(18か月で計算量が半減する)を想定した場合、2010年の時点において、160ビットというパラメータ設定によって1982年時点のDESと等価の安全性を実現できる(すなわち、長期的に十分な安全性を確保できる)としている。解読アルゴリズムの進歩を想定しない場合には、2020年の時点において、1982年時点のDESと等価の安全性を実現できるとしている。NESSIEにおける計算量をベースとした試算(Preneel *et al.* [2004])では、今後中期的な安全性を確保するために必要な鍵長のサイズを160ビットと見積もっており、現在採用されている鍵長と統合的な評価結果となっている。一方、Certicom Research [2000]の試算では、160ビットというパラメータ設定は、RSAやDSAにおける1024ビット鍵長、共通鍵暗号における80ビット鍵長と等価の安全性のレベルを意味すると評価されている。

Lenstra and Verheul [2001]の試算に従うとすれば、ECDSAにおいて160ビットというパラメータ設定を2011年以降も引き続き採用することについては特段の問題は発生しないように思われる。一方、Certicom Research [2000]の試算に従うとすれば、鍵長を224ビット以上に変更することが求められることになる。このように、鍵長の評価結果には幅が存在しており、どの試算に従うかは一概には決められない。ただし、安全性に万全を期するという観点からみると、最も厳しい評価を行っているCerticom Research [2000]を前提として検討することが妥当であると考えられる。

(3)ハッシュ関数

ハッシュ関数の中でも最も広く利用されているとみられるSHA-1は、安全性上問題があることを示唆する研究成果が発表されている。具体的には、2005年

2月、Wang, Yin and Yu [2005]によってSHA-1の衝突¹¹を 2^{69} 回程度のハッシュ関数演算と同程度の計算量によって探索可能であるとの試算結果が発表されたほか、最近では、 2^{63} 回程度のハッシュ関数演算と同程度の計算量によって探索可能であるとの見解も示された (Wang, Yao and Yao [2005])。

アルゴリズムに欠陥がないハッシュ関数の場合、衝突を高い確率で見つけるためには、誕生日攻撃法により、ハッシュ値のサイズを n ビットとすると $2^{(n/2)}$ 個のハッシュ値を集めてくる必要がある。このため、 $2^{(n/2)}$ 回のハッシュ関数演算よりも少ない計算量によって衝突を探索可能であることが判明した場合、安全性上問題があると評価されることとなる。SHA-1 の場合、ハッシュ値のサイズが 160 ビットであることから $2^{(n/2)} = 2^{80}$ であり、ワン (Wang) らが示した計算量の方が小さいことがわかる。

もっとも、衝突が発見されたとはいっても、意味があるようなメッセージにおいて衝突が見つかるケースは稀であり、実際の運用においては文意的に改竄を検出できる可能性が高い。つまり、直ちにそのハッシュ関数が実用的な意味で安全性上問題があるというわけではなく、文意的にも改竄を検知できないような意味のある現実的な攻撃を行うことは依然として困難であると考えられる。

ただ、深刻な事例を引き起こす可能性がないとはいえない。例えば、制御コードやパディング・データ、乱数列などメッセージに付加される情報の部分を意図的にコントロールすることが可能であるならば、文章そのものには関係していない、あるいは文意的には正当性が判断できないような異なる 2 つのメッセージ同士で衝突を起こさせるケースがありうる (Lucks and Daum [2005])。この場合には、文意的にも改竄を検知することは不可能となる。

つまり、衝突の可能性が深刻な事例になるかどうかはハッシュ関数の使い方に依存しており、一概には明確な判断を下すことが困難である。ただ、万全を期するのであれば、ハッシュ関数の汎用的な利用においては、一度でも衝突の可能性が指摘された場合、より安全なハッシュ関数へ移行することが妥当であると考えられる。

¹¹ 衝突 (collision) は、ハッシュ関数において同じ出力となる (異なる) 入力のパアのことを指す。本来ハッシュ関数はこうした衝突の探索が困難となるように設計されている。

4 . NIST と 2010 年問題

本節では、前節で紹介した各種暗号アルゴリズムの安全性評価結果を踏まえた現時点における NIST のスタンスについて説明したうえで、2010 年問題とその影響について説明する。

(1) 暗号アルゴリズム選定における NIST のスタンス

イ . FIPS と SP

米国では、コンピュータ・セキュリティ法 (Computer Security Act of 1987)、情報技術管理改革法 (Information Technology Management Reform Act of 1996)、連邦情報セキュリティ管理法 (Federal Information Security Management Act of 2002)、大統領令第 13011 号 (Executive Order #13011) 等によって、米国連邦政府内の情報セキュリティ対策に関する権限が NIST に付与されている。これによって、NIST は、暗号技術、セキュリティ製品、それらの評価方法、セキュリティ・マネジメントに関するガイドライン等を内容とする標準 FIPS¹²やガイドライン SP¹³を策定している (図 4(1)参照)。

暗号アルゴリズムに関しては、ブロック暗号、デジタル署名、ハッシュ関数を規定する FIPS や SP が策定されている。ブロック暗号としては、AES (FIPS 197)、2-key/3-key トリプル DES (SP 800-67)、Skipjack (FIPS 185) が認定されているほか、デジタル署名としては、RSA、DSA、ECDSA (FIPS 186-2)、ハッシュ関数としては、SHA シリーズ (SHA-1、SHA-224、SHA-256、SHA-384、SHA-512) (FIPS180-2) が認定されている。鍵配送については、DH と Menezes-Qu-Vanstone 方式 (以下 MQV と呼ぶ、SP 800-56) が認定されている。

2-key/3-key トリプル DES については、2005 年 5 月、トリプル DES を規定していた FIPS 46-3 が廃止され、SP 800-67 にのみ規定される扱いとなった。さら

¹² 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政府標準暗号と呼ばれる。

¹³ SP (Special Publications) 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こととなっている。ただし、FIPS の付随情報の場合には、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。

表 4(1) 暗号技術に関する主な FIPS と SP

種別	規格番号	タイトル	発行日
実装上の指針	SP 800-21	Guideline for Implementing Cryptography in the Federal Government	1999.11
鍵管理	SP 800-57	Recommendation on Key Management	2005.8
本人確認用の暗号アルゴリズムと鍵長	SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	2005.4
ブロック暗号とその利用モード	FIPS 197	Advanced Encryption Standard (AES)	2001.11
	SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	2004.5
	FIPS 185	Escrowed Encryption Standard (EES)	1994.2
	SP 800-38A	Recommendation for Block Cipher Modes of Operation – Methods and Techniques	2001.12
	SP 800-38B	Recommendation for Block Cipher Modes of Operation: Authentication Mode	2005.5
	SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality	2004.5
デジタル署名	FIPS 186-2	Digital Signature Standard (DSS)	2000.2
ハッシュ関数	FIPS 180-2	Secure Hash Standard (SHS)	2002.8
鍵配送	SP 800-56	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (draft)	2005.7
メッセージ認証	FIPS 113	Computer Data Authentication	1985.5
	FIPS 198	The Keyed-Hash Message Authentication Code (HMAC)	2002.3
エンティティ認証	FIPS 196	Entity Authentication Using Public Key Cryptography	1997.2
パスワード利用・生成	FIPS 181	Automated Password Generator	1993.10

に、本 SP の中で、2-key トリプル DES は 2010 年まで使用が可能であり、それ以降は使用しない扱いとする予定である旨が記述されている。

ロ．暗号アルゴリズム・鍵長の移行見通し

NIST は、FIPS や SP において現在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を今後どのように移行するかの見通しに関する情報もガイドライン (SP 800-57 と SP 800-78) の中に記述している。

(イ) SP 800-57

SP 800-57 は、連邦政府内の情報システムにおいて利用される暗号アルゴリズムの鍵管理に関するガイドラインである。本 SP は、暗号アルゴリズムの実装に必要な各種暗号鍵の種類やその利用方法、必要とされる鍵長等を詳細に記述している (表 4(2)参照)。表 4(2)にあるように、推奨する暗号アルゴリズムと鍵長が、2010 年末までを使用期間とする場合、2030 年末までを使用期間とする場合、2031 年以降も使用する場合に分けて記述されている。

表 4(2) SP 800-57 に記述されている暗号アルゴリズムの移行見通し

使用期間	共通鍵暗号	素因数分解問題ベースの公開鍵暗号	離散対数問題ベースの公開鍵暗号	楕円曲線離散対数問題ベースの公開鍵暗号
2010 年末まで	・ 2-key トリプル DES ・ 3-key トリプル DES ・ AES (鍵長 128、192、256 ビット)	最小鍵長を 1024 ビットとする。	最小鍵長を 1024 ビットとする (ただし、有限体における部分群の位数 q のサイズは 160 ビットとする)。	最小鍵長を 160 ビットとする。
2030 年末まで	・ 3-key トリプル DEA ・ AES (鍵長 128、192、256 ビット)	最小鍵長を 2048 ビットとする。	最小鍵長を 2048 ビットとする (ただし、 q のサイズは 224 ビットとする)。	最小鍵長を 224 ビットとする。
2031 年以降	AES (鍵長 128、192、256 ビット)	最小鍵長を 3072 ビットとする。	最小鍵長を 3072 ビットとする (ただし、 q のサイズは 256 ビットとする)。	最小鍵長を 256 ビットとする。

備考：NIST [2005a] の Table 4 をベースに作成。

2010 年末までを使用期間とする場合においては、推奨される共通鍵暗号に 2-key トリプル DES が含まれているものの、2030 年末まで使用期間を拡張すると 2-key トリプル DES は推奨されなくなる扱いとなっている。また、公開鍵暗号の場合、素因数分解問題ベースのものと離散対数問題ベースのものについて、2011 年以降も使用することを想定すると 2048 ビット鍵長が推奨されることとなっている。楕円曲線離散対数問題ベースの公開鍵暗号については、2011 年以降の使用を想定した場合には 224 ビット鍵長のものが推奨されている。

このように、現時点で金融分野において広く利用されているとみられる 2-key トリプル DES、1024 ビット RSA、1024 ビット鍵長の DSA については、NIST は、2011 年以降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示している。

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。

(口) SP 800-78

SP 800-78 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本人確認を行うシステム (PIV<personal identity verification>システム) で使用される暗号アルゴリズムおよび鍵長を記述するものである。PIV システムの概要については FIPS 201 (Personal Identity Verification for Federal Employees and Contractors、NIST [2005c]) 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 カードと呼ばれる) を配布し、その PIV カードや PIN 等によって PKI を活用して本人確認を行うシステムの構成が記述されてい

表 4(3) SP 800-78 に記述されている暗号アルゴリズムの移行見通し

暗号鍵の種類	使用期間	推奨する暗号アルゴリズムと鍵長	
個人識別用の鍵 (公開鍵暗号)	2010 年 末 まで	<ul style="list-style-type: none"> ・ RSA (鍵長: 1024、2048、3072 ビットのいずれか) ・ ECDSA (鍵長: 224 ビットから 283 ビットまで) 	
	2011 年 以降	<ul style="list-style-type: none"> ・ RSA (鍵長: 2048 ビットまたは 3072 ビット) ・ ECDSA (鍵長: 224 ビットから 283 ビットまで) 	
PIV カード認証用の鍵 (共通鍵暗号 または公開鍵暗号)	2010 年未 まで	共通鍵暗号の 場合	<ul style="list-style-type: none"> ・ 2-key トリプル DES ・ 3-key トリプル DES ・ AES (鍵長: 128、192、256 ビットのいずれか)
		公開鍵暗号の 場合	<ul style="list-style-type: none"> ・ RSA (鍵長: 1024、2048、3072 ビットのいずれか) ・ ECDSA (鍵長: 224 ビットから 283 ビットまで)
	2011 年 以降	共通鍵暗号の 場合	<ul style="list-style-type: none"> ・ 3-key トリプル DES ・ AES (鍵長: 128、192、256 ビットのいずれか)
		公開鍵暗号の 場合	<ul style="list-style-type: none"> ・ RSA (鍵長: 2048、3072 ビットのいずれか) ・ ECDSA (鍵長: 224 ビットから 283 ビットまで)
デジタル署名 生成用の鍵	2008 年未 まで	<ul style="list-style-type: none"> ・ RSA (鍵長: 1024、2048、3072 ビットのいずれか) ・ ECDSA (鍵長: 224 ビットから 283 ビットまで) 	
	2009 年 以降	<ul style="list-style-type: none"> ・ RSA (鍵長: 2048、3072 ビットのいずれか) ・ ECDSA (鍵長: 224 ビットから 283 ビットまで) 	
鍵配送用の鍵 (公開鍵暗号)	2008 年未 まで	<ul style="list-style-type: none"> ・ RSA (鍵長: 1024、2048、3072 ビットのいずれか) ・ ECDH もしくは ECC MQV (鍵長: 224 ビットから 283 ビットまで) 	
	2009 年 以降	<ul style="list-style-type: none"> ・ RSA (鍵長: 2048、3072 ビットのいずれか) ・ ECDH もしくは ECC MQV (鍵長: 224 ビットから 283 ビットまで) 	

備考: NIST [2005b] の Table 3-1 をベースに作成。

る。SP 800-78 はこうした FIPS 201 を暗号アルゴリズムの観点で補完する内容となっており、FIPS 201 の付随情報として事実上の強制規定として取り扱われるものとみられる。

SP 800-78 には、PIV カードに格納される 4 種類の鍵、個人識別用の鍵 (必須)、PIV カード認証用の鍵 (オプション)、デジタル署名生成用の鍵 (オプション)、鍵配送用の鍵 (オプション) について記述されている。個人識別用の鍵は当該 PIV カードの所有者である個人の秘密鍵であり、PIV カード認証用の鍵は当該カードに対して生成される秘密鍵 (公開鍵暗号ベースの場合と共通鍵暗号ベースの場合が想定されている) である。デジタル署名生成の鍵は、個人識別用の鍵によって生成されるデジタル署名の対象データとは別に、他のデータに対してデジタル署名を別の鍵で生成する必要がある場合に準備されるものである。

これらの暗号鍵に利用される暗号アルゴリズムと鍵長は表 4(3) のとおりである。共通鍵暗号については AES もしくはトリプル DES が推奨されているほか、公開鍵暗号については RSA もしくは ECDSA (その他の楕円曲線暗号) が推奨されている。

PIV カードに搭載されることが必須となっている個人識別用の鍵に着目すると、2010 年末までの使用であれば 1024 ビット RSA が認められているが、

それ以降の使用が想定される場合にはRSAの鍵長を2048ビット以上に設定することが推奨されている。また、共通鍵暗号については、規定されているPIVカード認証用の鍵として2-keyトリプルDESの使用が推奨されているのは2010年末までとなっている。このほか、ICカードでの実装が想定されていることから、署名生成用のアルゴリズムとしてRSAのほかに楕円曲線暗号であるECDSAが含まれている。ECDSAの鍵長については、2011年以降には224ビット以上に設定することが推奨されている。

ハッシュ関数についても、SP 800-78では、2010年末まではSHA-1、SHA-224、SHA-256のいずれかの使用が推奨されており、それ以降についてはSHA-224またはSHA-256の使用が推奨されている。

八．SHA-1に対する見方

NISTは、SHA-1の前身であるSHA-0における衝突が発見された直後に、SHA-1の今後の取扱いに関するコメントを発表している(NIST[2004])。NIST[2004]には、「SHA-0への攻撃に関する発表自体はSHA-1の安全性に影響を与えるものではない。しかし、暗号解読技術が今後進展していくことが予想されることから、2010年までに、SHA-1の使用をとりやめて、よりハッシュ値のサイズが大きなもの(SHA-224、SHA-256、SHA-384、SHA-512)に移行することを検討している」旨が記述されている。さらに、その後、実際にSHA-1に対する攻撃法が提案された際には、「新たに作られるシステムではよりハッシュ値のサイズが大きなもの、すなわち、SHA-224、SHA-256、SHA-384、SHA-512(以下、これらをまとめてSHA-2と呼ぶ)を使用する、またシステムの重要性を考慮した移行計画を策定する」旨のより踏み込んだ内容のコメントを発表している(NIST[2005d])。

こうした発表と、上記口(口)において説明したSP 800-78におけるハッシュ関数の使用に関する記述は整合しており、実際にSHA-1の利用は2010年までに限定される方向性が濃厚になっているといえる。

(2) ISO/TC68における過去の対応：DESおよびトリプルDESの場合

3節と4節(1)において紹介したように、現在金融分野において幅広く利用されているとみられる暗号アルゴリズムは、今後長期的に十分な安全性を確保することが難しくなってきたとの評価が大勢であるといえる。また、こうした評価結果を受けて、NISTは2010年を目処に米国連邦政府機関における暗号アルゴリズムの移行を計画している。NISTのこうした動きは、既存の暗号アルゴリズムに対する安全性の「お墨付き」を廃することを意味しており、現在使用されている暗号アルゴリズムの安全性に対するレピュテーションを著しく低下

させることにつながる。

従来、金融分野においては、NISTによって十分安全と評価された暗号アルゴリズムを国際標準等に採用してきた経緯があり、2010年問題と類似の状況が過去に2度生じている。

1度目は、1977年に、NISTの前身であったNBS(National Bureau of Standards)がDESをFIPS 46に採用することを決定した際のことである。FIPS 46が発行された後、ISO/TC68もDESをベースとした情報セキュリティ技術の国際標準の審議を開始し、関連する標準が相次いで策定された。こうしたISO/TC68における国際標準の審議においてDESを採用することに踏み切った背景として、NISTがDESをFIPSに認定したという事実が有力な材料になったとみられている(谷口・太田・大久保 [1999])。

2度目は、NISTが、DESからAESへの「つなぎ」として、1999年にDESを廃してトリプルDESをFIPS 46-3として認定した際のことである。ISO/TC68では、FIPS 46としてDESが認定された後もDESの安全性低下を裏付ける研究成果について適宜フォローし、1997年には日本からDESの安全性評価に関する論文(Kusuda and Matsumoto [1997])を技術的な貢献として提出した経緯がある。1999年にNISTがFIPS 46-3を発行してDESからトリプルDESへの移行を決定した際には、ISO/TC68は、国際標準へのトリプルDESの採用について遅滞なく検討を開始した。この間の経緯をやや詳しく説明すると、トリプルDESに関する金融分野における標準としては、1998年に策定された米国国内標準ANS X 9.52が既に存在しており、NISTはANS X 9.52を参照するかたちでトリプルDESを規定するFIPS 46-3を発行した。これを受けて、ISO/TC68は、ANS X 9.52を国際標準にするための審議を開始し、金融業務において利用される暗号アルゴリズムの標準化を担当するISO/TC68/SC2/WG11における審議を経て、2004年にISO/TR 19038として標準化を完了している。さらに、ISO/TC68では、従来DESを規定していた各種標準を、すべてトリプルDESを規定するよう見直しが行われてきた。

このように、ISO/TC68におけるDES、トリプルDESの標準化は、NISTにおける暗号アルゴリズムのFIPS認定と整合性を保ちつつ進められてきたといえる。

(3) 2010年問題への対応とその影響

2010年問題は、NISTによる暗号アルゴリズムの安全性に関する「お墨付き」が2010年頃に喪失してしまうことに伴って発生する問題である。金融分野における国際標準の過去の経緯をみると、NISTによる暗号アルゴリズムの評価結果に信頼を置き、NISTの方針と歩調を合わせるかたちで暗号アルゴリズムの移行が行われてきたといえる。したがって、今回の2010年問題においても、各金融

機関あるいは ISO/TC68 等の標準化団体は、NIST の方針に沿って暗号アルゴリズムの移行を進めることが妥当であると考えられる¹⁴。

こうした対応は、ISO/TC68 の国際標準における安全性の観点からのレピュテーションを引き続き維持するという意味でも重要であるといえる。仮に、2010 年のタイミングで FIPS 認定を得ている、あるいは SP において使用が推奨されている暗号アルゴリズムに移行することができなかった場合であっても、当該情報システムにおける安全性のレベルが急激に低下するということはないと考えられる。しかし、こうした外部状況の変化を考慮せずに、NIST の「お墨付き」を得ていない暗号アルゴリズムを引き続き使用しているとすれば、当該情報システムにおける安全性に関するレピュテーションの低下を免れることはできないと思われる。また、より厳しい見方をすれば、「現時点（2005 年）において既に NIST の暗号アルゴリズムの移行スケジュールが明らかになっていたにもかかわらず、それに対応すべく迅速に検討を行うことができなかった」という意味で、当該金融機関は、情報セキュリティ対策に関する意識レベルが低いという観点からのレピュテーションへの悪影響も想定される。

2010 年問題への対応は、現在主流とみられるすべての暗号アルゴリズムが対象となることから、金融分野における暗号アルゴリズム利用の裾野が相対的に広いという点で、今までの DES やトリプル DES における単一の暗号アルゴリズム移行の場合とは状況が異なっている。しかも、暗号アルゴリズムを利用している金融機関の数が増えているだけでなく、金融機関間のネットワーク、IC キャッシュカード、インターネット・バンキング等、暗号アルゴリズムが利用されている金融サービスの種類も拡大している。こうした各種の情報システムにおいて、暗号アルゴリズムの移行を適切かつ迅速に進めていくことが求められる。したがって、必然的に金融機関における検討項目が相対的に多くなっているとみられ、移行の検討を開始してから移行完了にいたるまでに必要となる時間は多くなると考えられる。2010 年問題の対応については、なるべく早い時期に着手する必要があるといえる。

こうした点も踏まえたうえで、2010 年問題への対応の重要性を認識し、どのように 2010 年問題に対応するかについて検討を開始することが求められている。

¹⁴ NIST による暗号アルゴリズムの評価結果は NESSIE や CRYPTREC による評価においても重視されている。具体的には、NESSIE における AES の評価においては NIST が詳細な評価を実施していることを第 1 に指摘しているほか、2005 年 11 月 8 日時点で公表されている CRYPTREC による電子政府推奨暗号リスト（総務省・経済産業省 [2003]）においては、3-key トリプル DES を電子政府推奨暗号リストに記載する条件として、3-key トリプル DES が FIPS 46-3 として維持されていることが記述されている。

5. 2010年問題等への対応のあり方

2010年問題の対応を考える際には、どのような暗号アルゴリズムに移行させるかを検討するとともに、どのような手続で移行させるかについて検討する必要がある。これらの検討の内容は個々のアプリケーションに依存することとなるが、以下では実際に検討を行う際の留意点等を整理する。

(1) 各種機関・プロジェクトによって規定/認定/推奨されている暗号アルゴリズム

2011年以降使用する暗号アルゴリズムとしてどのようなものを選択するかについて、NISTが認定あるいは推奨しているものを採用するという選択肢が考えられる。また、現時点ではDESやトリプルDESを採用した場合とは異なり、暗号研究者らによるNIST以外の第三者的な組織が暗号アルゴリズムを評価した結果をもとに推奨暗号を選定しており、アプリケーションとの相性といった観点から、それらの評価結果を重視して最終的に暗号アルゴリズムを決定することもできる。具体的には、CRYPTRECによる電子政府推奨暗号リストやNESSIE推奨暗号などが挙げられる。

ISOは、汎業界における情報セキュリティ技術の標準化を担当するISO/IEC JTC1/SC27において、守秘目的の暗号アルゴリズムの国際標準ISO/IEC 18033シリーズを策定している。本標準は、NIST、CRYPTREC、NESSIEにおける評価結果を参照するかたちで審議され、これらによって推奨されている暗号アルゴリズムを含んでいる。

イ. NISTの方針

NISTは、SP 800-57に示しているように、2030年までの使用を想定した場合に次のアルゴリズムと鍵長を推奨している(表4(2)参照)。ハッシュ関数については、NIST [2004]を参照する。

- 共通鍵暗号：AES、もしくは、3-keyトリプルDESとする。
- 素因数分解問題ベースの公開鍵暗号：最小鍵長を2048ビットとする。
- 離散対数問題ベースの公開鍵暗号：最小鍵長を2048ビットとする。ただし、有限体における部分群の位数 q のサイズを224ビットとする。
- 楕円曲線離散対数問題ベースの公開鍵暗号：最小鍵長を224ビットとする。
- ハッシュ関数：SHA-2のいずれかとする。

表 5(1) ISO/IEC 18033 に規定されている暗号アルゴリズム

分類		暗号アルゴリズム
公開鍵暗号 (パート2)		<ul style="list-style-type: none"> ・素因数分解問題ベース：RSA-KEM、RSA-OAEP、HIME(R) ・離散対数問題ベース：ACE-KEM ・楕円曲線離散対数問題ベース：PSEC-KEM、ECIES-KEM
共通鍵 暗号	ブロック暗号 (パート3)	<ul style="list-style-type: none"> ・64ビット・ブロック暗号：CAST-128、MISTY1、トリプル DES ・128ビット・ブロック暗号：AES、Camellia、SEED
	ストリーム暗号 (パート4)	<ul style="list-style-type: none"> ・MUGI ・SNOW 2.0

公開鍵暗号の暗号アルゴリズムとしては、FIPS 186-2 (デジタル署名方式) に認定されているものを挙げると、素因数分解問題ベースでは RSA (ANS X 9.31 を引用)、離散対数問題ベースでは DSA、楕円曲線離散対数問題ベースでは ECDSA となっている。また、鍵配送方式については、離散対数問題および楕円曲線離散対数問題をベースとする鍵配送方式を推奨する SP 800-56 の中で、DH、MQV、これらをそれぞれ楕円曲線上で実行する方式が推奨されている (NIST [2005d])。鍵長については、上記 SP の離散対数問題ベースの公開鍵暗号、楕円曲線離散対数問題ベースの公開鍵暗号に準拠するものとみられる。

ロ . ISO/IEC 18033 シリーズ

ISO/IEC 18033 シリーズは、汎業界における守秘目的の暗号アルゴリズムとして初めての国際標準であり、2000 年 4 月から標準化の審議が開始された。本国際標準のパート 2 は公開鍵暗号、パート 3 はブロック暗号、パート 4 はストリーム暗号を規定するという構成となっている (ISO/IEC [2005a, b, c])。ISO/IEC 18033 シリーズに規定される暗号アルゴリズムは、ISO/IEC JTC1/SC27 傘下で審議されている他の国際標準にも利用されることとなっており、幅広い分野に普及することが予想される。

本国際標準の審議を担当する ISO/IEC JTC1/SC27 は、各国から候補アルゴリズムの提案を募るのに際し、公的な機関等による客観的な安全性評価・性能評価が実施されていることを必要条件として挙げていた。その結果、NIST による FIPS 認定を受けた暗号アルゴリズム、CRYPTREC や NESSIE において推奨された暗号アルゴリズム等が提案され、安全性や実装性能の観点から総合的に審議が行われた。最終的には、各パートにおいて複数の暗号アルゴリズムが規定されることとなった。

ISO/IEC 18033 シリーズに規定されている暗号アルゴリズムは表 5(1)のとおりである。公開鍵暗号については、素因数分解問題ベース、離散対数問題ベ-

ス、楕円曲線離散対数問題ベースの暗号アルゴリズムがそれぞれ規定されており、いずれも証明可能安全性を有している。ただし、鍵長については規定されておらず、ユーザ自らが適切な鍵長の選択を行う必要がある。

共通鍵暗号のうち、ブロック暗号については、64 ビット・ブロック暗号と128 ビット・ブロック暗号の2種類に分けて規定されている。64 ビット・ブロック暗号としては、CAST-128、MISTY1、トリプル DES の3つが規定されている。特に、トリプル DES については、2-key と3-key の2つのオプションがある旨が記述されているものの、3-key の方が推奨されているほか、2-key トリプル DES については2009年頃までしかNISTによって推奨されない予定であるとの説明が記述されている。こうしたことから、ISO/IEC 18033-3 は、トリプル DES を採用するならば3-key トリプル DES の利用を促していると考えられることができる。128 ビット・ブロック暗号については、AES、Camellia、SEED が規定されており、鍵長は128 ビット以上に設定することが規定されている。

ストリーム暗号については、MUGI、SNOW 2.0 が規定されており¹⁵、現在広く使われているRC4は規定されていない。

ロ．CRYPTREC による電子政府推奨暗号リスト

CRYPTREC は、2003年度までに基盤整備が予定されていた電子政府で利用可能な暗号アルゴリズムのリスト(電子政府推奨暗号リスト)を作成することを最終的な目的として、その候補となる暗号アルゴリズムの評価を主として実施するために2000年5月に発足した¹⁶。CRYPTREC においては、電子政府システムで必要とされる暗号アルゴリズムを公募したうえで、応募された暗号アルゴリズムに関して国内外の主要な暗号研究者に依頼した安全性評価報告と国内外での学会発表論文をベースに評価を行い、実際に調達可能な暗号アルゴリズムであることに加え、電子政府での利用に安全性の観点から特に問題がないと認められるものを電子政府推奨暗号リストとして2003年2月に公表した(表5(2)参照、総務省・経済産業省 [2003])。

2003年度からは、CRYPTREC は、電子政府推奨暗号リストに掲載された暗号アルゴリズムに安全性上の問題が生じていないかどうかを監視するための暗号技術監視委員会と暗号技術調査ワーキンググループ、安全な暗号モジュールを実現・評価するための調査研究を行う暗号モジュール委員会に改組され、現在も活動を継続している。

¹⁵ ISO/IEC 18033-4 における「ストリーム暗号の一般モデル」には、ストリーム暗号の出力関数として、鍵ストリームと平文の XOR を計算する手法と、MULTI-S01 を利用する手法の2つが規定されている。

¹⁶ CRYPTREC の最近の活動に関する情報は <http://www.cryptrec.jp> を参照されたい。

表 5(2) 電子政府推奨暗号リスト (総務省・経済産業省[2003])

分類		暗号アルゴリズム名
公開鍵暗号	署名	DSA、ECDSA、RSASSA-PKCS1-v1_5 (RSA 署名)、RSA-PSS
	守秘	RSA-OAEP、RSAES-PKCS1-v1_5 (RSA 暗号) ^(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 トリプル 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 ビット 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)	<ul style="list-style-type: none"> ・ 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) Appendix3.1 ・ PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix3.1

備考：

- (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-DEM 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 トリプル DES は、以下の条件を考慮し、当面の使用を認める。
 - 1) FIPS 46-3 として規定されていること。
 - 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 ビット 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。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。

CRYPTREC における電子政府推奨暗号の選定においては、応募された暗号アルゴリズム、および、幅広い分野で利用されている(いわゆるデファクトの)暗号アルゴリズムを対象として、電子政府システムにおける利用に適した十分な安全性を有しているか否かを評価し、一定の基準に合格したものをリストに掲載した。CRYPTREC の評価においては、安全性が主たる評価項目となっている点が特徴である。

暗号技術評価報告書 2002 年度版 (IPA・TAO [2003]) の公開鍵暗号における推奨鍵長をみると、2002 年の時点において、RSA の場合には 1024 ビット以上、DSA および DH の場合には 1024 ビット以上、ECDSA の場合には 160 ビット以上となっている。また、RSA の場合、署名方式としては PKCS #1 version 2.1 に記載されている RSAES-PKCS1-v1_5 と RSA-PSS、守秘方式としては PKCS #1 version 2.1 に記載されている RSASSA-PKCS1-v1_5 と RSA-OAEP が記載されて

いる。これらの方式の優劣について暗号技術評価報告書 2002 年度版には明示されていない。一般には、RSA-PSS と RSA-OAEP が証明可能安全性を有しているという点で安全性上相対的に望ましいとみられている。なお、PSEC-KEM においては、「KEM¹⁷-DEM¹⁸構成における利用を前提とする」との但し書がある。

共通鍵暗号においては、2005 年 11 月 8 日時点で公表されている電子政府推奨暗号リストに、但し書として「より長いブロック長の暗号を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」と記載されている。また、64 ビット・ブロック暗号についてみると、2-key トリプル DES が含まれていないほか、3-key トリプル DES に関しては、「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」を考慮して使用を認めるとの但し書が付いている。3-key トリプル DES は、現時点で既に FIPS 46-3 として認定されていないことから、他の 64 ビット・ブロック暗号に比べて安全性の面でやや見劣りする状況となっている。また、鍵長 128 ビットの RC4 も推奨されているものの、「SSL version 3.0/TLS version 1.0 以上に限定して利用することを想定している。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。」との但し書が付いている。

ハッシュ関数については、SHA-1 が含まれているものの、「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」との但し書が付いている。このことから、SHA-256、SHA-384、SHA-512 が相対的に望ましいハッシュ関数として推奨されているといえる。

¹⁷ KEM(key encapsulation mechanism)は、守秘目的の公開鍵暗号方式の 1 利用形態であり、共通鍵暗号方式で用いられるセッション鍵の配送に特化した暗号アルゴリズムを実現する。KEM における暗号化処理では、通信相手の公開鍵と一定のパラメータが暗号化関数に入力され、通信相手との間で共有される暗号鍵 K (セッション鍵に相当)と、 K を得るためのデータ C が出力される。通信相手に対してはデータ C が送信され、 K は当該エンティティが秘密に保管する。復号処理では、受信者の秘密鍵とデータ C が復号関数に入力され、暗号鍵 K が出力される仕組みとなっており、暗号鍵 K が通信者間で共有されることとなる。なお、受信者が正しい暗号鍵 K を得られなかった場合、データ C は自動的に破棄される。

¹⁸ DEM (data encapsulation mechanism) は、共通鍵暗号の 1 利用形態であり、共通鍵暗号をベースとして、メッセージの守秘性と一貫性の両方を確保するための手法である。DEM は、採用される共通鍵暗号方式が一定の安全性を満足すると仮定した場合、DEM の安全性が証明可能になるという性質を有している。ISO/IEC 18033-2 においては、KEM を実現する公開鍵暗号において DEM を組み合わせる手法 (KEM-DEM 構成) が規定されており、その場合には KEM-DEM 構成による暗号全体の安全性も証明可能であることが知られている。

表 5(3) NESSIE 推奨暗号

分類		暗号アルゴリズム名
公開鍵 暗号	署名	RSA-PSS (第1推奨) ^(注1) 、ECDSA (第2推奨) ^(注2) 、 SFLASH (特定用途)
	守秘	PSEC-KEM (第1推奨) ^(注2) 、RSA-KEM (第2推奨) ^(注1) 、 ACE-KEM (特定用途) ^(注3)
	認証	GPS
共通鍵 暗号	64 ビット・ブロック暗号	MISTY1
	128 ビット・ブロック暗号	AES、Camellia
	256 ビット・ブロック暗号	SHACAL-2
その他	ハッシュ関数	Whirlpool ^(注4) 、SHA-256、SHA-384、SHA-512
	メッセージ認証子	UMAC、TTMAC、EMAC、HMAC

備考：

- (注1) 中期的(5~10年)な安全性を確保する目的で、鍵長は1536ビット以上を推奨。
- (注2) 中期的な安全性を確保する目的で、鍵長は160ビット以上を推奨。
- (注3) 中期的な安全性を確保する目的で、楕円曲線を利用する場合には鍵長は160ビット以上を推奨するほか、有限体を利用する場合には鍵長は1536ビット以上を推奨。
- (注4) Whirlpool のハッシュ値のサイズは512ビットである。
- (出典) NESSIE consortium [2003] (2003年2月27日付) をベースとして作成した。

二 . NESSIE 推奨暗号

欧州連合では、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 を2000年にスタートさせた。その目的は、欧州企業の国際競争力の強化や研究開発力の維持に有用な NESSIE 推奨暗号 (NESSIE ポートフォリオとも呼ばれる) を選定し、さまざまな標準化団体等によって採用してもらうことで標準化への合意形成を図ることであった。NESSIE における評価活動は、欧州の大学に所属している暗号研究者およびセキュリティ関連企業が中心となって実施され、安全性、実装性能、知的財産権の取扱い等が総合的に判断され、表 5(3)に示す暗号アルゴリズムが最終的に選定された (NESSIE consortium [2003])。NESSIE 自体は、2003年3月の最終報告書の取りまとめをもって終了し、ここでの成果は、NESSIE 推奨暗号として、ISO/IEC や IETF 等における標準化活動に提供された。

NESSIE 推奨暗号における公開鍵暗号は、署名方式では RSA-PSS (第1推奨、primary recommendation)、ECDSA (第2推奨、secondary recommendation) となっており、守秘方式では PSEC-KEM (第1推奨)、RSA-KEM (第2推奨) となっている。鍵長については、いずれも中期的(5~10年)に十分な安全性を確保できるとみられるレベルが設定されており、RSA 系の暗号アルゴリズムについては1536ビット以上が推奨されている。また、楕円曲線暗号系の ECDSA と PSEC-KEM においては、160ビット以上が推奨されている。2010年問題に対応するためには、NESSIE における評価において想定されている中期よりも長い期間の安全性が要求されることになると考えられる。したがって、NESSIE

の評価結果に従うとすれば、RSA 系については 1536 ビットを超えるサイズの鍵長に設定する必要があるほか、楕円曲線暗号系については 160 ビットを超える鍵長を選択することが求められると考えられる。

共通鍵暗号に関しては、64 ビット・ブロック暗号として MISTY1(三菱電機)が推奨されているほか、128 ビット・ブロック暗号としては AES と Camellia (NTT・三菱電機)が推奨されている。なお、RC4 をはじめとするストリーム暗号については NESSIE による推奨暗号に含まれていない。

ハッシュ関数については、4 つのハッシュ関数のいずれもハッシュ値のサイズが 256 ビット以上となっている。この点に関しては、CRYPTREC の電子政府推奨暗号リストのハッシュ関数に関する評価と整合的となっている。

ホ．規定 / 認定 / 推奨されている暗号アルゴリズムの比較

NIST、ISO/IEC 18033 シリーズ、CRYPTREC、NESSIE における暗号アルゴリズムの選択について取り上げたが、その概要を一覧表にまとめると表 5(4)のとおりである。

これらを横並びにみて比較を行う。まず、公開鍵暗号のうちデジタル署名については、NIST、CRYPTREC、NESSIE のいずれからも認定あるいは推奨されている暗号アルゴリズムは ECDSA のみとなっている。ただし、ECDSA の鍵長については、224 ビット以上を推奨する NIST を除いて 160 ビット以上が推奨されている。また、2 つの機関・プロジェクトから推奨されているものとしては、RSASA-PKCS1-v1_5、RSA-PSS、DSA が存在するが、鍵長はそれぞれ異なっている。

守秘目的の方式については、ISO/IEC 18033-2 においては、RSA-KEM をはじめとする 6 種類の暗号アルゴリズムが規定されており、このうち RSA-OAEP は CRYPTREC の電子政府推奨暗号リストにも含まれているほか、PSEC-KEM、RSA-KEM、ACE-KEM は NESSIE 推奨暗号にも含まれている。CRYPTREC と NESSIE の評価結果を比較すると、両方から共通して推奨されている暗号アルゴリズムは存在しないほか、NESSIE 推奨暗号ではいずれの暗号アルゴリズムも鍵配送を目的とした KEM を備えたものが推奨されている。RSA に関しては、推奨される鍵長も異なっている。

鍵配送目的の方式については、NESSIE 推奨暗号において守秘目的の方式として分類されている PSEC-KEM を鍵配送目的の方式とみなすと、NESSIE 推奨暗号と CRYPTREC の電子政府推奨暗号リストに共通して含まれている暗号アルゴリズムとして PSEC-KEM が挙げられる。PSEC-KEM における鍵長も 160 ビットで共通している。また、DH も、NIST と CRYPTREC から推奨されている。

表 5(4) 国際標準等に規定 / 認定 / 推奨されている暗号アルゴリズム

		NIST の FIPS・SP < 2030 年末までの使用を想定 >	CRYPTREC 電子政府推奨暗号リスト < 電子政府向けに調達可能な暗号アルゴリズムの中から選定 >	NESSIE 推奨暗号 < 中期的な安全性を想定 >	ISO/IEC 18033 シリーズ
公開鍵暗号	署名	<ul style="list-style-type: none"> • RSA (2048 bits) • DSA (2048 bits) • ECDSA (224 bits) 	<ul style="list-style-type: none"> • DSA (1024 bits) • ECDSA (160 bits) • RSASA-PKCS1-v1_5 (1024 bits) • RSA-PSS (1024 bits) 	<ul style="list-style-type: none"> • RSA-PSS (1536 bits) • ECDSA (160 bits) • SFLASH 	(ISO/IEC 9796-2 と 14888-3 において規定)
	守秘	(推奨なし)	<ul style="list-style-type: none"> • RSA-OAEP (1024 bits) • RSAES-PKCS1-v1_5 (1024 bits) 	<ul style="list-style-type: none"> • PSEC-KEM (160 bits) • RSA-KEM (1536 bits) • ACE-KEM 	<ul style="list-style-type: none"> • RSA-KEM • RSA-OAEP • HIME(R) • ACE-KEM • PSEC-KEM • ECIES-KEM
	鍵配送	<ul style="list-style-type: none"> • DH • MQV 	<ul style="list-style-type: none"> • DH (1024 bits) • ECDH (160 bits) • PSEC-KEM (160 bits) 	(推奨なし)	(ISO/IEC 11770-3 において規定)
共通鍵暗号	64 ビットブロック暗号	3-key トリプル DES	<ul style="list-style-type: none"> • CIPHERUNICORN-E • Hierocrypt-L1 • MISTY1 • 3-key トリプル DES 	MISTY1	<ul style="list-style-type: none"> • CAST-128 • MISTY1 • トリプル DES (3-key を推奨)
	128 ビットブロック暗号	AES	<ul style="list-style-type: none"> • AES • Camellia • CIPHERUNICORN-A • Hierocrypt-3 • SC2000 	<ul style="list-style-type: none"> • AES • Camellia 	<ul style="list-style-type: none"> • AES • Camellia • SEED
	ストリーム暗号	(推奨なし)	<ul style="list-style-type: none"> • MUGI • MULTI-S01 • RC4 (128 bits) 	(推奨なし)	<ul style="list-style-type: none"> • MUGI • SNOW 2.0
ハッシュ関数		<ul style="list-style-type: none"> • SHA-224 • SHA-256 • SHA-384 • SHA-512 	<ul style="list-style-type: none"> • RIPEMD-160 • SHA-1 • SHA-256 • SHA-384 • SHA-512 	<ul style="list-style-type: none"> • Whirlpool • SHA-256 • SHA-384 • SHA-512 	(ISO/IEC 10118 シリーズにおいて規定)

備考：表中の鍵長は、いずれも、推奨されているものの中で最小のものとなっている。

共通鍵暗号のうち 64 ビット・ブロック暗号をみると、ISO/IEC 18033-3 に規定されているとともに、NIST によって認定され、かつ、CRYPTREC、NESSIE のいずれからも推奨されている暗号アルゴリズムは存在しない。ただし、ISO/IEC 18033-3 において規定され、かつ、CRYPTREC と NESSIE から推奨されているものとしては、MISTY1 が挙げられる。128 ビット・ブロック暗号に関しては、AES が ISO/IEC 18033-3 において規定されているほか、NIST によって認定され、CRYPTREC、NESSIE のいずれからも推奨されている。また、Camellia は ISO/IEC 18033-3 に規定されているほか、CRYPTREC と NESSIE から推奨されている。なお、RC4 については、条件付きで CRYPTREC によって

推奨されているだけとなっている。

ハッシュ関数については、SHA-256、SHA-384、SHA-512 が NIST によって認定されているほか、CRYPTREC と NESSIE から推奨されている。

(2) 暗号アルゴリズムを選択する際の主な論点

このようにみていくと、新しく採用する暗号アルゴリズムはかなり絞られてくる。ただし、最終的にどの暗号アルゴリズムにするか、また、鍵長をどのように設定するかについては、各アプリケーションや既存のシステム構成等に依存することになると考えられる。したがって、個別のシステムごとに検討を深めていく必要がある。そうした検討を進めるうえで、論点となりうる項目を以下で説明する。

【論点 1】各機関やプロジェクトの評価結果をどのように重み付けして解釈するか。

具体的には、ISO/IEC 18033 シリーズ、NIST の FIPS および SP、CRYPTREC、NESSIE の評価結果のうち、どれを重視して検討するか（それとも横並びでみるか）をまず検討する必要がある。その際には、各機関・プロジェクトが採用している評価基準には差異が存在する点にも留意することが重要である。NIST や NESSIE においては、暗号アルゴリズムを評価する際に安全性のみならず実装性能も考慮している。一方、CRYPTREC では、基本的に安全性を重視した評価を行っているほか、電子政府推奨暗号リストが作成された時点で実際に調達可能な暗号アルゴリズムが推奨の対象となっている。こうした評価基準の違いを踏まえたうえで、必要とされる安全性のレベルを満足していることをまず確認し、「当該アプリケーションにおいてどの要素（安全性のマージンか実装性能か）を重視するか」といった点を考慮することが求められる。その結果、例えば、評価結果を横並びで考えてよいと判断した場合には、「少なくとも2つの先から推奨されているものを選択する」といった要件を設定し、暗号アルゴリズムを選択することも考えられる。

【論点 2】同一の暗号アルゴリズムであっても各機関やプロジェクトによって認定あるいは推奨される鍵長が異なっていた場合、鍵長をどのように設定するか。

鍵長をどのように設定するかを考える場合も、各機関・プロジェクトにおける評価のスタンスに留意することが重要である。例えば、CRYPTREC の電子政

府推奨暗号リストの場合、そのリストが公表された時点において実際に電子政府向けに調達可能かといった観点からも暗号アルゴリズムの選択が行われており、その意味で最小鍵長が他の推奨鍵長よりも短めに設定されているものもある。こうした点について配慮することが重要である。

原則的には、推奨されている最小鍵長が最も長いものに合わせることで安全性上望ましい。ただし、他の情報システムとの相互運用性を確保することが求められるとすれば、他の既存システムが採用している鍵長と同一に当該システムにおける鍵長を設定することも考えられる。また、IC カードの性能条件などによっては物理的に対応できない場合もありうる。最終的には、こうしたアプリケーションに依存するさまざまな要素も加味して最適な鍵長を選択することが求められる。

【論点 3】暗号化・復号処理速度等の実装性能に関する要件をどのように考慮して暗号アルゴリズムを選択するか。

例えば、IC カードのような比較的計算能力が低い計算機において実装することが想定されており、なるべく処理速度の低下を抑えながら一定の安全性のレベルを達成したいという要求がアプリケーション側から出る可能性がある。こうした状況では、同程度の安全性のレベルを確保可能な暗号アルゴリズムの中で、計算量が比較的少ないものを選択することになると予想される。「どの程度の処理速度の低下であれば許容できるのか」といった個別のアプリケーションにおける実装性能に関する要件を踏まえながら、暗号アルゴリズムの選択について検討することとなる。

【論点 4】公開鍵暗号において KEM や DEM を採用するか否か。

公開鍵暗号においては、ISO/IEC 18033-2、CRYPTREC の電子政府推奨暗号リスト、NESSIE 推奨暗号において、鍵配送目的の暗号アルゴリズムとして KEM が推奨されている。また、ISO/IEC 18033-2 においては KEM に加えて共通鍵暗号を利用する DEM を併用した「KEM-DEM 構成」での使用形態も規定されているほか、CRYPTREC では KEM-DEM 構成での利用が前提とされている。

従来は、鍵配送方式の安全性とメッセージの守秘性や一貫性を確保する方式の安全性が別々に議論されてきたが、近年提案された KEM-DEM 構成に基づいて公開鍵暗号と共通鍵暗号を組み合わせることで、鍵配送方式の安全性とメッセージの守秘性・一貫性をセットで証明可能にすることができるようになった。KEM-DEM 構成は、こうした安全性上の利点に加えて、国際

標準等にも採用されたことを踏まえると、今後さまざまな場面で利用されるようになる可能性がある。こうした点を加味すると、KEM や KEM-DEM 構成に基づく方式の採用も選択肢の 1 つとして検討することが考えられる。

公開鍵暗号を守秘目的で利用する場合でも、実際には共通鍵暗号のセッション鍵の配送に利用されるケースが多いことを考慮すれば、KEM を装備することによって機能上問題が発生することはほとんどないと考えられる。ただし、KEM と DEM を組み合わせた KEM-DEM 構成で暗号を実装する場合には、従来の公開鍵暗号や共通鍵暗号の利用方法とは異なるため、追加的なシステム変更を強いられる可能性も考えられる。また、他の金融機関等の情報システムとの相互接続性が求められるケースでは、通信相手の情報システムにもシステム変更を求めることが必要になる可能性もある。KEM-DEM 構成での暗号の利用を検討する場合には、こうした点についても確認しておく必要がある。

【論点 5】共通鍵暗号において 64 ビット・ブロック暗号と 128 ビット・ブロック暗号のどちらを選択するか。

共通鍵暗号に関しては、ISO/IEC 18033-3、NIST、CRYPTREC、NESSIE のいずれにおいても 64 ビット・ブロック暗号と 128 ビット・ブロック暗号の 2 種類が対象となっている。ただし、代表的な 64 ビット・ブロック暗号であるトリプル DES が FIPS 認定や NESSIE での推奨暗号から外れ、2005 年 11 月 8 日時点で公表されている CRYPTREC の電子政府推奨暗号リストの但し書にある条件も満足されない状態となったことから、十分な「お墨付き」を得た暗号アルゴリズムとしてトリプル DES を位置づけることは難しいと考えられる。また、上記時点における電子政府推奨暗号リストには、「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」との記述がある。こうした点を踏まえると、128 ビット・ブロック暗号の採用をまず検討することが自然であり、仮に、ISO/IEC 18033-3 をベースとして検討する場合には、暗号アルゴリズムとしては AES、Camellia、SEED を最初の検討対象とすることが妥当であると考えられる。

ストリーム暗号については、高速での暗号化処理が可能であることから、既存のブロック暗号を処理速度等の観点で利用困難な場合に活用することも考えられる。ただし、こうしたケースは比較的少ないと考えられる。また、ISO/IEC 18033-4 においては MUGI と SNOW 2.0 が規定されているが、NIST および NESSIE においては認定・推奨されていないことや、そもそもブロック暗号に比べてセキュリティ評価手法が確立していないことを踏まえると、安全性評価の蓄積が相対的に厚いブロック暗号を利用可能な状況下においてあえてストリーム暗号

をブロック暗号に優先して検討する必要性は薄いのではないかとと思われる。

【論点 6】ハッシュ関数におけるハッシュ値のサイズをどのように決めるか。

ハッシュ関数においては、SHA-2 が NIST から、SHA-256、SHA-384、SHA-512 が CRYPTREC と NESSIE から推奨されており、これらのうちどれを選択するかが検討項目となる。基本的には、ハッシュ値のサイズが当該情報システムにおける仕様に合致するかという観点での検討を行うことになると考えられる。

ただし、注意しなければならないのは、NIST 自身、SHA-1 からの移行先として SHA-2 が適切であるかどうか見極められていないことである。これは、SHA-0 に対する攻撃があったときのコメントでもわかるように、当面 SHA-1 が安全であることを前提として、より安全と期待される SHA-2 への移行を計画していた。しかし、予想に反して、実際には SHA-1 に対する攻撃も成功してしまったため、SHA-1 の設計方法をベースに作られている SHA-2 についても本当に安全なのか疑問符が突きつけられているためである。SHA-2 に替わる、もしくは並存する新しいハッシュ関数を策定することが必要かどうかを含めて、NIST 内部で検討が行われているとみられる。

2010 年での SHA-1 の米国政府標準からの廃止がほぼ規定路線である以上、暫定的にせよ、SHA-2 への移行が求められる可能性は高い。ただ、中長期的には、新たなハッシュ関数の追加、移行がある可能性も否定できないことに留意されたい。

(3) その他の留意点

以上の論点のほかに、暗号アルゴリズムの移行に伴って情報システムの仕様変更を行う際に留意すべき項目として、次の 3 点が挙げられる。

【留意点 1】暗号アルゴリズムの仕様変更によって、当該情報システムと接続している他の情報システムとの相互運用性が失われないように配慮する。

金融機関の情報システムは他の情報システムと連携しているケースは少なくない。このようなケースにおいては、例えば、ある銀行が自社の ATM ネットワーク・システムで採用している暗号アルゴリズムを別のものに移行した際に IC キャッシュカードや ATM の仕様を一部見直した結果、当該銀行の IC キャッシュカードが他の銀行の ATM で利用できなくなる、あるいは、他の銀行の IC キャッシュカードが当該銀行の ATM で利用できなくなるといった状況が発生してしま

うおそれがある。

このような問題が発生しないように、暗号アルゴリズムの移行に関連する仕様の変更が情報システムの他の部分にどのような影響を与えるかを見極めることが重要であり、場合によっては当該銀行向けシステムで利用する暗号アルゴリズムと他銀行向けシステムで利用する暗号アルゴリズムを分けることも検討対象となる。また、他の金融機関への影響に関しても、事前に必要に応じて他の銀行とシステム変更の内容を擦りあわせたり、システム変更のタイミングを調整したりすることによって、影響をなるべく小さくするための取組みが重要であると考えられる。

【留意点 2】移行後の新しい暗号アルゴリズムが適切に使用されるように設定変更するとともに、使ってはいけない移行前の暗号アルゴリズムが使用できないようにするための設定変更も行う。

多大なコストを投入して 2010 年問題に対応すべく新しい暗号アルゴリズムを導入したとしても、当該情報システムの設定の不具合によってその暗号アルゴリズムが使用されず、従来の安全性が低い暗号アルゴリズムが引き続き利用できるようになっては意味がない。こうした状況は、インターネット・バンキングにおいて発生する可能性が考えられる。例えば、サーバー側における SSL に関する設定が不適切である場合、128 ビットの鍵長の共通鍵暗号による暗号化通信だけでなく、40 ビット鍵長や 56 ビット鍵長の共通鍵暗号による暗号化通信も可能になっている可能性がある。こうした問題が発生する可能性をなくするためには、単に暗号アルゴリズムの移行を行ってそれを利用可能にするだけでなく、使ってはいけない移行前の安全性の低い暗号アルゴリズムによる通信をできなくするような設定変更をサーバー側で適切に実行することが必要となる。インターネット・バンキングの場面だけに限らず、暗号アルゴリズムの移行の対象となる情報システムにおいてこうした点に留意した対応が求められる。

【留意点 3】やむを得ず、複数の暗号アルゴリズムを利用する場合には、たとえ同種の暗号技術であっても暗号鍵を共用してはならない。

留意点 1 にあるように、他の情報システムとの相互運用性を確保するために、やむを得ず、利用する暗号アルゴリズムを分けるケースがありうる。例えば、ある銀行内部の情報システムにおいて ISO/IEC 18033-3 をベースとして AES や Camellia や SEED に移行したとしても、他銀行向けの情報システムにおいてはトリプル DES の使用が継続されるといったような場合である。

このような場合に同じ共通鍵暗号であるからといって当該銀行向けシステムと他銀行向けシステムとで同じ暗号鍵を利用することは、どちらのシステムにおいても暗号強度の弱い暗号（この場合ではトリプル DES）による安全性しか確保できないことにつながる。その結果、当該銀行向けシステムにおいてトリプル DES よりも安全な暗号アルゴリズムへ移行した効果が失われる。このように、たとえ同種の暗号技術であっても暗号鍵を共用することは、安全性上、極めて問題が多い運用の仕方といえるので、避けなければならない。

(4) 中期的な検討課題

2010 年問題は暗号アルゴリズムの移行をどのように行うかという問題であるが、2010 年という「お墨付き」が失われるタイミングがあらかじめ明確になっているという点で、比較的対応しやすいのではないかと考えられる。一方、極めて発生確率が低いとはいえ、多くの安全性評価が行われた暗号アルゴリズムであっても十分な安全性を有していると今日まで評価されていたものであっても、一夜明けると新しい攻撃法が考案されていて、当該暗号アルゴリズムの安全性が著しく損なわれてしまうという状況が発生する可能性を否定することはできない。こうした暗号アルゴリズムの危殆化が突然発生することも、暗号アルゴリズムのユーザとしては本来想定しておく必要がある。2010 年問題に関する検討を契機として、暗号アルゴリズムの危殆化にも円滑に対応できる体制整備について、個別の金融機関が今後検討することはもちろん、金融業界としても対応について検討することが望まれる。

そうした体制整備に関して、次の 2 つの課題がまず挙げられる。

【課題 1】暗号アルゴリズムの安全性評価の最新情報をフォローするとともに、NIST をはじめとする暗号アルゴリズムの評価を行っている機関・プロジェクトの動向を注視する体制を、個別の金融機関はもちろん、金融業界としても検討し、構築する。

暗号アルゴリズムの安全性に関する「お墨付き」が失われるかが明確でない場合、金融機関自らがどのタイミングで暗号アルゴリズムの移行を行う必要があるかを決定しなければならない。そのためには、現時点までに公表されている暗号アルゴリズムの安全性評価の結果をフォローしておく必要があるほか、先行きの安全性に関する見通しについても、NIST 等の発表を踏まえながら常時検討を行っておくことが求められるといえる。もちろん、暗号アルゴリズムの安全性評価は非常に専門性が高い分野であり、一朝一夕にこうした体制を整備することは容易でない。しかし、金融という公共性の高い分野における情報シ

システムの安全性に関して責任を負っているという立場も踏まえ、地道かつ積極的に対応していくことが金融機関に求められているといえる。

その意味では、NISTをはじめとする各種機関や暗号学会のサポートが受けられない暗号アルゴリズムの安全性評価はすべて自らの努力で行っていく必要がある。そのようなアルゴリズムを採用・運用することは、通常よりも高度な暗号アルゴリズムの安全性評価能力が求められることになる。

また、金融機関が今後デジタル・タイムスタンプ等のサービスを利用するケースも考えられるが、そうした場合には、当該サービスにおいて採用されている暗号アルゴリズムにも留意することが求められると考えられる。特に、デジタル・タイムスタンプは中長期的にデジタル・データの一貫性等を確保するものであり、そこで利用される暗号アルゴリズムが中長期的に安全であることが前提となる。こうした観点からも、暗号アルゴリズムの安全性評価を自ら実施するための体制を構築しておくことが重要であるといえることができる。

【課題 2】暗号アルゴリズムの変更や鍵長の伸長を円滑に行うことができるという意味等での「拡張性」を有する情報システムを実現する。

暗号アルゴリズムの危殆化に対して円滑に対応する方法の 1 つとして、暗号アルゴリズムや鍵長の変更を柔軟かつ容易に行うことができるように情報システムを設計・構築することが考えられる。具体的には、容易に入替え可能な暗号モジュールを用いて暗号アルゴリズムを実装する、鍵長や暗号文のサイズの変更を可能にする通信フォーマットを採用するといった方法がまず考えられる。

また、暗号アルゴリズムの危殆化への対策としては、安全性に関する特性が異なった複数の暗号アルゴリズムをあらかじめ実装しておくという方法も考えられる。このような情報システムの場合、複数の暗号アルゴリズムのうち 1 つが危殆化したとしても、別の暗号アルゴリズムが引き続き十分な安全性を確保し、情報システム全体としては要求される安全性のレベルを維持できる可能性がある。複数の暗号アルゴリズムを利用できるようにしておくというシステムの特性は、別の意味での「拡張性」と捉えることもできる。

また、暗号アルゴリズムの危殆化に備えるという観点からは、例えば、計算量的な安全性に基づく方式の代わりに、一定の情報量を入手困難である限りいくら計算能力を有していても安全性を確保できるという「情報量的な安全性」に基づく方式も有用であり、今後の研究動向に注目することが有用であろう。また、量子力学の原理を活用する方式（量子暗号）に関しても、近年その実用化に向けた研究開発が盛んに行われており、今後の研究動向に注目することが有用であると思われる。

6. おわりに

2010年問題は、2-key トリプル DES や 1024 ビット RSA、SHA-1 等を利用している金融機関にとって重要な問題である。金融分野においては、これまで暗号アルゴリズムの選定を行う際に、NIST がどの暗号アルゴリズムに米国政府標準暗号という「お墨付き」(FIPS 認定)を付与しているかが重要なベンチマークとされてきた。すなわち、多くの金融機関は、暗号アルゴリズムの審査機関として定評のある NIST の審査結果を重視し、その意思決定に沿った暗号アルゴリズムの選定を行うことによって、採用した暗号アルゴリズムの安全性や信頼性を顧客等に対してアピールすることができた。金融機関は、こうした過去の経緯を踏まえたうえで、NIST による意思決定の背景を理解し、今後どのように対応するかを検討する必要がある。

1970年代末に NIST が DES を FIPS 認定暗号としたことで DES がその後民間部門で広く普及したときと比較すると、今回は、新しく採用することができる暗号アルゴリズムの選択肢が広い。すなわち、NIST による FIPS 認定暗号だけでなく、ISO/IEC 18033 シリーズの国際標準暗号、CRYPTREC の電子政府推奨暗号リスト、NESSIE 推奨暗号といった、暗号研究者らによって客観的に評価された安全な暗号アルゴリズムを利用することが可能となっている。これらの暗号アルゴリズムは、安全性が依拠している数学問題やアルゴリズムの構造等が異なっているほか、実装性能も異なっている。金融機関は、そうした各暗号アルゴリズムの特性を理解したうえで、どの暗号アルゴリズムに移行することが適当かを検討することが求められている。

ただし、どの暗号アルゴリズムに移行するのか、また、既存の情報システムや顧客利便性への影響を最小限にしながらどのように移行を進めていくのかについては、各金融機関が自社のアプリケーションと照らし合わせて検討しなければならない。例えば、当該システムに関連する別の情報システムとの相互運用性の確保、移行前の弱い暗号アルゴリズムの使用を排除するための設定変更等に配慮することが求められる。また、2010年問題を暗号アルゴリズムの危殆化の一形態と位置づけることも可能であり、そうした観点から、将来の暗号アルゴリズムの危殆化に備えた検討も望まれる。暗号アルゴリズムの安全性評価結果や NIST 等の動向をフォローする体制を整備するとともに、拡張性を有する情報システムの設計・開発について検討することが重要であろう。

2010年問題に対して適切に対処するためには山積している検討課題を1つ1つクリアしていく必要があり、2010年までに残されている時間は決して多いとはいえない。今後の金融機関による早急な対応が望まれる。 以 上

【参考文献】

- 岩下直行、『金融分野における情報技術の国際標準化動向 - ISO/TC68 における最近の議論を中心に』、第 8 回決済システムフォーラム (2004 年 11 月 5 日) におけるプレゼンテーション資料、2004 年 (アクセス日: 2005 年 9 月 14 日、<http://www.boj.or.jp/set/04/data/set0411b5.pdf>)
- 情報処理振興事業協会 (IPA)・通信・放送機構 (TAO)、『暗号技術評価報告書 (2001 年度版)』、2002 年
- ・、『暗号技術評価報告書 (2002 年度版)』、2003 年
- 総務省・経済産業省、『電子政府推奨暗号リスト』、2003 年
(http://www.cryptec.jp/images/cryptec_01.pdf、アクセス日: 2005 年 11 月 8 日)
- 谷口文一・太田和夫・大久保美也子、「Triple DES を巡る最近の標準化動向について」、『金融研究』第 18 巻別冊第 1 号、日本銀行金融研究所、1999 年、29~50 頁
- 吉田雅徳・古原和邦・今井秀樹、「最新の製品における WEP 実装の検証」、『第 28 回情報理論とその応用シンポジウム予稿集』、2005 年 (発表予定)
- Adleman, Leonard M., "The function field sieve," *Algorithmic Number Theory*, LNCS 887, Springer-Verlag, 1994, pp. 108-121.
- American National Standards Institute, *X9.52: Triple Data Encryption Algorithm Modes of Operation*, 1998.
- Blake-Wilson, Simon, Magnus Nystrom, David Hopwood, Jan Mikkelsen and Tim Wright, *RFC 3546: Transport Layer Security (TLS) Extensions*, 2003.
- , -----, -----, ----- and -----, *IETF Internet Draft: Transport Layer Security (TLS) Extensions*, 2005.
- Brent, Richard, "Recent progress and prospects for integer factorization algorithms," *Proceedings of COCOON 2000*, LNCS 1858, Springer-Verlag, 2000, pp. 3-20.
- Certicom Research, *SEC 1: Elliptic Curve Cryptography, Version 1.0*, 2000.
- Coppersmith, Don, "Fast evaluation of logarithms in fields of characteristic two," *IEEE Transaction on Information Theory*, IT-30 (4), 1984, pp. 587-594.
- Dierks, Tim, and Christopher Allen, *RFC 2246: The TLS Protocol Version 1.0*, 1999.
- Dierks, Tim, and Eric Rescorla, *IETF Internet Draft: The TLS Protocol, Version 1.1*, 2005.
- ElGamal, Taher, "A subexponential-time algorithm for computing discrete logarithms over $GF(p^2)$," *IEEE Transactions on Information Theory* 31, 1985, pp. 473-481.
- EMVco, *EMV Integrated Circuit Card Specifications for Payments Systems Version 4.1, Book 2: Security and Key Management*, 2004.
- , *EMV Issuer and Application Security Guidelines, Version 1.3*, 2005.
- European Committee for Standardization and Information Society Standardization System (CEN/ISSS), *Pr CWA 14174-3: Financial transactional IC card reader (FINREAD) - Part 3: Security requirements*, 2002.
- Factor World, *General Purpose Factoring Records*. (<http://www.crypto-world.com/FactorRecords.html>)
- Fluhrer, Scott, Itsik Mantin, and Adi Shamir, "Attacks On RC4 and WEP," *CryptoBytes*

- Volume 5, No. 2, 2002. (<http://www.rsasecurity.com/rsalabs/CRYPTObytes/index.html>)
- Franke, Jens, Thorsten Kleinjung, Christof Paar, Jan Pelzl, Christine Priplata, and Colin Stahlke, "SHARK: A Realizable Special Hardware Sieving Device for Factoring 1024-Bit Integers," *Proceedings of CHES 2005*, LNCS 3659, Springer-Verlag, 2005, pp. 119-130.
- Frey, Gerhard and Hans-George Rück, "A Remark Concerning m-divisibility and the Discrete Logarithm in the Divisor Class Group of Curve," *Mathematics of Computation* 62 (206), 1994, pp. 865-874.
- Geiselmann, Willi, Adi Shamir, Rainer Steinwandt, and Eran Tromer, "Scalable Hardware for Sparse Systems of Linear Equations with Applications to Integer Factorization," *Proceedings of CHES 2005*, LNCS 3659, Springer-Verlag, 2005, pp. 131-146.
- Gordon, Dan, "Discrete Logarithms in $GF(p)$ Using the Number Field Sieve," *SIAM Journal on Discrete Mathematics* 6, 1993, pp. 124-138.
- Information-technology Promotion Agency, Japan, *CRYPTREC Report 2002*, 2003. (http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/c02e_report2.pdf)
- International Organization for Standardization (ISO), *ISO 9564-1: Banking -- Personal Identification -- Number management and security -- Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*, 2002.
- , *ISO 9564-2: Banking -- Personal Identification -- Number management and security -- Part 2: Approved algorithms for PIN encipherment*, 2005a.
- , *ISO 11568-2: Banking -- Key management (retail) -- Part 2: Key management techniques for symmetric ciphers*, 2005b.
- , *ISO 11568-4: Banking -- Key management (retail) -- Part 4: Key management techniques using public key cryptography*, 1998a.
- , *ISO 13491-2: Banking -- Secure cryptographic devices (retail) -- Part 2: Security compliance checklists for devices used in financial transactions*, 2005c.
- , *ISO/TR 13569: Banking and related financial services -- Information security guidelines, Amendment 1*, 1998b.
- , *ISO/TR 17944: Banking -- Security and other financial services -- Framework for security in financial systems*, 2002.
- and International Electrotechnical Commission (IEC), *ISO/IEC 10118-2: Information technology -- Security techniques -- Hash functions -- Part 2: Hash functions Using an n-bit Block Cipher Algorithm*, 2000.
- and -----, *ISO/IEC 10118-3: Information technology -- Security techniques -- Hash functions -- Part 3: Dedicated Hash functions*, 2004.
- and -----, *ISO/IEC 10118-4: Information technology -- Security techniques -- Hash functions -- Part 4: Hash functions Using Modular Arithmetic*, 1998a.
- and -----, *ISO/IEC 11770-3: Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques*, 1999.
- and -----, *ISO/IEC 14888-3: Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Certificate-based mechanisms*, 1998b.
- and -----, *ISO/IEC FCD 18033-2: Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers*, 2005a.
- and -----, *ISO/IEC 18033-3: Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers*, 2005b.
- and -----, *ISO/IEC 18033-4: Information technology -- Security techniques -- Encryption algorithms -- Part 4: Stream ciphers*, 2005c.
- and -----, *ISO/IEC 9796-2: Information technology -- Security techniques -- Digital*

- signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms*, 2002.
- Japan Bankers Association (JBA), *Standard Specifications of IC Cash Cards*, 2001 (in Japanese)
- Kaliski, Bart, *TWIRL and RSA Key Size*, 2003.
(<http://www.rsasecurity.com/rsalabs/node.asp?id=2004>)
- Kusuda, Koji, and Tsutomu Matsumoto, "A Strength Evaluation of the Data Encryption Standard," *IMES Discussion Paper Series 97-E-5*, Bank of Japan, 1997.
- Lenstra, Arjen K., and Eric R. Verheul, "Selecting Cryptographic Key Size," *Journal of Cryptology*, 14(4), 2001, pp.255-293.
- Lucks, Stefan, and Magnus Daum, "The Story of Alice and her Boss: Hash Functions and the Blind Passenger Attack," *Presentation at Rump Sessions of Eurocrypt 2005*, 2005.
- Menezes, Alfred J., Tatsuaki Okamoto, and Scott A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, 1991, pp. 80-89.
- Merkle, Ralph, and Martin Hellman, "On the Security of Multiple Encryption," *Communication of ACM*, Vol. 24, No. 7, 1981, pp.465-467.
- National Institute of Standards and Technology (NIST), *Recommendation on Key Management, SP800-57*, 2005a.
(<http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf>)
- , *Cryptographic Algorithms and Key Sizes for Personal Identity Verification, SP800-78*, 2005b. (<http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf>)
- , *Personal Identity Verification of Federal Employees and Contractors, FIPS 201*, 2005c.
(<http://csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf>)
- , *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, SP 800-56*, Draft, 2005d.
- , *NIST Brief Comments on Recent Cryptanalytic Attacks on Secure Hashing Functions and the Continued Security Provided by SHA-1*, 2004.
(<http://csrc.nist.gov/NIST%20Brief%20Comments%20on%20Hash%20Standards%208-25-2004.pdf>)
- , *NIST Brief Comments on Recent Cryptanalytic Attacks on SHA-1*, 2005e.
(<http://csrc.nist.gov/news-highlights/NIST-Brief-Comments-on-SHA1-attack.pdf>)
- New European Schemes for Signatures, Integrity, and Encryption (NESSIE) consortium, *Portfolio of recommended cryptographic primitives*, 2003.
(<https://www.cosic.esat.kuleuven.be/nessie/deliverables/decision-final.pdf>)
- Pomerance, Carl, "Fast, Rigorous Factorization and Discrete Logarithm Algorithms," *Discrete Algorithms and Complexity*, edited by D. S. Johnson, T. Nishizeki, A. Nozaki, and H. S. Wilf, Academic Press, 1987, pp. 119-143.
- Preneel, Bart, Alex Biryukov, Charles De Cannière, Sidikka B. Örs, Elisabeth Oswald, Bart Van Rompay, Louis Granboulan, Emmanuelle Dottax, Gilles Martinet, Sean Murphy, Alexander Dent, Rachel Shipsey, Christine Swart, Juliette White, Markus Dichtl, Stefan Pyka, Marcus Schafheutle, Pascale Serf, Edi Biham, Elad Barkan, Yan Braziler, Orr Dunkelman, Vladimir Furman, Dan Kenigsberg, Julia Stolin, Jean-Jacques Quisquater, Mathieu Ciet, Francesco Sica, Håvard Raddum, Lars Knudsen, and Matthew Parker, *Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption*, Version 0.15 (beta), 2004.
- Sato, Takakazu, and Kiyomichi Araki, "Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves," *Commentarii Mathematici Universitatis Sancti Pauli* 47 (1), 1998, pp. 81-92.

- Schirokauer, Oliver, "Discrete Logarithms and Local Units," *Journal of Philosophical Transactions of the Royal Society of London, Series A*, Vol. 345, 1993, pp. 409-423.
- , Damian Weber, and Thomas Denny, "Discrete Logarithms: The Effectiveness of the Index Calculus Method," *Algorithmic Number Theory*, LNCS 1122, Springer-Verlag, 1996, pp. 335-361.
- SWIFT, "Secure Card Reader Upgrade Coming Up," *SWIFT Bulletin*, No.13, 2000, pp.1-2.
- Thomé, Emmanuel, *Discrete Logarithms in $GF(2^{607})$* , 2002.
(<http://www.lix.polytechnique.fr/Labo/Emmanuel.Thome/announcement/announcement.html>)
- Wang, Xiaoyun, Andrew Yao, and Frances Yao, "New Collision Search for SHA-1," *Presentation of Rump Session of CRYPTO 2005*, 2005.
(<http://www.iacr.org/conferences/crypto2005/r/2.pdf>)
- , Yiqun Lisa Yin, and Hongbo Yu, "Finding Collisions in the Full SHA-1," 2005.
(<http://www.infosec.sdu.edu.cn/paper/sha1-crypto-auth-new-2-yao.pdf>)