■11 群（社会情報システム）－ 7 編（金融情報システム）

2 章 金融情報システムに利用される暗号技術

（執筆者：宇根正志）［2009 年 3 月 受領］

■概要■

金融分野では，重要なデータの機密性や一貫性を確保するために暗号アルゴリズムが利用されており，例えば，キャッシュカード取引における IC カード認証，PIN 認証や銀行のホスト・コンピュータと営業店端末間の伝送データの保護などがあげられる．各金融機関が具体的にどのような暗号アルゴリズムを利用しているかについては，安全性の観点から公開されていないケースが多いが，金融分野における情報セキュリティ技術の国際標準や海外の各種ガイドラインを参照すると，2-key トリプル DES，公開鍵長を 1 024 ビットとする RSA（以下，1 024 ビット RSA と呼ぶ），SHA-1 が主流になっているとみられる．

これらの暗号アルゴリズムは，今後のコンピュータのコスト・パフォーマンス向上や暗号解読技術の進展を前提とすると，中・長期にわたって十分な安全性を確保することが難しいとの見方が暗号研究者のなかで一般的となっている．特に，米国立標準技術研究所（NIST：National Institute of Standards and Technology）は，これらを米国連邦政府機関の情報システムで中・長期的に使用しない方針を SP800-57 などの各種ガイドラインで示している．

金融分野においては，現行の暗号アルゴリズムを今後どのように移行していくかが重要な問題となっており，本問題への対応のあり方について検討が進められている．金融サービスを対象とする国際標準化機構（ISO）の専門委員会である ISO/TC68 では，暗号アルゴリズムの移行に関する検討が 2005 年以降行われており，2007 年には ISO/TC68 としての推奨対応策が取りまとめられた．本内容はおおむね NIST による方針と整合的なものとなっているが，2-key トリプル DES については，暗号アルゴリズムの移行にかかるコストも考慮した検討の結果，一定の状況下では 2030 年末まで使用可能とされた．

我が国においても，CRYPTREC（Cryptography Research and Evaluation Committees）による電子政府推奨暗号リストが 2013 年に改訂される見通しであるほか，内閣官房情報セキュリティセンター（NISC：National Information Security Center）は政府機関の情報システムにおける 1 024 ビット RSA と SHA-1 の移行指針案を 2008 年 2 月に発表するなど，暗号アルゴリズム移行に向けた取り組みが進められている．

暗号アルゴリズムの移行に関する問題は，現時点で暗号アルゴリズムを利用している金融機関に関係するほか，今後新規に暗号アルゴリズムの採用を検討する際にも将来的な暗号アルゴリズム移行に備えたシステム設計や手続のあり方など，考慮すべき論点を含んでいる．我が国の金融機関においても，ISO/TC68 などの対応を参考にしつつ，個々のアプリケーションに応じてリスク分析を行い，必要な対応のあり方を自ら検討していくことが求められる．本章では，宇根・神田論文[1)]を参照しつつ，暗号アルゴリズムの移行に関する現状を説明する．

【本章の構成】

本章では，金融分野の国際標準や各種ガイドラインに記述されている暗号アルゴリズムを説明し（2-1 節），共通鍵暗号，公開鍵暗号，ハッシュ関数における安全性評価結果を説明す

る（2-2 節）．そのうえで，NIST や ISO/TC68 による推奨対応策， 我が国の電子政府などの動向について説明しつつ，今後の暗号アルゴリズムの移行に関する検討課題を整理する（2-3 節）．

■11 編 － 7 編 － 2 章

2-1 現在主流となっている暗号アルゴリズム

（執筆者：宇根正志）［2009 年 3 月 受領］

2-1-1 国際標準やガイドラインなど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利用されている暗号アルゴリズムとして，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 の国際標準やそのほかの各種ガイドラインを参照すると，**表 2･1** のとおりである．

共通鍵暗号に関しては，トリプル DES が中心となっている．PIN の暗号化方法を規定する ISO 9564-1 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 でのトリプル DES が前提となっているほか，ISO 16609，ISO 11568， ISO TR 19038 においてもトリプル DES が規定されている．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．また，国際標準ではないが，2007 年 11 月に ISO/TC68 が取りまとめた暗号アルゴリズムの移行推奨策に関するスタンディング・ドキュメント [2] においては，2-key トリプル DES からより安全性の高いアルゴリズムへの移行について記述されており，2-key トリプル DES がデファクト標準として普及している現状を示唆している．

公開鍵暗号に関しては，関連する多くの ISO/TC68 の国際標準に，素因数分解問題の困難性に依拠する暗号アルゴリズムである RSA が規定されている．鍵長については，具体的な数値を規定した国際標準はみられないが，暗号アルゴリズムの移行推奨策に関するスタンディ

表 2･1 ISO/TC68 の主な国際標準など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	暗号アルゴリズム
ISO 16609（MAC の要件）	【共通鍵暗号】DES，トリプル DES
ISO TR 17944 （セキュリティ管理の枠組み）	【共通鍵暗号】トリプル DES（ANS X9.52），AES（FIPS 197） 【公開鍵暗号】RSA（ANS X9.31），DSA（ANS X9.30-1），ECDSA（ANS X9.62） 【ハッシュ関数】ISO/IEC 10118 に規定されているもの．
ISO 11568-2, 4（鍵管理）	【共通鍵暗号】トリプル DES 【公開鍵暗号】用途によって異なるアルゴリズムを規定． ・鍵配送：RSA，ECIES-KEM（ISO/IEC 18033-2） ・鍵共有：Diffie-Hellman（ANS X9.42），EC-Diffie-Hellman，EC-MQV（以上 ISO/IEC 15946-3） ・ディジタル署名：RSA（ISO/IEC 9796-2），DSA，ECDSA（以上，ISO/IEC 14888-3） 【ハッシュ関数】ISO/IEC 10118 に規定されているもの．
ISO 9564-1, 2（PIN の暗号化）	【共通鍵暗号】トリプル DES 【公開鍵暗号】RSA（EMV2000 仕様）
ISO TR 19038 （トリプル DES 利用モード）	【共通鍵暗号】トリプル DES
【参考】全銀協 IC キャッシュカード標準仕様（第 2 版）	【共通鍵暗号】DES，トリプル DES 【公開鍵暗号方式】RSA 【ハッシュ関数】SHA-1
【参考】EMV 仕様（version 4.2）	【共通鍵暗号】2-key トリプル DES　【ハッシュ関数】SHA-1 【公開鍵暗号】RSA（ISO/IEC 9796-2，鍵長は 1984 ビット以下）

（備考）暗号アルゴリズムにおける括弧内の標準・ガイドラインは，当該アルゴリズムが準拠することが求められている標準・ガイドラインを表す．

ング・ドキュメントにおいては 1 024 ビット RSA からの移行について記述されており，1 024 ビットの RSA が主流となっているとみられる．また，RSA 以外のアルゴリズムについては，公開鍵暗号の鍵管理に関する国際標準である ISO 11568-4 において用途別にいくつか規定されている．鍵共有用途として，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）の困難性に依拠する Diffie-Hellman 鍵共有方式（DH），有限体上で定義される楕円曲線上の離散対数問題（以下，楕円曲線上の離散対数問題）の困難性に依拠する EC-Diffie-Hellman 鍵共有方式（ECDH）と EC-MQV が規定されている．鍵配送用途としては，ECIES-KEM が規定されている．ディジタル署名用途としては，離散対数問題の困難性に依拠する DSA と楕円曲線上の離散対数問題の困難性に依拠する ECDSA が ISO/TR 17944 と ISO 11568-4 に規定されている．

ハッシュ関数に関しては，ISO 11568-4 と ISO TR 17944 において，汎業界向けのハッシュ関数の国際標準である ISO/IEC 10118 シリーズに規定されているものを採用することが規定されている．金融分野では，同シリーズにも規定されているハッシュ関数 SHA-1 が主流とみられており，暗号アルゴリズムの移行推奨策に関するスタンディング・ドキュメントにおいても，SHA-1 からより安全性の高いハッシュ関数への移行について主に記述されている．

これらのほか，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，IC カードの業界標準である EMV 仕様（version 4.2）をみると，上記と同様の傾向にあることが分かる．EMV のセキュリティ・ガイドラインには，EMV 仕様に準拠した IC カードに実装する RSA の推奨鍵長が記述されており，1 024 ビットの鍵の使用が 2012 年末まで推奨されているほか，1 152 ビットの鍵の使用が 2015 年末まで，1 408 ビットと 1 984 ビットの鍵の使用が 2018 年末までそれぞれ推奨されている．

このように，上記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，共通鍵暗号としては 2-key トリプル DES，公開鍵暗号としては 1 024 ビット RSA，ハッシュ関数としては SHA-1 がそれぞれ金融分野において広く利用されていると考えることができる．

2-1-2 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）として IETF（Internet Engineering Task Force）の RFC に規定されており，TLS の最新のバージョンは 1.2 となっている [3]．SSL version 3.0/TLS version 1.2 において利用される暗号アルゴリズムとしては，共通鍵暗号方式が DES，トリプル DES，IDEA，AES，Camellia，SEED，RC4，公開鍵暗号方式が RSA，DSA，ECDSA，DH，ECDH，ハッシュ関数が SHA-1，SHA-256，SHA-384，SHA-512，MD5 となっている．共通鍵暗号方式については，トリプル DES，RC4，AES が利用されるケースが多いほか，公開鍵暗号方式については，鍵長として 1 024 ビットを採用するケースが多いとみられている [4]．ハッシュ関数については，MD5 や SHA-1 が利用されるケースが多いとみられている．

■11 編 － 7 編 － 2 章

2-2 主要な暗号アルゴリズムの安全性評価結果

（執筆者：宇根正志）［2009 年 3 月 受領］

2-2-1 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）に分けられる．ブロック暗号は，平文を一定のサイズの「ブロック」と呼ばれるデータに区切り，ブロックごとに暗号化する．ストリーム暗号は，平文のサイズと同じサイズの鍵ストリームと呼ばれる擬似乱数を生成し，鍵ストリームと平文の排他的論理和によって暗号化する．以下では，前節で紹介した DES，トリプル DES，IDEA，AES，Camellia，SEED（以上がブロック暗号），RC4（ストリーム暗号）の安全性評価結果を説明する．

(1) ブロック暗号

(a) ショート・カット攻撃

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・カット攻撃は暗号アルゴリズムの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，各アルゴリズムの構造に依存する．本稿執筆時点では，トリプル DES，IDEA，AES，Camellia，SEED（DES を除く）のいずれにおいても，鍵を一つ一つしらみつぶしに試す全数探索攻撃よりも効率的なショート・カット攻撃は発表されていないようである．

(b) ブルート･フォース攻撃

ブルート・フォース攻撃は，暗号鍵の候補を一つず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．64 ビット・ブロック暗号のトリプルDESの場合，基本的に，2^m個の平文・暗号文ペアを入手すれば，2-keyでも 3-keyでも全数探索攻撃より少ない計算量（それぞれ 2^{112-m}，2^{168-m}）で暗号鍵を推定可能となることが知られている．本攻撃の実行可能性は攻撃者が入手する平文・暗号文ペアの量に依存するが，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との評価が主流である．また，IDEAについては，全数探索攻撃より強力なブルート・フォース攻撃は発表されていないようである．ただし，これらの暗号アルゴリズムはブロック長が 64 ビットと比較的短く暗号文一致攻撃[1]に留意する必要があり，攻撃に必要なメモリ・サイズが約 32 ギガ・バイトと実現困難とはいえなくなりつつある．

128 ビット・ブロック暗号の AES，Camellia，SEED に関しては，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の調達は困難と考えられることから，128 ビット・ブロック暗号は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．

[1] 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，それらのなかから同一の暗号文となるものを探索し，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，一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を高い確率で発見できることとなる．

(2) ストリーム暗号

RC4 については，鍵ストリームが特定のビット・パターンをもつ確率の偏りを手がかりに鍵ストリームを効率的に推定するという攻撃法（内部状態復元攻撃）が提案されている．最近では，鍵長が 128 ビットの RC4 において，2^{112} のオーダーの内部状態に関するデータを用いると 2^{114} のオーダーの計算量によって鍵ストリームを推定可能との研究成果が知られている [5]．ただし，本攻撃法は現実的な脅威とはいえない．一方，無線 LAN で利用されている暗号通信プロトコル WEP（Wired Equivalent Privacy）における RC4 の利用形態については，約 3 万個の暗号化パケットを入手できれば，2^{20} 回の（RC4 における）鍵セットアップ処理と等価な計算量によって約 50%の確率で 104 ビットの WEP 鍵を推定可能であるとの研究成果が最近発表されている [6]．

2-2-2 公開鍵暗号

公開鍵暗号として，ここではRSA，DSA，DH，ECDSAを取り上げて説明する[2]．

(1) RSA（素因数分解問題の困難性評価）

大きな合成数の素因数分解が困難であることに依拠する RSA は，守秘方式として PKCS#1 version 1.5 や OAEP があげられるほか，署名方式として PSS や ISO/IEC 9796 シリーズがあげられるなど，方式にはいくつかのバリエーションがある．これらのなかには，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であることを証明可能な「証明可能安全性」を有しているものがある．そうした方式の安全性を評価する際には，素因数分解問題の困難性の評価がまず必要となる．

1 024 ビット合成数の素因数分解の困難性については，最近の CRYPTREC の評価結果 [7]が参考になる．本評価では，一定の仮定のもとで，「法パラメータのサイズが 1 024 ビットの IFP（$n=pq$ 型素因数分解問題）を 1 年間の計算によって完了されるためには，（中略），高性能なスーパーコンピュータが過去の成長率を続けて成長した場合に，そのレベルに達成する時期は 2010 年～2020 年の間と推定することができた」として，「法パラメータ $n=pq$ のサイズが 1 024 ビットである $n=pq$ 型 IFP は強い安全性を求められる利用には有効とは言えない」と評価している．更に，「仮に専用ハードウェア装置の実装が可能となった場合には，攻撃可能となる時期がソフトウェア処理による場合よりも更に早まる可能性がある」としている．

(2) DSA と DH（離散対数問題の困難性評価）

ディジタル署名方式である 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本稿執筆時点で発表されていないようである．鍵配送方式である DH についても，本アルゴリズム自体の安全性に着目した場合，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ようである．

DSA と DH の安全性は，離散対数問題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

[2] 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．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みられているため，ここ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．

して様々な手法が提案されている．指数計算法は，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おり，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一般数体ふるい法と同程度と評価されている．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．DSA や DH においても 1 024 ビットの鍵長が利用される場面が多く，1 024 ビット RSA と同様の状況となっているとみられている．

(3) ECDSA（楕円曲線上の離散対数問題の困難性評価）

ECDSA は，本稿執筆時点では本方式の安全性に関して致命的となる攻撃法が提案されておらず，安全性を評価する際には楕円曲線上の離散対数問題の困難性に着目することが妥当と考えられる．楕円曲線上の離散対数問題には指数計算法が適用困難であることが知られている．楕円曲線の種類によっては独自の高速解法が適用可能なケースもあり，そうした楕円曲線を選択しないようにすれば，鍵長をどのように設定するかが安全性を左右する．現時点では，鍵長（有限体の位数のサイズ）を 160 ビットに設定するケースが多いとみられている．

160 ビットの楕円曲線上の離散対数問題に関しては，解読アルゴリズムの進歩（18 か月で計算量が半減する）を想定すると，2010 年の時点で，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（長期的に十分な安全性を確保できる）との試算結果が知られている [8)] ほか，2004 年の時点から中期的に安全性を確保するために必要な鍵長を 160 ビットと評価する研究成果もある．また，2000 年時点におけるサーティコム社の試算では，160 ビットの ECDSA の安全性が 1 024 ビットの RSA や DSA の安全性と同等であり，2011 年以降も中期的に安全性を確保するには鍵長を 224 ビット以上とする必要があるとしている．

2-2-3 ハッシュ関数

ハッシュ関数 SHA-1 については安全性上の問題が既に指摘されている．ハッシュ関数の安全性評価では，同じ出力となる（異なる）入力のペア（衝突ペア）の計算困難性（衝突計算困難性）がポイントとなるが，SHA-1 の場合，2^{63} 回程度のハッシュ関数演算と同程度の計算量で衝突ペアの計算が可能との見解がワン（Wang）らによって示された [9)]．安全な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 $2^{(n/2)}$個のハッシュ値（n はハッシュ値のサイズのビット値）を集める必要があるが，160 ビットのハッシュ値を有する SHA-1 では，この計算量は $2^{(n/2)}= 2^{80}$ となり，ワンらによる試算の方が効率的に衝突計算を実行可能となり，安全性とはいえないとの評価結果となる．

SHA-1 の衝突計算困難性に加え，ハッシュ関数の安全性の別の評価項目である第 2 原像計算困難性[3]や原像計算困難性[4]の評価結果が最近発表されている．安全なハッシュ関数の場合，これらは 2^nとなるが，例えば，入力値が 2^{64} 程度と比較的大きな場合，SHA-1 において 2^{109} の計算量で第 2 原像を探索可能と評価されているほか，45 ステップに縮退したSHA-1 の場合，2^{159} の計算量で探索可能との見積りも示されている．また，34 ステップに縮退したSHA-1 の場合，$2^{153.5}$ の計算量で原像を探索可能と評価されている．

[3] 与えられた入力 x に対して，$H(x)=H(x')$を満たす別の入力（第 2 原像）x' $(\neq x)$を探索困難であること．
[4] 与えられたハッシュ値 y に対して，$y=H(x)$を満たす入力（原像）x を探索困難であること．

■11 編 － 7 編 － 2 章

2-3 暗号アルゴリズムの 2010 年問題への対応のあり方

（執筆者：宇根正志）［2009 年 3 月 受領］

2-3-1 各種機関・プロジェクトによる規定/認定/推奨

2-key トリプル DES，1 024 ビット RSA，SHA-1 は，安全性の観点から今後も中・長期的に利用を継続することが困難との見方が暗号研究者の間で一般的となっており，暗号アルゴリズムの世代交代が重要な問題となっている．こうした問題は，当初 NIST が 2010 年末までに上記の暗号アルゴリズムの利用を中止する旨を発表したことから，「暗号アルゴリズムの 2010 年問題」と呼ばれている．

(1) NIST による米国連邦政府標準暗号の移行

米国では，NIST が，米国連邦政府推奨暗号の利用に関するいくつかのガイドラインにおいて，暗号アルゴリズムの移行の方針を示してきた．これらの方針は，暗号アルゴリズムが適用されるアプリケーションによって若干異なるものの，基本的には，鍵管理のガイドラインである SP800-57 に示されている．本ガイドラインでは，攻撃に必要な計算量のオーダーが 2^n となる場合の安全性を「n ビット安全性（n-bits of security）」と呼んでおり，共通鍵暗号については秘密鍵探索の計算量，公開鍵暗号については暗号アルゴリズムの安全性が依拠する問題（素因数分解問題など）を解く計算量，ハッシュ関数についてはハッシュ関数を利用した用途（ディジタル署名など）への攻撃に必要な計算量をベースとしている．

表 2・2　SP800-57 における暗号アルゴリズムの使用推奨期間

n ビット安全性の N の値	共通鍵暗号	公開鍵暗号と鍵長			ハッシュ関数とハッシュ値のサイズ		使用推奨期間
		素因数分解問題ベース（RSA 等）	離散対数問題ベース（DSA 等）	楕円曲線上の離散対数問題ベース（ECDSA 等）	ディジタル署名用	HMAC，鍵生成関数，擬似乱数生成	
80	2-key トリプル DES	1 024	(1 024，160)	160～223	SHA-1	-----	～2010 年末
112	3-key トリプル DES	2 048	(2 048，224)	224～255	SHA-224	-----	～2030 年末
128	AES-128	3 072	(3 072，256)	256～383	SHA-256	SHA-1	2030 年超
192	AES-192	7 680	(7 680，384)	384～511	SHA-384	SHA-224	
256	AES-256	15 360	(15 360，512)	512～	SHA-512	SHA-256, 384, 512	

（備考）離散対数問題ベースの鍵長は，$y=g^x$ としたときの y と x のビット長をそれぞれ表す．

SP800-57 をみると（**表 2・2**），2-key トリプル DES，1 024 ビット RSA，SHA-1（ディジタル署名用）はいずれも 2010 年末までの使用が推奨されている．ハッシュ関数については，擬似乱数生成用であれば，SHA-1 を 2010 年以降も使用可能とされている．また，NIST は，SHA-1 から SHA-2 ファミリー（SHA-224，SHA-256，SHA-384，SHA-512）への移行に加え，SHA-2 ファミリーの次の世代のハッシュ関数として SHA-3 ファミリーを開発する方向で検討を進めている．現時点で発表されているスケジュールによれば，SHA-3 ファミリーは公募・選考によって 2012 年に米国連邦政府標準暗号として発表される予定である．

(2) ISO/TC68 における推奨対応策

こうした NIST の対応を受けて，ISO/TC68 は，金融分野で利用されている暗号アルゴリズムの移行への推奨対応策を検討し，検討結果をスタンディング・ドキュメントとして 2007 年に公表した [1]．同ドキュメントにおいては，ブロック暗号について，トリプル DES と AES の使用推奨期間が記述されている（**表 2･3**）．特に，2-key トリプル DES については，金融分野において広く利用されている現状を勘案し，攻撃者が入手する平文・暗号文のペア数に応じて使用推奨期間を設定している．具体的には，当該平文・暗号文ペア数が 2^8 程度の場合は 2030 年末まで，2^{24} 程度の場合は 2020 年末まで，2^{40} 程度の場合は 2010 年末までの使用を推奨している．3-key トリプル DES の安全性については，攻撃者が 2^{57} 程度の平文・暗号文ペアを入手するケースを想定し，2030 年末までの使用を推奨している．

表 2・3　ブロック暗号とその安全性評価に基づく使用推奨期間

暗号アルゴリズム	鍵長	*n* ビット安全性	使用推奨期間	攻撃者が入手する平文・暗号文ペア数
2-key トリプル DES	128 ビット	80 ビット安全性	～2010 年末	2^{40} 程度
		96 ビット安全性	～2020 年末	2^{24} 程度
		112 ビット安全性	～2030 年末	2^{8} 程度
3-key トリプル DES	192 ビット			条件なし
AES	128 ビット	128 ビット安全性	2030 年超	
	192 ビット	192 ビット安全性		
	256 ビット	256 ビット安全性		

公開鍵暗号については，メッセージ復元型ディジタル署名の国際標準である ISO/IEC 9796-2 と ISO/IEC 9796-3 の暗号アルゴリズム，メッセージ添付型ディジタル署名の国際標準である ISO/IEC 14888-2 と ISO/IEC 14888-3 の暗号アルゴリズム，守秘目的の公開鍵暗号の国際標準 ISO/IEC 18033-2 の暗号アルゴリズムが推奨対象となっている．さらに，これらの暗号アルゴリズムの使用推奨期間は，**表 2･4** のとおり，NIST の推奨とほぼ同一に設定されている．RSA については，暗号化の高速処理に対応して指数公開鍵 e が一般に小さく設定されるが，安全性上の問題から e の値として $2^{16}+1$ 以上の値を設定することが推奨されている．

表 2・4　公開鍵暗号の鍵長と使用推奨期間

公開鍵暗号とその鍵長			使用推奨期間
素因数分解問題ベース（RSA など）	離散対数問題ベース（DSA など）	楕円曲線上の離散対数問題ベース（ECDSA など）	
1 024	（1 024，160）	160～191	～2010 年末
1 536	（1 536，192）	192～223	～2020 年末
2 048	（2 048，224）	224～255	～2030 年末
3 072	（3 072，256）	256	2030 年超

（備考）離散対数問題ベースの鍵長は，$y=g^x$ としたときの y と x のビット長をそれぞれ表す．

ハッシュ関数については，ブロック暗号に基づくハッシュ関数の国際標準 ISO/IEC 10118-2，及び，SHA-1 をはじめとする専用ハッシュ関数の国際標準 ISO/IEC 10118-3 のハッシュ関数の使用推奨期間が記述されている．本スタンディング・ドキュメントでは，ブロック暗号に基づくハッシュ関数を利用する必要がない場合は専用ハッシュ関数を推奨するとしている（ブロック暗号に基づくハッシュ関数を利用する場合には AES が推奨されている）．

専用ハッシュ関数については，ISO/IEC 10118-3 規定の八つのハッシュ関数が記述されており，衝突計算困難性と第 2 原像計算困難性のそれぞれが求められるケースに分けて使用推奨期間が記述される形となっている（**表 2･5**）．

表 2･5　ハッシュ関数と使用推奨期間

ハッシュ関数 (ISO/IEC 10118-3)	ハッシュ値のサイズ	*n* ビット安全性	使用推奨期間	
			衝突計算困難性が求められるケース	第 2 原像計算困難性が求められるケース
RIPEMD-128	128 ビット	高々60 ビット安全性	推奨しない	～2020 年末
RIPEMD-160	160 ビット	80 ビット安全性	～2020 年末	～2030 年末
SHA-1		63 ビット安全性	～2010 年末	
SHA-224	224 ビット	112 ビット安全性	～2030 年末	2030 年超
SHA-256	256 ビット	128 ビット安全性		
SHA-384	384 ビット	192 ビット安全性	2030 年超	
SHA-512	512 ビット	256 ビット安全性		
WHIRLPOOL				

SHA-1 については，衝突計算困難性の観点から 63 ビット安全性との評価に基づき，使用推奨期間が 2010 年末までとされている．ただし，衝突計算困難性に安全性を依拠しているアプリケーションにおいて SHA-1 を利用している場合には，より安全性が高いと評価されている別のハッシュ関数への移行を早急に検討すべきであるほか，当該アプリケーションが依拠している安全性が明確でない場合には，衝突計算困難性に依拠する場合の使用推奨期間を前提とすることとされている．また，仮に 2010 年までに移行が完了しなかった場合には，危殆化の影響を軽減するための措置が検討する必要があるとしている．

(3)　CRYPTREC や NISC における対応

(a)　CRYPTREC による電子政府推奨暗号リストの改訂

CRYPTREC は，2003 年発表の電子政府推奨暗号リストを改訂し，新しいリストを 2013 年度頃に発表するとの方針を 2008 年に示した．具体的な改訂案としては，「電子政府推奨暗号リスト（仮称）」，「推奨暗号候補リスト（仮称）」，「互換性維持暗号リスト（仮称）」，「リストガイド」を策定し，これらをまとめて「CRYPTREC 暗号リスト（仮称）」とすることが予定されている．今後も継続して発生し得る暗号アルゴリズムの移行への対応としては，移行が求められる暗号アルゴリズムを「互換性維持暗号リスト（仮称）」として管理することが提案されている．これらのリストとリストガイドの役割は以下のとおりである．

- 電子政府推奨暗号リスト（仮称）：CRYPTREC によって安全性が確認され，かつ，市場において利用実績が十分である暗号アルゴリズムを掲載する．電子政府構築の際に推奨する暗号アルゴリズムとして位置づけられる．

- 推奨暗号候補リスト（仮称）：CRYPTREC によって安全性が確認されているが，市場において利用実績な十分でない普及段階にある暗号アルゴリズムを掲載する．電子政府構築の際に利用してもよい暗号アルゴリズムとして位置づけられる．
- 互換性維持暗号リスト（仮称）：電子政府推奨暗号リストに登録されていたが，実際に解読されるリスクが高まるなど，推奨すべき状態でなくなったもののうち，互換性維持のために継続利用を容認する暗号アルゴリズムを掲載する．暗号解読のリスクと，電子政府システムにおける移行コストなどを勘案して，定期的に掲載継続の可否が判断される．CRYPTREC として新規調達を推奨しない暗号アルゴリズムとして位置づけられる．
- リストガイド：電子政府で利用されている，あるいは，利用する可能性のある技術について，その技術概要と推奨する利用方法を記述する．また，次期リストに記載されたアルゴリズムのなかで，具体的なパラメータ設定方法の記述を行う．

(b) NISC によるガイドライン

NISC は，2008 年 4 月，我が国の政府機関の情報システムで利用する暗号アルゴリズムのうち，SHA-1 と 1 024 ビット RSA をより安全な暗号アルゴリズムへ移行するための指針を発表した．本指針では，政府認証基盤と商業登記認証局の情報システムの設計要件として，政府が発行する公開鍵証明書の生成・検証に利用する暗号アルゴリズムを複数のなかから選択できる構成として特定の時期に切替え可能とすることを示しており，暗号アルゴリズムには 2,048 ビット RSA と SHA-1 の組合せ，及び，2 048 ビット RSA と SHA-256 の組合せを含むこととされている．現時点で発表されているスケジュールでは，2008 年度中に必要な対応について検討を行い，2013 年度までに各情報システムに暗号アルゴリズムの移行を可能とする機構を組み込むこととなっている．

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

2-3-2 暗号アルゴリズムを選択する際の主な論点

(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

NIST や CRYPTREC の評価結果などのうち，どれを重視するか（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，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留意することが重要である．NIST 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，現在の CRYPTREC の評価は，基本的に安全性を重視しているほか，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．こうした違いを踏まえた検討が求められる．

(2) 暗号化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ける実装では，処理速度の低下を抑えつつ一定の安全性を達成したいというケースが考えられる．こうした状況では，処理速度などの実装性能を考慮しつつ，暗号アルゴリズムの選択を検討する必要がある．

(3) 公開鍵暗号において KEM や DEM を採用するか

ISO/TC68 のスタンディング・ドキュメントにおいては，鍵配送目的の公開鍵暗号の利用形態 KEM（key encapsulation mechanism）と，暗号化・復号処理を行う共通鍵暗号の利用形態 DEM（data encapsulation mechanism）が推奨に加えられている．こうした KEM や DEM は，鍵配送の安全性とメッセージの守秘性・一貫性に関する安全性をセットで証明可能であり，実装上の問題がなければ選択肢の一つとなりうる．ただし，ほかの金融機関の情報システムなど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への負担などにも配慮する必要がある．

(4) ブロック暗号においてブロック・サイズを 64 ビットと 128 ビットのどちらにするか

ISO/TC68 のスタンディング・ドキュメントにおいては，64 ビット・ブロック暗号と 128 ビット・ブロック暗号の 2 種類が推奨に含まれている．ただし，CRYPTREC の電子政府推奨暗号リストでは，「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」と記述されている．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，ISO/TC68 のスタンディング・ドキュメントをベースとして検討する場合には，AES の採用がまずは検討対象となる．

(5) SHA-1 からどのハッシュ関数に移行するか

SHA-1 は，衝突計算困難性に安全性を依拠するアプリケーションにおいて早期の対策実施が望まれる．別のハッシュ関数に移行するとすれば，SHA-2 ファミリーがまず候補となるほか，中・長期的にみると現在 NIST が開発を進めている SHA-3 ファミリーも候補に入ってくることになる．こうしたハッシュ関数が利用可能になりつつあるなかで，どのハッシュ関数に移行するかについて，アプリケーションに求められるハッシュ関数の安全性や処理速度，当該システムの使用期間などを勘案しながら検討する必要がある．

2-3-3 そのほかの留意点

(1) ほか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こと

金融機関の情報システムはほかの情報システムと連携しているケースが多い．例えば，ある銀行が自社の ATM のシステムの暗号アルゴリズムを別のものに移行した際に，当該銀行の IC キャッシュカードがほかの銀行の ATM で利用できなくなるといった状況が発生するおそれがある．そのため，暗号アルゴリズムの移行に伴う仕様変更が情報システムに与える影響を見極めるとともに，ほかの金融機関への影響に関しても事前に他の金融機関とシステム変更の内容を擦りあわせするなどして，影響をなるべく小さくする取組みも重要である．

(2) 移行前の暗号アルゴリズムを移行後には使用できないようにする設定変更も行うこと

例えば，サーバ側における SSL に関する設定が不適切な場合，128 ビット・ブロック暗号の暗号通信だけでなく，40 ビットや 56 ビットのブロック暗号の暗号化通信も可能になるおそれがある [3)]．このように，新しい暗号アルゴリズムを利用可能にするだけではなく，移行前の暗号アルゴリズムを使用できなくする設定変更を適切に実行する必要がある．

(3) 複数の暗号アルゴリズムを利用する場合には暗号鍵を共用しないこと

上記（a）のように，ほかの情報システムとの相互運用性を確保するために，複数の暗号アルゴリズムを分けて使用するケースがありうる．このようなケースにおいて，同じブロック暗号であるからといって複数の暗号アルゴリズムにおいて同じ暗号鍵を利用した場合，安全

性が相対的に低い暗号アルゴリズムによる安全性しか確保できないことにつながる．同じカテゴリーの暗号アルゴリズムでも，暗号鍵を共用することは安全性上問題が多いといえる．

2-3-4 中期的な検討課題

暗号アルゴリズムの 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をどのように進めるかを中期的に検討する必要がある．具体的には次の二つの課題があげられる．

(1) 暗号アルゴリズムの安全性評価や同評価を実施する機関・プロジェクトの動向を注視する体制を構築すること

暗号アルゴリズムの安全性に関する「お墨付き」がいつ失われるかが明確でない場合，金融機関自らが移行のタイミング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，先行きの安全性に関する見通しを常時検討しておく必要がある．そうした暗号アルゴリズムの評価動向を注視する体制を構築しておくことが重要である．

(2) 暗号アルゴリズムの危殆化に対して「拡張性」を有する情報システムを実現すること

例えば，入替えが容易な暗号モジュールによって暗号アルゴリズムを実装する，鍵長や暗号文のサイズ変更が容易な通信フォーマットを採用するなど，暗号アルゴリズムや鍵長を容易に変更できるように情報システムを設計・構築するという方法がある．また，異なる安全性上の特性をもつ複数の暗号アルゴリズムを実装するという方法も拡張性を付与する方法の一つである．計算量的な安全性に基づく方式のほか，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る．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．

■参考文献

1) 宇根正志・神田雅透，“暗号アルゴリズムにおける 2010 年問題について，”金融研究，vol.25，no.s1，pp.31-72，日本銀行金融研究所，2006.
2) ISO, “Financial services – Recommendations on cryptographic algorithms and their use – Standing Document,” ISO, 2007.
3) T. Dierks and E. Rescorla, “Request for Comments 5246: The Transport Layer Security (TLS) Protocol,” Version 1.2, Aug. 2008.
4) 神田雅透・山岸篤弘，“暗号世代交代についての暗号学会とビジネスサイドのギャップをどう埋めるか～SSL サーバの暗号設定の現状からの考察～，”2009 年暗号と情報セキュリティシンポジウム予稿集，4E2-4，電子情報通信学会，2009.
5) A. Maximov and D. Khovratovich, “New State Recovery Attack on RC4,” Proc. CRYPTO 2008, LNCS 5157, Springer-Verlag, pp.297-316, 2008.
6) R. Teramura, Y. Asakura, T. Ohigashi, H. Kuwakado, and M. Morii, “Breaking WEP with Any 104-bit Keys -All WEP Keys Can Be Recovered Using IP Packets Only-,” Proc. Symposium on Cryptography and Information Security 2009, 1A2-6, IEICE, 2009.
7) 情報通信研究機構・情報処理推進機構，“CRYPTREC Report 2006，”2007.
8) A.K. Lenstra and E.R. Verheul, “Selecting Cryptographic Key Size,” J. Cryptology, vol.14, no.4, pp.255-293, 2001.
9) X. Wang, A. Yao, and F. Yao, “New Collision Search for SHA-1,” Presentation at CRYPTO 2005 Rump Session 2005.