

金融分野における暗号アルゴリズムの 2010 年問題について

宇根正志 (日本銀行金融研究所)・神田雅透 (NTT 情報流通プラットフォーム研究所)

1. はじめに

金融分野では、ATM・ホスト間で交信される金融取引データの機密性・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・クライアント間での相互認証といった目的で、暗号アルゴリズムが利用されている。

データの機密性確保には共通鍵暗号が、共通鍵暗号で利用する秘密鍵の配送には公開鍵暗号が、データの一貫性確保や通信相手の確認にはメッセージ認証コード (MAC) やデジタル署名が用いられている。こうした暗号アルゴリズムを構成する要素としてハッシュ関数も利用されている。現在利用中の主流とみられる暗号アルゴリズムは、共通鍵暗号は 2-key トリプル DES¹ と RC4、公開鍵暗号・デジタル署名は鍵長 1024 ビットの RSA (以下、1024 ビット RSA と呼ぶ)、ハッシュ関数は SHA-1 である。

しかし、これらは、2010 年に、米国立標準技術研究所 (NIST: National Institute for Standards and Technology) による安全性に関する「お墨付き」を喪失する公算が高い。NIST は、米国連邦政府機関での情報システムにおける 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発表している。また、RC4 は、もともと NIST によって認定あるいは推奨されていない。

このため、上記の暗号アルゴリズムを今後も長

¹ トリプル DES は、DES を「暗号化アルゴリズム→復号アルゴリズム→暗号化アルゴリズム」の順番で 3 回適用して暗号化を行う方式であり、これら 3 つの DES アルゴリズムに用いられる鍵をすべて異なるものに設定する (3 種類の鍵を用いる) ケースは 3-key トリプル DES、2 回の暗号化アルゴリズムの鍵を同一に設定する (2 種類の鍵を用いる) ケースは 2-key トリプル DES と呼ばれる。

期間使用し続けることは、レピュテーションの観点から難しい情勢となっており、2011 年以降も中長期にわたって継続して利用する予定のシステムにおいては、より高い安全性を有する暗号アルゴリズムへの移行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、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、2010 年問題と略す) と呼ぶ。

以下では、まず、金融分野で主流となっている暗号アルゴリズムの現時点における安全性評価結果を整理する。次に、NIST のほか、ISO (International Organization for Standardization)、CRYPTREC (Cryptography Research and Evaluation Committees)、NESSIE (New European Schemes for Signatures, Integrity, and Encryption) で認定、規定、あるいは、推奨されている暗号アルゴリズムを紹介し、2010 年問題に対処していく際の論点を示す。

なお、本稿中の意見は、すべて筆者に属し、日本銀行あるいは NTT の見解を示すものではない。

2. 金融分野の主流となっている暗号アルゴリズム

金融分野における情報セキュリティ技術の国際標準化を担当する ISO/TC68 傘下の国際標準・ガイドラインや金融向けの各種デファクト標準等をみると (表 1 参照)、共通鍵暗号にはトリプル DES が採用されているケースが多い。トリプル DES の中でも、PIN (Personal Identification Number) の暗号化方式を規定する ISO 9564-2 (ISO [2005]) や、Europay、Mastercard、Visa が共同で作成した金融向け IC カードの技術仕様である EMV (EMVCo [2004]) で採用されている 2-key トリプル DES が広く利用されているとみられる。

公開鍵暗号・デジタル署名としては RSA、DSA、ECDSA が挙げられるが、ISO 9564 シリーズをはじめとする ISO/TC68 のほとんどの標準に規定されている RSA が広く利用されているとみられる。

鍵長については、情報セキュリティ・ガイドライ

表1 金融分野で利用されている暗号アルゴリズム

国際標準等	共通鍵暗号	公開鍵暗号	ハッシュ関数
ISO 16609 (MAC の要件)	DES, トリプルDES	(記載なし)	(記載なし)
ISO/TR 13569 (情報セキュリティ・ ガイドライン)	鍵長 80 ビット 以上	鍵長 1024 ビット以上 (楕円曲線暗号は 160 ビット以上)	(記載なし)
ISO 11568-2 (鍵管理: 共通鍵暗号)	トリプルDES	(記載なし)	(記載なし)
ISO 11568-4 (鍵管理: 公開鍵暗号)	(記載なし)	RSA, DSA	ISO/IEC 10118-2, 4 に規定
ISO 9564-2 (PIN 暗号化)	トリプルDES (鍵長 112 ビット以上)	RSA	(記載なし)
ISO/TR 19038 (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】 EMV v.4.1	2-key トリプルDES	RSA(鍵長 1984 ビット以下)	SHA-1
【参考】 FINREAD	DES, トリプルDES	RSA(鍵長 1024 ビット以下)	SHA-1, MD5 RIPEMD-160

ン ISO/TR 13569 (ISO [1998]) において 1024 ビット以上が推奨されていることや、EMV のセキュリティ・ガイドライン (EMVCo [2005]) では 2009 年末までの利用を想定する場合に 1024 ビットが推奨されていることから、1024 ビット RSA が利用されるケースが多いとみられる。

ハッシュ関数は、SHA-1 がハッシュ関数に関連する ISO/TC68 の標準すべてに規定されている。

また、インターネット上での金融取引では、IETF 標準の暗号通信プロトコルも利用されるケースが多いとみられる。例えば、最も一般的な暗号通信プロトコルである SSL version 3.0/TLS version 1.0 (Blake-Wilson et al. [2003])²ほか) で採用されている暗号アルゴリズムとしては、トリプルDES, RSA, SHA-1 のほか、共通鍵暗号が DES, RC2, RC4, IDEA, AES, Camellia, SEED, 公開鍵暗号が DSA, Diffie-Hellman 鍵配送方式 (以下、DH と呼ぶ)、ハッシュ関数が MD5 となっている。このうち、共通鍵暗号では特に RC4 が利用される場面が多いとみられている。

このほか、IETF が発行する文書に記載されているものとして、共通鍵暗号では MISTY1、公開鍵暗号では ECDSA, ECDH などが挙げられる。

3. 暗号アルゴリズムの安全性評価結果

前節で説明した暗号アルゴリズムの安全性に関して、本稿を執筆した平成 18 年 2 月末時点における評価結果を整理する。

3.1 共通鍵暗号

(1) ブロック暗号

トリプルDESは、2-keyと 3-keyのいずれも中間値一致攻撃²によって鍵全数探索法³よりも少ない計算量で秘密鍵の推定が可能との評価結果が示されている。特に、 2^{56} 個の平文・暗号文ペアを利用したときの攻撃に必要な計算量のオーダーが 2^{57} と試算されている 2-key トリプルDESは、CRYPTREC暗号技術評価報告書 (2002 年度版, IPA/TAO [2003]) において、その計算量に関して「現実的な意味でも解読可能な領域に達しつつある」とされている。

RC2 は、差分解読法⁴や関連鍵攻撃⁵によって鍵全数探索法よりも効率的に秘密鍵の推定が可能との評価結果が発表されている (IPA/TAO [2002])。

その他の 64 ビット・ブロック暗号 IDEA, MISTY1 については、筆者の知る限り、鍵全数探索法よりも効率的な攻撃法は提案されていない。

なお、64 ビット・ブロック暗号に対しては暗号文一致攻撃⁶に留意が必要とされている。暗号文一致攻撃の実行に必要なメモリ・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ためである。

128 ビット・ブロック暗号 AES, Camellia, SEED については、筆者の知る限り、鍵全数探索法よりも効率的に秘密鍵の推定が可能になる攻撃法は提

² 組み合わせ暗号 (DESを繰り返して構成するトリプルDESが代表例) に対する攻撃方法の一種

³ 秘密鍵の候補を一つずつ検査し、正しい秘密鍵を求める攻撃方法。原始的な手法ではあるが、理論上は必ず秘密鍵を求めることができるという意味で最も確実な攻撃方法でもある

⁴ 共通鍵暗号に対する最も強力な攻撃方法の一種

⁵ 鍵生成部の特性を考慮に入れたブロック暗号に対する攻撃方法の一種

⁶ ランダムに集めた暗号文のなかから一致するデータ組を利用した攻撃手法

案されていない。また、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みられている。

(2) ストリーム暗号

ストリーム暗号である RC4 は、無線 LAN での暗号通信プロトコルである WEP (Wired Equivalent Privacy) における利用形態で安全性上の問題点が指摘されている (吉田ほか [2005], Fluhrer [2002])。ただし、SSL version 3.0/TLS version 1.0 の標準的なパラメータ設定を行う限り、鍵全数探索法よりも効率的に秘密鍵の推定が可能になる攻撃法は提案されていないようである。

このため、電子政府推奨暗号リストにおいては、SSL/TLS の標準的なパラメータ設定以外での利用は推奨されていない。

3.2 公開鍵暗号

(1) 1024 ビット RSA

RSA のアルゴリズムを利用した暗号化や署名生成の手法としてさまざまな方式が提案されており、RSA-OAEP や RSA-PSS のように、攻撃者の能力等に関する一定の前提のもとで素因数分解の困難性との等価性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、そうした方式でも、素因数分解が現実的な資源と時間によって実行可能となれば、暗号文の解読や署名の偽造が可能になってしまう。つまり、1024 ビット RSA は、1024 ビット合成数の素因数分解の困難性に安全性を依拠している。

そこで、1024 ビット合成数の素因数分解がどれだけ難しいかが検討されているが、その結果からは、1024 ビット RSA が今後 10~15 年にわたって十分な安全性を確保することは難しいとの見方を示す研究成果が発表されている。

例えば、Brent [2000] は、2018 年頃には一般数体ふるい法によって 1024 ビット合成数が現実的に素因数分解可能になる領域に入る可能性があるとしている。Lenstra and Verheul [2001] は、1982 年時

点の DES の安全性を基準とすれば、2001 年から 20 年間の利用を想定した場合に 2048 ビット以上の鍵長を推奨している。NESSIE の評価では、512 ビットの素因数分解に必要な計算量が鍵長 56 ビットの共通鍵暗号 (DES の鍵全数探索法に対する安全性に相当) に対して鍵全数探索法を適用する際の計算量と等価になるとの前提のもとで、2003 年から 5~10 年の安全性を確保するためには 1536 ビット以上を推奨している (Preneel et al. [2004])。なお、欧州では、暗号技術の評価や研究の推進を目的としたプロジェクト ECRYPT (European Network of Excellence for Cryptology) が 2004 年から開始されており、NESSIE と同様のケースにおいて 1248 ビット以上を推奨している (Gehrmann and Naslund [2005])。

実際の計算機実験によれば、一般数体ふるい法による 663 ビットの合成数と、特殊数体ふるい法による 911 ビットの特種合成数⁷の素因数分解がそれぞれ成功している。これらの結果は Brent らの素因数分解可能な領域予測にほぼ一致している。

(2) DSA と DH

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。DSA は、証明可能安全性を有していないものの、擬似乱数等の運用上の留意点を除けば、筆者が知る限り、アルゴリズムに安全性上の致命的な欠陥は報告されていない。また、DH についても同様である。したがって、DSA と DH の安全性を考えるうえで離散対数問題の困難性がポイントとなる。

本問題解法への最速アルゴリズムとして、現時点では指数計算法が知られている。指数計算法は一般数体ふるい法と密接に関係しており、指数計算法で離散対数問題を解くために必要な計算量のオーダーは、鍵長を一定とすれば、一般数体ふる

⁷ ある性質を持った素数であることが事前に分かっている 2 つの素数の積からなる合成数

い法で素因数分解を行うための計算量と同程度になるとみられている。

そのため、DSA と DH の鍵長は RSA と同様に 1024 ビットに設定されるケースが多いとみられる。1024 ビット合成数の素因数分解に関する評価結果を考慮すると、同サイズの鍵長を利用している DSA や DH も鍵長見直しを検討することが求められているといえる。

(3) ECDSA と ECDH

ECDSA と ECDH は、有限体上で定義される楕円曲線の有理点の集合をベースとした離散対数問題（以下、楕円曲線離散対数問題と呼ぶ）の困難性に依拠している。ECDSA と ECDH も、証明可能安全性を有していないものの、筆者が知る限り、アルゴリズムに安全性上致命的な欠陥は報告されていない。

そこで、高速解法が存在が知られているある種の楕円曲線を除外したうえで、どの程度の鍵長であれば楕円曲線離散対数問題の困難性の観点で十分な安全性を確保できるかが問題となる。

ISO/TR 13569 に鍵長として規定されている 160 ビットに焦点を当てると、Lenstra and Verheul [2001]は、一定条件のもとで、2010 年の時点で 160 ビットによって十分な安全性を確保できると評価しているほか、NESSIE の評価でも、今後 5～10 年の間安全性を確保するために必要な鍵長を 160 ビット以上としている。一方、Certicom [2000]は、楕円曲線暗号における 160 ビット鍵長は RSA における 1024 ビット鍵長と同程度の安全性を意味するとしている。これらの評価はそれぞれ異なる前提のもとで行われたものであり、横並びでの比較は適切でないが、例えば、安全性に万全を期すならば、最も厳しい評価結果である Certicom の評価を参照するという考え方もある。

3.3 ハッシュ関数

SHA-1 では、同一の出力値となる異なる入力値

のペア（衝突と呼ばれる）を効率的に探索可能との研究結果が発表されている（Wang et al. [2005a, b]）。実際の衝突は現時点で報告されていないものの、安全性の観点からはより安全なハッシュ関数への移行が求められる。

MD5 については、実際に衝突する実験例が示されているうえ、衝突するデータとアプリケーションのデータフォーマットの利用したデジタル署名の偽造方法もすでに発表されている（Gebhardt et al.[2005]）。

4. NIST の方針

4.1 共通鍵暗号と公開鍵暗号

トリプル DES（SP 800-67 で推奨）、1024 ビット RSA（FIPS 186-2 で認定）、SHA-1（FIPS 180-2 で認定）を実際に米国連邦政府機関の情報システム向け暗号アルゴリズムとして認定または推奨してきた NIST は、より安全性が高いアルゴリズムに移行する方針を各種ガイドライン（SP シリーズ）において示している。

鍵管理方法に関するガイドライン SP 800-57 では、2010 年末までは 2-key トリプル DES と 1024 ビット RSA も推奨されている（NIST [2005a]、表 2 参照）。しかし、2030 年末までの利用を想定する場合はこれらの使用を推奨しておらず、共通鍵暗号としては AES または 3-key トリプル DES を、公開鍵暗号としては鍵長 2048 ビット以上の RSA 等を推奨している。なお、RC4 はもともと NIST が推奨する暗号アルゴリズムに含まれていない。

また、SP 800-78 は、米国連邦政府の職員等が政府機関の施設や情報システム等にアクセスする際に本人確認を行うシステムで使われる暗号アルゴリズムや鍵長を規定しており、SP 800-57 と概ね整合的な内容となっている（NIST [2005b]）。

4.2 ハッシュ関数

NIST は、2004 年 8 月、2010 年までに SHA-1 の

表 2 SP 800-57 における暗号アルゴリズム/鍵長の移行見通し

	2010 年末 までの使用	2030 年末 までの使用	年以降の使用
共通鍵暗号	AES, 2-/3-key トリプル DES	AES, 3-key トリプル DES	AES
公開鍵暗号 素因数分解 問題ベース	最小鍵長 1024 ビット	最小鍵長 2048 ビット	最小鍵長 3072 ビット
公開鍵暗号 離散対数問題 ベース	最小鍵長 1024 ビット (位数サイズは 160 ビット)	最小鍵長 2048 ビット (位数サイズは 224 ビット)	最小鍵長 3072 ビット (位数サイズは 256 ビット)
公開鍵暗号 楕円曲線離散 対数問題ベース	最小鍵長 160 ビット	最小鍵長 224 ビット	最小鍵長 256 ビット

使用をとりやめて SHA-224, SHA-256, SHA-384, SHA-512 に移行することを検討している旨を発表していた (NIST [2004]). その後, SHA-1 への Wang らの攻撃が成功した 2005 年 2 月には, 正式に 2010 年までに SHA-1 の使用を終了させるため, 新たに構築されるシステムへはこれらのハッシュ関数の使用を推奨する旨の発表を行っている (NIST [2005c]).

実際に, SP 800-78 では, 2010 年末までは SHA-1, SHA-224, SHA-256 を, それ以降は SHA-224 と SHA-256 を推奨している.

5. 2010 年問題の金融業界への影響

NIST の評価結果は安全性上の「お墨付き」として様々な場面で活用されている。例えば, NESSIE では, AES を推奨暗号 (recommended algorithm) とした理由の中で NIST が詳細な評価を実施済みであることを指摘している。また, CRYPTREC による電子政府推奨暗号リスト (2005 年 2 月末時点で入手可能なもの) では, 3-key トリプル DES を本リストに記載する条件として, NIST による推奨 (SP 800-67) が挙げられている (総務省・経済産業省 [2003]).

したがって, 最近の NIST の評価結果やそれに基づく暗号アルゴリズムの移行方針が, 今後国際的にも大きな影響を与えることは容易に想像できる。そのことを考慮せずに, 金融機関が 2010 年頃までに暗号アルゴリズムを移行しなかったとする

と, 当該金融機関の情報システムにおける安全性レベルに対するレピュテーションが低下してしまう可能性がある。すなわち, 「現時点 (2005 年) において既に NIST が暗号アルゴリズムの移行スケジュールを明らかにしていたにもかかわらず, それに対応すべく迅速な検討を行わなかった」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受け止められる可能性がある。

6. 2010 年問題への対応

6.1 暗号アルゴリズムと鍵長

2011 年以降使用する暗号アルゴリズムとその鍵長としては, NIST が認定あるいは推奨しているものを採用するという方法がまず考えられる。また, 暗号研究者らによる第三者的な組織・プロジェクト, 具体的には CRYPTREC と NESSIE によって推奨されている暗号アルゴリズムを参照することもできる。さらに, 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 が策定した守秘目的の暗号アルゴリズムの国際標準 ISO/IEC 18033 を参照することも可能である (ISO/IEC [2005a, b, c]).

各機関・プロジェクトで選択されている暗号アルゴリズムは, 表 3 のとおりである。

6.2 暗号アルゴリズムを選択する際の主な論点

新しく採用する暗号アルゴリズムとその鍵長を選択するうえで論点となりうる項目を整理する。

まず, 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 (論点 1), 同一の暗号アルゴリズムであっても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 (論点 2) が問題となる。

具体的には, ISO/IEC 18033, NIST の FIPS と SP, CRYPTREC, NESSIE の評価結果のうち, どれを重視するかを決める必要がある。その際, 各機関・プロジェクトが採用している評価基準にも留意す

表3 各機関・プロジェクトにおいて選択されている暗号アルゴリズム/鍵長

	NISTのFIPS/SP ^(1,2)	電子政府推奨暗号リスト	NESSIEによる推奨暗号	ISO/IEC 18033	
公開鍵暗号	デジタル署名	RSA(2048ビット) DSA(2048ビット) ECDSA(224ビット)	RSA-PSS, RSASA-PKCS1-v1_5 (以上, 1024ビット) DSA(1024ビット) ECDSA(160ビット)	RSA-PSS(1536ビット) ECDSA(160ビット) SFLASH	(記載なし, ISO/IEC 9796-2 等において規定)
	守秘	(推奨なし)	RSA-OAEP, RSAES-PKCS1-v1_5 ^(3, 注1) (以上, 1024ビット) PSEC-KEM(鍵配送/160ビット) ^(3, 注2)	RSA-KEM(secondary/1536ビット) PSEC-KEM(primary/160ビット) ACE-KEM(special/160ビット)	RSA-KEM, RSA-OAEP PSEC-KEM ACE-KEM HIME(R) ECIES-KEM
	鍵配送	DH MQV	DH(1024ビット) ECDH(160ビット)	(推奨なし)	(記載なし, 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	3-key トリプルDES ^(3, 注3, 注4) MISTY1 ^(3, 注3) CIPHERUNICORN-E ^(3, 注3) Hierocrypt-L1 ^(3, 注3)	MISTY1	トリプルDES(3-key)を推奨 MISTY1 CAST-128
	128ビット・ブロック暗号	AES	AES Camellia CIPHERUNICORN-A Hierocrypt-3 SC2000	AES Camellia	AES Camellia SEED
	ストリーム暗号	(推奨なし)	MUGI MULTI-S01 RC4(128ビット) ^(3, 注5)	(推奨なし)	MUGI MULTI-S01(モードとして規定) SNOW 2.0
ハッシュ関数	SHA-(224, 256, 384, 512)	SHA-(256, 384, 512) SHA-1 ^(3, 注6) RIPEMD-160 ^(3, 注6)	SHA-(256, 384, 512) Whirlpool	(記載なし, ISO/IEC 10118 において規定)	

備考：(1)NIST SP800-57 の Table 4 をベースに作成
(2)NIST の評価・認定結果の欄には2030 年未までの使用を想定したものを記述
(3) 電子政府推奨暗号リストにおいては以下の注釈が付記されている。
(注1) SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。
(注2) KEM(Key Encapsulation Mechanism)-DEM(Data Encapsulation Mechanism) 構成における利用を前提とする。
(注3) 新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使用できるのであれば、128 ビットブロック暗号を選択することが望ましい。
(注4) 3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。1) SP800-67 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
(注5) 128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。
(注6) 新たな電子政府用システムを構築する場合、より長いハッシュ値のもので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。
(4) 鍵配送における“DH”は Diffie-Hellman 方式を、“MQV”は Menezes-Qu-Vanstone 方式を意味する。

るべきである。例えば、CRYPTREC では、電子政府推奨暗号リストが公表された時点での調達可能性にも配慮されており、鍵長が他の推奨鍵長よりも相対的に短めに設定されているとみられるものもある。

こうした点を踏まえ、当該アプリケーションに依存する様々な要素を加味して最適な鍵長を選択することが求められる。

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(論点3)も論点となる。例えば、ICカード等比較的計算能力が低い計算機で実装することが想定され、処理速度の低下をなるべく抑えなが

ら一定の安全性のレベルを達成したいケースも考えられる。

この場合、どの程度の処理速度の低下であれば許容できるかを検討したうえで、同程度の安全性を確保可能なもの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。

公開鍵暗号の移行を検討する場合、KEM や DEM を採用するか否か(論点4)が論点となる。

KEM-DEM 構成は、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・一貫性を同時に証明可能にするという特徴を有する。また、ISO/IEC 18033-2 等にも採用され、今後幅広い分野で利用されるよ

うになる可能性も出てきている。こうした点を踏まえ、KEM や KEM-DEM 構成に基づく方式も選択肢の1つとして検討することが考えられる。

共通鍵暗号については、64 ビット・ブロック暗号と 128 ビット・ブロック暗号、ストリーム暗号のどれを選択するか（論点5）が論点となる。

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 推奨暗号から外れていること、電子政府推奨暗号リストにおいて 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とを踏まえると、128 ビット・ブロック暗号の採用をまず検討することになると考えられる。

ストリーム暗号は、高速処理が可能であり、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、NIST と NESSIE では認定あるいは推奨されておらず、ブロック暗号に比べて安全性評価手法が確立していないことも考慮すると、まずブロック暗号を検討対象とするのが自然と考えられる。

ハッシュ関数に関しては、ハッシュ値のサイズをどのように決めるか（論点6）が論点となる。

すなわち、SHA-224、SHA-256、SHA-384、SHA-512 のうちどれを選択するかが検討項目となり、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検討する必要がある。ただ、2005 年 10 月にハッシュ関数のワークショップが NIST によって開催され、様々な議論が席上行われたことからわかるように、NIST が上記 SHA シリーズを中長期的に採用するか否かは不透明であり、新たなハッシュ関数を推奨あるいは認定する可能性も否定できない。

6.3 システム仕様変更時の留意点

これらのほか、暗号アルゴリズムの移行に伴って情報システムの仕様を変更する際には、当該情報システムと接続している他のシステムとの相互運用性にも配慮する（留意点 1）ことが求められ

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も多く、暗号アルゴリズムの移行が他の情報システムに与える影響を見極めることが重要である。また、他の金融機関と事前に必要に応じて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、相互運用性への影響をなるべく小さくする取組みが重要である。

また、移行後の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を使用できないようにするための設定変更も行う（留意点 2）ことが求められる。やむを得ず複数の暗号アルゴリズムを利用する場合、たとえ同種の暗号技術であっても鍵情報を共用しない（留意点 3）ようにする必要があると考えられる。

6.4 中期的な検討課題

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をどのように整備するかに関して、個別の金融機関として、また、金融業界全体としても今後検討することが望まれる。

具体的には、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構築する（課題 1）ことが求められよう。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、こうした体制を整備することは容易ではないが、金融という公共性の高い分野であることも踏まえ、地道かつ積極的に対応していくことが求められているといえる。

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等での「拡張性」を有する情報システムを実現する（課題 2）という方向性も重要である。

具体的には、容易に交換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等がまず考えられる。また、安全性上の特性が異なる複数の暗号アルゴリズムを実装しておくという手法も考えられる。例えば、計算量的な安全性に基づく方式のほかに情報量的な安全性に基づく方式の活用を検討するといった方向性も考えられる。

7. おわりに

本稿では、暗号アルゴリズムの2010年問題の概要を説明し、金融分野への影響と対応のあり方について考察した。今後、金融業界において本問題に関する議論が活発化し、具体的な対応の検討が早急に行われることを期待したい。

【参考文献】

- 宇根・神田, 暗号アルゴリズムの2010年問題について, 「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」, No. 2005-J-22, 2005年
- 総務省・経済産業省, 「電子政府推奨暗号リスト」, 2003年
- 吉田・古原・今井, 最新の商品における 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
- S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen and T. Wright, *RFC 3546: Transport Layer Security (TLS) Extensions*, 2003.
- R. Brent, “Recent progress and prospects for integer factorization algorithms,” *Proceedings of COCOON 2000*, LNCS 1858, Springer-Verlag, pp.3-20, 2000
- Certicom Research, *SEC 1: Elliptic Curve Cryptography, Version 1.0*, 2000.
- 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.
- C. Gehrman and M. Naslund, *ECRYPT Yearly Report on Algorithms and Keysizes (2004)*, 2005.
- S. Fluhrer, I. Mantin and A. Shamir, “Attacks on RC4 and WEP,” *CryptoBytes*, 5 (2), 2002.
- IPA and TAO, *CRYPTREC Report 2001*, 2002.
- --- and ---, *CRYPTREC Report 2002*, 2003.
- ISO, *ISO/TR 13569: Banking and related financial services – Information security guidelines, Amendment 1*, 1998.
- ---, *ISO 9564-2: Banking – Personal Identification – Number management and security – Part 2: Approved algorithms for PIN encipherment*, 2005.
- --- and IEC, *ISO/IEC 18033-2: Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*, 2005a.
- --- and IEC, *ISO/IEC 18033-3: Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*, 2005b.
- --- and IEC, *ISO/IEC 18033-4: Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers*, 2005c.
- A. K. Lenstra and E. R. Verheul, “Selecting Cryptographic Key Size,” *Journal of Cryptology*, 14 (4), pp. 255-293, 2991.
- NESSIE Consortium, *Portfolio of recommended cryptographic primitives*, 2003.
- NIST, *SP 800-57: Recommendation on Key Management*, 2005a.
- ---, *SP 800-78: Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, 2005b.
- ---, *NIST Brief Comments on Recent Cryptanalytic Attacks on Secure Hashing Functions and the Continued Security Provided by SHA-1*, 2004.
- ---, *NIST Brief Comments on Recent Cryptanalytic Attacks on SHA-1*, 2005c.
- B. Preneel, A. Biryukov, C. De Canniere, S. B. Ors, E. Oswald, B. V. Rompay, L. Granboulan, E. Dottax, G. Martinet, S. Murphy, A. Dent, R. Shipsey, C. Swart, J. White, M. Dichtl, S. Pyka, M. Schafheutle, P. Serf, E. Biham, Y. Braziler, O. Dunkelman, V. Furman, D. Kenigsberg, J. Stolin, J.-J. Quisquater, M. Ciet, F. Sica, H. Raddum, L. Knudsen and M. Parker, *Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, Version 0.1 (beta)*, 2004.
- X. Wang, A. Yao and F. Yao, “New Collision Search for SHA-1,” *Presentation of Rump Session of CRYPTO 2005*, 2005a.
- X. Wang, Y. L. Yin and H. Yu, “Finding Collisions in the Full SHA-1,” *Proceedings of CRYPTO 2005*, LNCS 3621, Springer-Verlag, pp. 17-36, 2005b.
- M. Gebhardt, G. Illies, and W. Schindler, “A Note on the Practical Value of Single Hash Collisions for Special File Formats,” *Proceedings of Cryptographic Hash Workshop*, 2005.