# 暗号アルゴリズムにおける2010年問題について

宇根正志（うねまさし）／神田雅透（かんだまさゆき）

## 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1,024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などを前提とすると、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1,024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きており、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の対応状況などについて説明する。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、2010年問題、ハッシュ関数、トリプルDES、RC4、RSA、SHA-1

本稿は、2006年3月28日に日本銀行で開催された「第8回情報セキュリティ・シンポジウム」への提出論文に加筆・修正を施したものである。本稿を作成するに当たっては、今井秀樹教授（中央大学、産業技術総合研究所情報セキュリティ研究センター長）、および松本勉教授（横浜国立大学）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。本稿で示されている内容および意見は筆者たち個人に属し、産業技術総合研究所情報セキュリティ研究センター、NTT情報流通プラットフォーム研究所、あるいは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たち個人に属する。

宇根正志　日本銀行金融研究所
（現 産業技術総合研究所情報セキュリティ研究センター、E-mail: masashi-une@aist.go.jp）
神田雅透　NTT情報流通プラットフォーム研究所（E-mail: kanda.masayuki@lab.ntt.co.jp）

## １．はじめに

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など）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）など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1,024ビットに設定した方式（以下、1,024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・バンキングなどにおいては、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1,024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などによって、2-keyトリプルDES、1,024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ている点が挙げられる。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（および処理速度など）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、安全性など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なども不可欠であり、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。

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。

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（後掲の表10参照）。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など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る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する。そのうえで、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などに規定されているもの、および、インターネット・バンキングなど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などに規定・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規定・記述されているかを整理すると、表1のとおりである。

表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1,024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1,024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］）。

そのほか、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（全国銀行協会［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。

**表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）<br>― メッセージ暗号化 | DES | （記載なし） | （記載なし） |
| ISO 16609（MACの要件） | DES<br>トリプルDES | （記載なし） | （記載なし） |
| ISO TR 13569<br>― ガイドライン | 鍵長80ビット以上 | 鍵長1,024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<br>― 鍵管理（共通鍵暗号） | トリプルDES | （記載なし） | （記載なし） |
| ISO TR 17944<br>― セキュリティ管理の枠組み | トリプルDES（ANS X9.52）<br>AES（FIPS 197） | RSA（ANS X9.31）<br>DSA（ANS X9.30-1）<br>ECDSA（ANS X9.62）<br>ISO/IEC 15946<br>ISO/IEC 9796<br>ISO/IEC 14888 | ISO/IEC 10118<br>・10118-2:共通鍵暗号ベースの方式（4つ）を規定<br>・10118-3:RIPEMD-(128, 160)、SHA-(1, 224, 256, 384, 512)、Whirlpool<br>・10118-4:MASH-(1, 2) |
| ISO/DIS 11568-4<br>― 鍵管理（公開鍵暗号） | （記載なし） | RSA（ISO/IEC 9796）<br>DSA | |
| ISO 9564-1, 2<br>― PINの暗号化 | トリプルDES（鍵長は少なくとも112ビット） | RSA（EMV） | （記載なし） |
| ISO TR 19038<br>―トリプルDESの利用モード | トリプルDES | （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<br>トリプルDES（2-keyの明示はないがEMVに準拠） | RSA（鍵長は1,984ビット以下、EMVと同じ） | SHA-1 |
| 【参考】EMV version 4.1 | 2-key トリプルDES | RSA（ISO/IEC 9796-2、鍵長は1,984ビット以下） | SHA-1 |
| 【参考】FINREAD | DES<br>トリプルDES | RSA（鍵長は1,024ビット以上） | SHA-1<br>MD5<br>RIPEMD-160 |

これらの国際標準やガイドラインなど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ス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]。

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］）。

RSAについても、鍵長に関してISO TR 13569に1,024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1,024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、1,024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交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1,024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1,024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1,152ビット、1,408ビット、1,984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・エクスプローラやネットスケープなど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 *et al.*［2003］）ほか、TLS version 1.1のInternet draftが提案されている（Dierks and Rescorla［2005］、Blake-Wilson *et al.*［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1,024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）。

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、これらの分類に従って、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

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・フォース攻撃の一種である。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で真の鍵をみつけるための計算量は$2^n$となる。

**表2　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。

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2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］）ものの、そのほか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

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　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。<br>【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。<br>【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。 |
| IDEA | 128 | 64 | |
| MISTY1 | 128 | 64 | |
| AES | 128, 192, 256 | 128 | 【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。 |
| 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。

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必要がある。

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、バースデー・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。

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、初期状態からの撹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エ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。

1,024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1,024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、1,024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2,048

8 なお、量子コンピュータが登場すれば、素因数分解問題など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ヵ月で倍増する」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。

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1,024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2,048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1,536ビットと見積もっており、1,024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、1,024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エアについても、その設計方法とハードウエ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エアSHARKを提案しており、1,024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、1,024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エ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ヵ月で実行可能であるとしている。こうした専用ハードウエアの実現可能性に関する研究結果も、1,024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。

### ロ．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など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［1987］、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1,024ビットの鍵長が利用される場面が多いようである。本節(2)イ.において説明したように、2010年の時点からみると1,024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。

**ハ．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などから、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ヵ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整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1,024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、衝突を高い確率でみつけるためには、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みつかるケースはまれであり、実際の運用においては文意的に改ざんを検

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）入力のペアのことを指す。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。

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、文意的にも改ざん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、文意的にも改ざん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。

## 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）などによって、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などを内容とする標準FIPS[12]やガイドラインSP[13]を策定してい

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など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　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 |

る（表4参照）。

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シリーズである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、Menezes-Qu-Vanstone方式（以下、MQVと呼ぶ）とDH（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となる各種暗号鍵の種類やその利用方法、必要とされる鍵長などを詳細に記述している（表5参照）。表5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。

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2,048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、1,024ビットRSA、1,024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。

### （ロ）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など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、連邦政府の職員などにICカー

**表5　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<br>3-keyトリプルDES<br>AES（鍵長128、192、256ビット） | 最小鍵長を1,024ビットとする。 | 最小鍵長を1,024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<br>AES（鍵長128、192、256ビット） | 最小鍵長を2,048ビットとする。 | 最小鍵長を2,048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3,072ビットとする。 | 最小鍵長を3,072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。

ド（PIVカードと呼ばれる）を配布し、そのPIVカードやPINなどによって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、(1) 個人識別用の鍵（必須）、(2) PIVカード認証用の鍵（オプション）、(3) デジタル署名生成用の鍵（オプション）、(4) 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、ほか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6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。

**表6　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 | RSA（鍵長：1,024、2,048、3,072ビットのいずれか）<br>ECDSA（鍵長：224ビットから283ビットまで） | |
| | 2011年以降 | RSA（鍵長：2,048ビットまたは3,072ビット）<br>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年末まで | 共通鍵暗号の場合 | 2-keyトリプルDES<br>3-keyトリプルDES<br>AES（鍵長：128、192、256ビットのいずれか） |
| | | 公開鍵暗号の場合 | RSA（鍵長：1,024、2,048、3,072ビットのいずれか）<br>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 | 3-keyトリプルDES<br>AES（鍵長：128、192、256ビットのいずれか） |
| | | 公開鍵暗号の場合 | RSA（鍵長：2,048、3,072ビットのいずれか）<br>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年末まで | RSA（鍵長：1,024、2,048、3,072ビットのいずれか）<br>ECDSA（鍵長：224ビットから283ビットまで） | |
| | 2009年以降 | RSA（鍵長：2,048、3,072ビットのいずれか）<br>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年末まで | RSA（鍵長：1,024、2,048、3,072ビットのいずれか）<br>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 | RSA（鍵長：2,048、3,072ビットのいずれか）<br>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。

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1,024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2,048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。

**ハ．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、本節(1)ロ.(ロ)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

前節と本節(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ている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年をめど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評判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など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を規定するように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などの標準化団体は、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]。

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。

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評判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評判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評判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はなく、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・バンキングなど、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。

## 5．2010年問題などへの対応のあり方

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、どのような手続き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などを整理する。

### (1) 各種機関・プロジェクトによって規定あるいは認定あるいは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5参照）。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2,048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2,048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。

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ほか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、公的な機関など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などが提案され、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7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、離散対数問題ベース、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。

**表7　ISO/IEC 18033シリーズ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） | | 素因数分解問題ベース：RSA-KEM、RSA-OAEP、HIME(R)<br>離散対数問題ベース：ACE-KEM<br>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） | 64ビット・ブロック暗号 ：CAST-128、MISTY1、トリプルDES<br>128ビット・ブロック暗号：AES、Camellia、SEED |
| | ストリーム暗号（パート4） | MUGI<br>SNOW 2.0 |

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。

### ハ．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、実際に調達が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8参照、総務省・経済産業省［2003］）。

**表8　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）(備考1) |
| | 鍵共有 | DH、ECDH、PSEC-KEM (備考2) |
| 共通鍵暗号 | 64ビット・ブロック暗号(備考3) | CIPHERUNICORN-E、Hierocrypt-L1、MISTY1、3-keyトリプルDES (備考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 (備考5) |
| その他 | ハッシュ関数 | RIPEMD-160 (備考6)、SHA-1 (備考6)、SHA-256、SHA-384、SHA-512 |
| | 擬似乱数生成系 (備考7) | PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1<br>PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1<br>PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1 |

備考：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。
2. KEM-DEM構成における利用を前提とする。
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。
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）SP 800-67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。
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。
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。
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。

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。

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。

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1,024ビット以上、DSAおよびDHの場合には1,024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、「KEM[17]-DEM[18]構成における利用を前提とする」との但書がある。

共通鍵暗号においては、2006年5月29日時点で公表されている電子政府推奨暗号リストに、但書として「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、「SP 800-67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書が付いている[19]。また、鍵長128ビットのRC4も推奨されているものの、「SSL

17 KEM（key encapsulation mechanism）は、守秘目的の公開鍵暗号方式の利用形態の1つであり、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、共通鍵暗号の利用形態の1つであり、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。

19「SP 800-67として規定されていること」の但書は、2005年12月13日に、「FIPS 46-3として規定されていること」というものが変更されたものである。

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。

### ニ．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など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などが総合的に判断され、表9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など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。

**表9　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）(備考1)、ECDSA（第2推奨）(備考2)、SFLASH（特定用途） |
| | 守秘 | PSEC-KEM（第1推奨）(備考2)、RSA-KEM（第2推奨）(備考1)、ACE-KEM（特定用途）(備考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 (備考4)、SHA-256、SHA-384、SHA-512 |
| | メッセージ認証子 | UMAC、TTMAC、EMAC、HMAC |

備考：1. 中期的（5～10年）な安全性を確保する目的で、鍵長は1,536ビット以上を推奨。
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。
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1,536ビット以上を推奨。
4. Whirlpoolのハッシュ値のサイズは512ビットである。

資料：NESSIE consortium［2003］（2003年2月27日付）をベースとして作成した。

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1,536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1,536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．規定あるいは認定あるいは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10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10　国際標準などに規定あるいは認定あるいは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 | RSA（2,048ビット）<br>DSA（2,048ビット）<br>ECDSA（224ビット） | DSA（1,024ビット）<br>ECDSA（160ビット）<br>RSASSA-PKCS1-v1_5（1,024ビット）<br>RSA-PSS（1,024ビット） | RSA-PSS（1,536ビット）<br>ECDSA（160ビット）<br>SFLASH | （ISO/IEC 9796-2と14888-3において規定） |
| | 守秘 | （推奨なし） | RSA-OAEP（1,024ビット）<br>RSAES-PKCS1-v1_5（1,024ビット） | PSEC-KEM（160ビット）<br>RSA-KEM（1,536ビット）<br>ACE-KEM | RSA-KEM<br>RSA-OAEP<br>HIME (R)<br>ACE-KEM<br>PSEC-KEM<br>ECIES-KEM |
| | 鍵配送 | DH<br>MQV | DH（1,024ビット）<br>ECDH（160ビット）<br>PSEC-KEM（160ビット） | （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 | CIPHERUNICORN-E<br>Hierocrypt-L1<br>MISTY1<br>3-keyトリプルDES | MISTY1 | CAST-128<br>MISTY1<br>トリプルDES（3-keyを推奨） |
| | 128ビット・ブロック暗号 | AES | AES<br>Camellia<br>CIPHERUNICORN-A<br>Hierocrypt-3<br>SC2000 | AES<br>Camellia | AES<br>Camellia<br>SEED |
| | ストリーム暗号 | （推奨なし） | MUGI<br>MULTI-S01<br>RC4（128ビット） | （推奨なし） | MUGI<br>SNOW 2.0 |
| ハッシュ関数 | | SHA-224<br>SHA-256<br>SHA-384<br>SHA-512 | SHA-1<br>SHA-256<br>SHA-384<br>SHA-512<br>RIPEMD-160 | SHA-256<br>SHA-384<br>SHA-512<br>Whirlpool | （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など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ほか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が安全性上望ましい。ただし、ほか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、ほか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・復号処理速度など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て利用することによって、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、国際標準など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、ほかの金融機関など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など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に代わる、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。ただし、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いては意味がない。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はなく、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はなく、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、まず次の2つの課題が挙げられる。

【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など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・タイムスタンプなど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・データの一貫性など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うことができる。

【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などでの「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1,024ビットRSA、SHA-1など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など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など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など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など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。

## 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（http://www.boj.or.jp/type/release/zuiji/kako03/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）』、IPA・TAO、2002年

――― ・ ―――、『暗号技術評価報告書（2002年度版）』、IPA・TAO、2003年

全国銀行協会、『全銀協ICキャッシュカード標準仕様』、全国銀行協会、2001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）

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

Adleman, Leonard M., "The function field sieve," *Algorithmic Number Theory*, LNCS 887, Springer-Verlag, 1994, pp. 108-121.

American National Standards Institute (ANSI), *X9.52: Triple Data Encryption Algorithm Modes of Operation*, ANSI,1998.

Blake-Wilson, Simon, Magnus Nystrom, David Hopwood, Jan Mikkelsen, and Tim Wright, *RFC 3546: Transport Layer Security (TLS) Extensions*, 2003. (http://www.ietf-org/rfc/rfc3546.txt)

―――, ―――, ―――, ―――, and ―――, *IETF Internet Draft: Transport Layer Security (TLS) Extensions*, 2005. (http://www.3ietf-org/proceedings/06mar/IDs/draft-ietf-tls-rfc3546bis-02.txt)

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. (http://www.secg-org/collateral/sec1_final.pdf)

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. (http://rfc.net/rfc2246.html)

―――, and Eric Rescorla, *IETF Internet Draft: The TLS Protocol, Version 1.1*, 2005. (http://www3.ietf.org/proceedings/05nov/IDs/draft-ietf-tls-rfc2246-bis-13.txt)

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. (http://www.emvco.com/cgi_bin/detailspec.pl?id=5)

―――, *EMV Issuer and Application Security Guidelines, Version 1.3*, 2005. (http://www.emvco.com/cgi_bin/detailspec.pl?id=3)

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*, CEN/ISSS, 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*, 5 (2), 2002. (http://www.rsasecurity.com/rsalabs/cryptobytes/cryptobytes_v5n2.pdf)

Franke, Jens, Thorsten Kleinjung, Christof Paar, Jan Pelzl, Christine Priplata, and Colin Stahlke, "SHARK: A Realizable Special Hardware Sieving Device for Factoring 1,024-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*, ISO, 2002.

————, *ISO 9564-2: Banking– Personal Identification– Number management and security– Part 2: Approved algorithms for PIN encipherment*, ISO, 2005a.

————, *ISO 11568-2: Banking– Key management (retail)– Part 2: Key management techniques for symmetric ciphers*, ISO, 2005b.

————, *ISO 11568-4: Banking– Key management (retail)– Part 4: Key management techniques using public key cryptography*, ISO, 1998a.

————, *ISO 13491-2: Banking– Secure cryptographic devices (retail)– Part 2: Security compliance checklists for devices used in financial transactions*, ISO, 2005c.

————, *ISO TR 13569: Banking and related financial services– Information security guidelines, Amendment 1*, ISO, 1998b.

————, *ISO TR 17944: Banking– Security and other financial services– Framework for security in financial systems*, ISO, 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*, ISO, 2000.

————, and ————, *ISO/IEC 10118-3: Information technology– Security techniques– Hash functions– Part 3: Dedicated Hash functions*, ISO, 2004.

———, and ———, *ISO/IEC 10118-4: Information technology– Security techniques– Hash functions– Part 4: Hash functions Using Modular Arithmetic*, ISO, 1998a.

———, and ———, *ISO/IEC 11770-3: Information technology– Security techniques– Key management– Part 3: Mechanisms using asymmetric techniques*, ISO, 1999.

———, and ———, *ISO/IEC 14888-3: Information technology– Security techniques– Digital signatures with appendix– Part 3: Certificate-based mechanisms*, ISO, 1998b.

———, and ———, *ISO/IEC FCD 18033-2: Information technology– Security techniques– Encryption algorithms– Part 2: Asymmetric ciphers*, ISO, 2005a.

———, and ———, *ISO/IEC 18033-3: Information technology– Security techniques– Encryption algorithms– Part 3: Block ciphers*, ISO, 2005b.

———, and ———, *ISO/IEC 18033-4: Information technology– Security techniques– Encryption algorithms– Part 4: Stream ciphers*, ISO, 2005c.

———, and ———, *ISO/IEC 9796-2: Information technology– Security techniques– Digital signature schemes giving message recovery– Part 2: Integer factorization based mechanisms*, ISO, 2002.

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. (http://www.cits.rub.de/imperia/md/content/magnus/rump_eco5.pdf)

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*, ACM, 1993, pp. 80-89.

Merkle, Ralph, and Martin Hellman, "On the Security of Multiple Encryption," *Communication of ACM*, 24 (7), 1981, pp. 465-467.

National Institute of Standards and Technology (NIST), *Recommendation on Key Management, SP800-57*, NIST, 2005a. (http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf)

———, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification, SP800-78*, NIST, 2005b. (http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf)

———, *Personal Identity Verification of Federal Employees and Contractors, FIPS 201*, NIST, 2005c.

———, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, SP 800-56*, Draft, NIST, 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," in D. S. Johnson, T. Nishizeki, A. Nozaki, and H. S. Wilf, eds. *Discrete Algorithms and Complexity*, 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. (http://www.cryptonessie.org/)

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, SWIFT, 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," *Advances in Cryptology- CRYPTO 2005*, LNCS 3621, Springer-Verlag, 2005, pp. 17-36.