IMES DISCUSSION PAPER SERIES

Triple DESを巡る最近の標準化動向について

谷口文一・太田和夫・大久保美也子

Discussion Paper No. 99-J-6

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES
BANK OF JAPAN

日本銀行金融研究所

〒100-8630 東京中央郵便局私書箱203 号

IMES Discussion Paper Series 99-J-6
1999 年 3 月

Triple DES を巡る最近の標準化動向について

谷口 文一[*]・太田 和夫[**]・大久保 美也子[***]

要　旨

金融業界では、通信ネットワークを利用した金融取引の安全性を確保するために、暗号技術を広範に使用している。特に、DES（Data Encryption Standard）は、金融業界におけるニーズを背景として米国で開発された共通鍵暗号方式であり、米国政府標準に選定されたこと等を背景に、世界中で使用されてきた。しかし、近年、コンピュータの計算能力向上とコスト低廉化に伴い、DES の安全性低下が明らかとなってきている。このため、DES の後継として、DES を 3 回繰り返すことにより強度を高めた暗号である Triple DES への移行の動きが見られ始めている。

昨年末に、米国の金融業界では Triple DES に関する国内標準を作成した。これに伴い、Triple DES を米国政府標準や金融業務向けの国際標準に認定しようとする動きもある。こうした標準化作業の過程において、Triple DES の安全性に関する様々な検討が加えられている。本稿では、こうした Triple DES 標準化の動きを概観しつつ、その安全性を巡る議論を紹介する。

キーワード　暗号アルゴリズム、DES、Triple DES、AES、標準化、CBCM モード、ANSI X9

JEL classification: L86、Z00

[*] 日本銀行金融研究所 研究第 2 課（E-mail: fumikazu.taniguchi@boj.or.jp）
[**] NTT 情報流通プラットフォーム研究所（E-mail: ohta@isl.ntt.co.jp）
[***] NTT 情報流通プラットフォーム研究所（E-mail: mookubo@sucaba.isl.ntt.co.jp）

本稿は、電子情報通信学会主催の「1999 年暗号と情報セキュリティシンポジウム（SCIS'99）」への提出論文に加筆･修正を行ったものである。

目　　次

１．はじめに

DES（Data Encryption Standard）は、世界中で最も広範に利用されてきた暗号アルゴリズムである。特に金融業界は、機密度および重要度の高いデータを通信ネットワーク上でやり取りするために、DES を中心とする暗号技術を広範に利用してきた。そもそも DES は、こうした金融業界のニーズを背景として、1974 年に米国 IBM 社により開発されたものであった。1977 年に米国標準局（NBS：National Bureau of Standards）[1]が DES を米国政府標準（FIPS：Federal Information Processing Standard）として認定したことも、DES が金融業界で普及する大きな支援材料となった。金融業界は、欧米を中心に、DES を銀行間のオンラインシステムや CD/ATM における暗証番号（PIN：Personal Identification Number）の暗号化等に使用してきたほか、Fedwire、CHAPS、日銀ネット等の世界の主要な大口決済ネットワークにおいても採用されており、過去約 20 年の間、DES は名実ともに金融業界における標準暗号として利用されてきた。

しかし、近年、コンピュータの計算能力向上とコスト低廉化に伴い、入手した暗号文を候補となる全ての暗号鍵[2]で復号してみることによって真の鍵を探索する「全数探索法」に対する DES の安全性が低下しており、これに代わる暗号アルゴリズムが求められるようになってきた。現在、DES の後継として利用され始めているのは、DES を 3 回繰り返すことにより全数探索法への安全性を高めた Triple DES である。DES は全数探索法に対しては安全性が低下してきたものの、過去約 20 年間、世界中で利用されてきた中で、アルゴリズムとして致命的な欠陥は見つかっていない。このため、Triple DES は、その DES に対する信頼を活かすことにより、DES からのスムーズな移行を強く意識した暗号アルゴリズムである。実際、情報セキュリティへの要請の高い欧米の金融機関を中心に、既に DES を Triple DES 化する動きが見られる。

暗号アルゴリズムは高度な数学技術に依存していることが多いため、金融業界のような一般ユーザーはその安全性や暗号強度を十分評価することが困難である。したがって、暗号アルゴリズムを含む情報セキュリティについては、信頼できる機関が技術内容等について安全性を評価した結果として標準にふさわしい技術を明らかにすることにより、一般ユーザーもその技術を安心して使用することが可能となる。Triple DES に関しても、その利用の拡大に併せて金融業界に関するいくつかの標準化機関で標準化作業が進められており、基礎的な

---

[1] 米国内における科学技術全般の標準規格の策定を担当する米国商務省の下部組織であったが、1988 年に名称変更され、現在の NIST（National Institute of Standards and Technology）となった。

[2] 以降、単に「鍵」と表記する。

Triple DES の定義から各種応用分野における Triple DES の利用方法等まで、様々なプロジェクトが進行中である。今後、金融機関が Triple DES を利用していく際に、Triple DES の標準化を通じて検討された技術的な問題点について理解しておくことは有用であると考えられるため、本稿ではこれを紹介することとする。

本稿では、まず第 2 章で Triple DES の重要性が高まっている背景、第 3 章で Triple DES 化による暗号強度の向上について簡単に説明する。その後、第 4 章で DES を単純に Triple DES 化しただけでは暗号強度が改善しない場合があること、およびその対応法について説明し、第 5 章では対応法の一つである CBCM（Cipher Block Chaining with Output Feedback Masking）モードに対する攻撃法が発表されたために Triple DES の標準化作業が受けた事例について、その解読法の技術的詳細に触れながら説明する。最後に第 6 章では、現時点における Triple DES を巡る標準化動向について説明する。

２. Triple DES の重要性の高まり

（１）Single DES について

Single DES[3]は、これまで最も広範に利用されてきた暗号アルゴリズムである。特に、高額な資金決済や顧客の個人情報等の重要データを扱う金融業界においては、情報セキュリティへの要請が高い欧米の金融機関を中心として、データの漏洩や改竄を防ぐ目的で標準的に利用されてきた。

―― Single DES および Triple DES はデータの暗号化および復号に同じ鍵を用いる共通鍵暗号であり、暗号通信を行う前にデータの送信者と受信者が同じ鍵を共有している必要がある。一方、データの暗号化および復号に異なる鍵を用いる公開鍵暗号も実用化されつつある。公開鍵暗号は、処理速度が共通鍵暗号と比べて低速であることから、電子署名や鍵配送といった用途に利用されることが多い。このように、利用目的に応じて共通鍵暗号と公開鍵暗号を使い分ける必要がある。

―― 日本の金融機関は、セキュリティの確保に当たっては、コンピュータシステムおよびネットワークを外部から物理的に隔離することを重視してきたこと、金融ネットワークを対象とした犯罪がさほど多くなくセキュリティ対策に対する顧客の関心が低いこと等から、あまり暗号技術が採用されてこなかった（松本・岩下[1998]）。

Single DES が普及した主な理由として、以下の２つが挙げられる。

①米国政府標準暗号（FIPS46-2）として認定されたこと。

―― Single DES は標準暗号を定めるための公募に対して米国 IBM 社が提案した暗号方式が原形となって開発されたものであり、国家安全保障局（NSA：National Security Agency）[4]による変更提案を取り入れ、1977 年に NBS により米国政府標準暗号として認定された後、米国 IBM 社は Single DES の関連特許に対する権利の行使を放棄した。

②致命的な解読法が存在しない安全な暗号方式であると考えられてきたこと。

―― Single DES のアルゴリズムに対しては、20 年以上にわたって多くの暗号学者が解読を試みてきたが、今なお、致命的な効率的解読法（Short Cut Method）は見つかっていない。

そもそも、ブロック暗号の解読法には、大きく Brute Force Method と Short Cut Method に分類される。Brute Force Method は、全数探索法、暗号文一致攻撃（第 4 章で説明）、辞書攻撃（第 4 章で説明）等、全ての鍵の候補をしらみ潰しに試してみることにより真の鍵を見つけ出す方法であるのに対して、

---

[3] 本稿では、混乱を防ぐために、これ以降、単なる DES を Single DES と表記する。

[4] 国防総省の下部組織で、米国の暗号政策の企画立案や標準策定に強い影響力を持つと言われている。

Short Cut Method は、差分解読法、線形解読法等、暗号アルゴリズムの構造上の特徴や平文・暗号文の統計的偏りを利用して候補となる鍵の集合全体から真の鍵の候補を効率的に絞り込む方法である。Single DES の解読に関しては、差分解読法や線形解読法といった Short Cut Method は存在するものの、いずれも解読に必要となる平文・暗号文の組数が膨大であるため、現時点では現実的に致命的な解読法ではないと考えられている（第 3 章の表 1 参照）。しかし、近年、コンピュータ技術の向上と低価格化により、Brute Force Method のうち全数探索法により正しい鍵を見つけ出すための時間と所要費用が低下してきており、Single DES の安全性低下が指摘されてきた。

その安全性低下が現実となった象徴的な出来事は、1998 年 7 月に RSA 社が開催した懸賞金付 DES 解読コンテストにおいて、25 万ドルで製作された専用の暗号解読装置（DES Cracker）を用いて、全数探索法により Single DES が約 56 時間で解読（暗号文と平文の組から鍵を発見）されたと発表されたことである（Electronic Frontier Foundation[1998]）。また、その後 1999 年 1 月に行われた同コンテストでは、専用の暗号解読装置と約 10 万台のパソコンを用いて約 22 時間で全数探索法により解読されたと発表された。これらの出来事は、DES の安全性に対する不安を一層増加させ、Single DES に代わる暗号方式の必要性をより意識させることとなった。

（2）Triple DES について

Triple DES は IBM の Tuchman が 1979 年に提案した暗号方式であり、Single DES を 3 回繰り返すことにより、①鍵長の伸長（56bit[5]→112bit または 168bit）、②アルゴリズムの統計的偏りの減少（暗号化段数[6]の増加<16 段→48 段>）を図り、暗号強度を高めている。なお、Triple DES のブロックサイズは、Single DES と同様に 64bit である。一方、DES 処理を 3 回繰り返すことから、基本的には暗号化および復号に要する時間はそれだけ長くなる。

なお、図 1 のとおり、3 つの鍵が全て異なる場合を 3-key Triple DES、1 回目と 3 回目の Single DES に同じ鍵を用いる場合（図 1 で $K_1=K_3$）を 2-key Triple DES と呼ぶ。2-key Triple DES の場合、鍵長は 112bit、3-key Triple DES の場合、鍵長は 168bit である。また、Single DES を 3 回繰り返す際には、通常、図 1 のとおり 1 回目と 3 回目の Single DES では暗号化を、2 回目の Single DES では復号を行っている。これにより、3 つの鍵を全て同じにすれば（$K_1=K_2=K_3$）

[5] Single DES において実際に使用される鍵の長さは 64bit であるが、このうち 8bit はパリティビットであるため、鍵として利用可能なのは実質 56bit。

[6] 1 回の Single DES の中では、同じ暗号化処理を 16 回繰り返しているが、その暗号化処理を行う回数を暗号化段数と呼ぶ。

Single DES と同じ処理になるため、Single DES を前提として構築されている既存コンピュータシステムにおいて、トリプル DES に移行することは比較的容易である[7]。

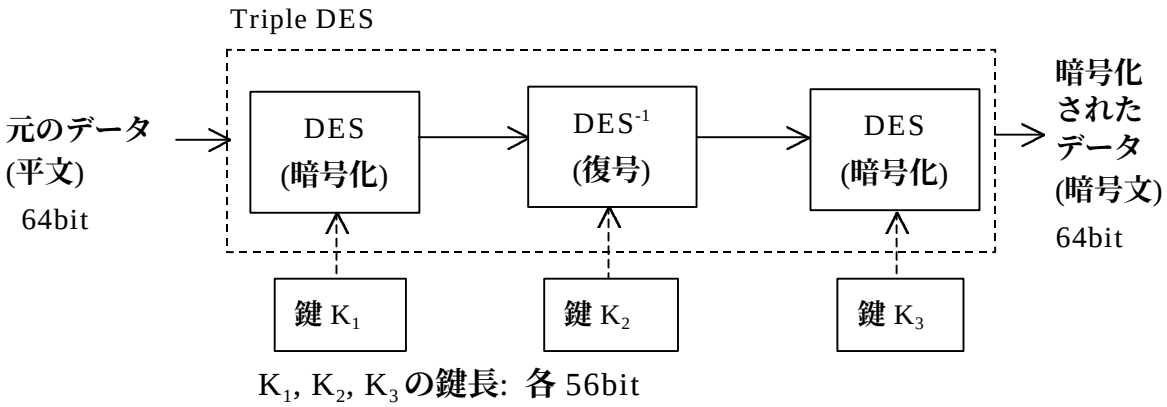


図１　Triple DES **の仕組み（**TECB **モード）**

また、一般に共通鍵ブロック暗号においては、平文を単純に暗号化するだけでは同一の鍵を用いて同じ平文を暗号化した場合常に同じ暗号文が得られることとなってしまう。これでは、鍵を頻繁に変更しない場合や長い平文を分割して（同一の鍵で）暗号化した場合に解読されやすい状況を作り出してしまうため、直前の暗号文をフィードバックさせ平文と排他的論理和[8]をとったものを暗号化する等の工夫を行うことにより、暗号強度を増そうとしている。このようなフィードバック等を行う方式をブロック暗号の利用モード（Modes of Operation）と呼ぶが、Triple DES は組み合わせ暗号であるため、その標準化では従来の Single DES 等にはなかったいくつかの新しい利用モードが提案されている。なお、図 1 のような Triple DES の最もシンプルな利用モードは TECB モードと呼ばれる。Triple DES の具体的な利用モードについては、第 6 章で紹介する。

[7] ただし、前述のとおり、Triple DES 化により暗号化・復号に係る処理速度は遅くなるため、その点での対応が必要になる場合があることにも留意すべきである。

[8] 通常、⊕で表わされ、ビット毎に、0 ⊕ 0 = 0、0 ⊕ 1 = 1、1 ⊕ 0 = 1、1 ⊕ 1 = 0 という加算を行うこと。

３. Triple DES の強度

Triple DES は鍵長が Single DES の 3 倍であるため（3-key Triple DES の場合）、全数探索法に対して現時点で十分安全であると考えられている。実際、前述の 1998 年 7 月に単体で Single DES の解読に成功した DES Cracker を使用して全数探索を行ったとしても、3-key Triple DES の解読には 10^{32} オーダーの年数[9]が必要になる（次頁表 1 参照）。また、差分解読法、線形解読法に関しても、Triple DES は暗号化段数が多いため、これらの解読法を仮に適用しようとしても現在知られている差分特性確率、線形特性確率から計算される必要平文数は膨大になる。したがって、ブロック長 64bit の下で理論的に作成可能な 2^{64} 個全ての平文・暗号文の組を利用したとしても、有効に鍵の候補を絞り込むことができないと考えられる。

一方、Triple DES は組み合わせ暗号であるため、ある条件の下では鍵長が拡大するほどには実質的な安全性は向上しないことが示されている。代表的な例として、Merkle と Hellman が提案した選択平文攻撃では、2-key Triple DES の場合は 2^{57}（全数探索法では 2^{112}）、3-key Triple DES の場合は 2^{112}（全数探索法では 2^{168}）と、全数探索法に対して大幅に計算量を削減することが可能であるとしている（Merkle and Hellman[1981]）。ただし、本解読法においては、解読成功確率を 50%とした場合、必要となる選択平文数が 2^{55} であり、平文と鍵のペアを記憶するのに必要な外部記憶媒体の量が 4.03×10^{10}Gbit と膨大になるほか、必要な情報を通信回線経由で入手するためにも困難を伴うことが指摘されており（Kusuda and Matsumoto[1997]）、現時点では本解読法が現実の脅威となる可能性は低いと考えられる。なお、Lucks は、Merkle と Hellman による選択平文攻撃の処理回数を削減する解読方法を提案しており、3-key Triple DES に対して、2^{108} 程度の計算量で解読できるとしている（Lucks[1998]）。ただし、Lucks による解読法もまた、必要となる記憶媒体の容量等から現実の脅威となる可能性は低いと考えられている。

また、2-key Triple DES に関しては、Oorschot と Wiener が Merkle と Hellman による選択平文攻撃をもとに拡張した既知平文攻撃を提案しており（Oorschot and Wiener[1990]）、既知平文 N に対して 120･N bit の記憶媒体を用意すれば $2^{120-\log_2 N}$ という計算量で解読できると指摘している。ただし、本解読法も現実的な脅威となるには今後約 30 年かかると予想されている（Kusuda and Matsumoto[1997]）。

このように、組み合わせ暗号であるため鍵長ほどには安全性が向上しないといっても、解読を実現するために必要な記憶媒体の容量等が非現実的であるこ

---

[9] DES Cracker の 1 秒当りの平均鍵検証個数は約 888 億個（1.3×2^{36} 個）であり、この処理速度で 2^{168} 個の鍵を全数探索した場合の解読に要する年数。

とに加え、いずれの解読方法の場合も、3-key Triple DES であれば 2^{108} 程度以上の膨大な計算量が必要になり、DES Cracker を用いて解読を行っても約 1.2×10^{14} 年以上かかることから、現時点では、これらの方法に対して Triple DES は十分安全であると考えられている。

表１　Triple DES の安全性評価結果

解読方法		Single DES		2-key Triple DES		3-key Triple DES	
		解読計算量	解読時間	解読計算量	解読時間	解読計算量	解読時間
Brute Force Method							
	全数探索法	2^{56}	約 225 時間（9.4 日）	2^{112}	1.8×10^{15} 年	2^{168}	1.3×10^{32} 年
	Merkle, Hellman による表索引－中間一致攻撃法（選択平文攻撃法）	——		2^{57}（選択平文数 2^{56}）*3		2^{112}（選択平文数 2^{56}）*3	
	Lucks による攻撃	——		——		$2^{108.2}$ *3	
	Oorschot, Wiener による既知平文攻撃法	——		$2^{120-\log2N}$ *4（既知平文数 N）		——	
Short Cut Method							
	差分解読法	2^{37}（選択平文数 2^{47}）*1		（選択平文数 2^{174}）*5			
	線形解読法	2^{42}（既知平文数 2^{43}）*2		（既知平文数 2^{118}）*5			

(注)解読計算量は解読に必要となる Single DES の暗号化処理または復号処理の回数である。解読時間は、前述の DES Cracker（1 秒あたり約 888 億$<1.3\times2^{36}>$回の DES 処理が可能）を用いて全数探索法により解読した場合に要する時間である。

*1 Biham and Shamir[1993]参照。

*2 Matsui[1994]参照。

*3 解読には膨大な記憶媒体の容量が必要なことが指摘されている（詳細は本文参照）。

*4 現実的な脅威となるには今後約 30 年かかると予想されている（詳細は本文参照）。

*5 差分解読法、線形解読法に関しても、Triple DES は暗号化段数が多いため、これらの解読法を仮に適用しようとしても、Triple DES を 48 段の Single DES とみなして最大差分特性確率と最大線形特性確率から計算される必要平文数は膨大になり、ブロック長 64bit の下で理論的に作成可能な 2^{64} 個全ての平文・暗号文の組を利用したとしても、有効に鍵の候補を絞り込むことができないと考えられる。

４．暗号文一致攻撃・辞書攻撃への対応

（１）暗号文一致攻撃・辞書攻撃

前章で指摘したとおり、Single DES を Triple DES 化することにより全数探索法に対しては安全性が向上するが、Triple DES のブロック長は Single DES と同じく 64bit と短いままであることから、Brute Force Method のうち暗号文一致攻撃（Matching Ciphertext Attack）や辞書攻撃（Dictionary Attack）に対する安全性には変化がないことが指摘されている。

暗号文一致攻撃とは、「m 個のデータの中から n 個をランダムに選択した時に、その中に同じデータが 2 個以上存在する確率 P は、P　1－exp（－n^2/2m）となり、その確率は一定の m に対して n の増加に伴い当初急激に増加する」という現象（バースデー・パラドックス[10]）を利用して解読を行う方法である。すなわち、DES の暗号文は 64bit のブロック長のデータであるため、それを 2^{32} ブロック分集めれば、約 0.5 の確率でその中に同じデータが存在することになる。本解読法では、これを手がかりに平文に関する情報を得る。暗号文一致攻撃で必要な暗号文の数はそのブロック長に依存するため、一般的には本攻撃に対する安全性は暗号文のブロック長に依存することとなる。

また、辞書攻撃とは、ある鍵によって暗号化された暗号文と平文の組を予め大量に集めて適当な外部記憶媒体に記憶しておき、それを辞書のように利用することによって、盗聴等により入手した暗号文に対応する平文を得るという攻撃法である。本攻撃では、ブロック長が n bit の場合、2^n 個の平文・暗号文の組を記録できる容量をもつ媒体が必要となるため、ブロック長が長いほど辞書攻撃に対する安全性は高くなる。

暗号文一致攻撃や辞書攻撃では、選択平文攻撃や選択暗号文攻撃のように攻撃者が平文や暗号文の内容を指定する必要はなく、膨大な数ではあるものの一連の暗号文（および平文）を入手さえできれば平文に関する情報が判明する。したがって、現時点ではさほど緊急の脅威とは考えられていないものの、通信回線の速度が上昇し、多くの暗号文を短時間に入手できる可能性が増えていくのにつれて、これらの攻撃はより現実的になっていくものと考えられる。

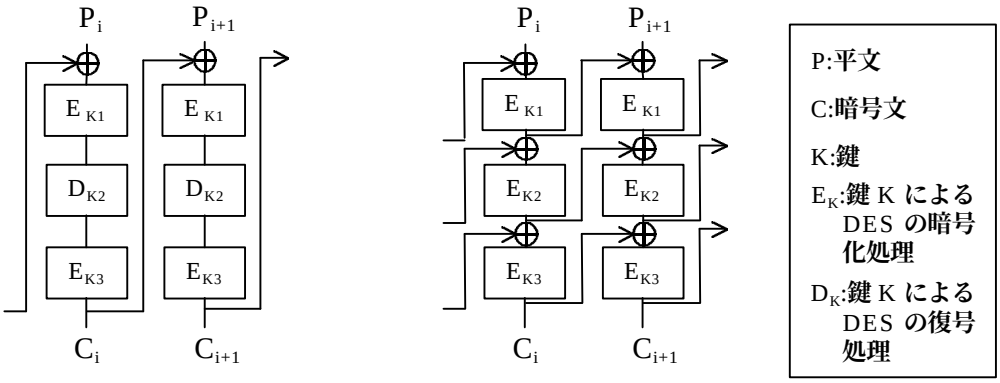
なお、これらの攻撃に対する安全性を高めるためには、ブロック長を長くすることが最も根本的な対応策であるが、ブロック長の伸長は暗号化・復号を行う情報システムにおいて大幅な変更を伴う可能性があり、また変更後も処理負担が大きいという実用面での問題がある。したがって、ブロック長の伸長は中長期的な対応にならざるを得ず（中長期的な対応方法については第 7 章で触れ

[10] あ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約 0.5 を超えるために必要なグループの人数は 23 人であり、1 年 365 日あ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、バースデー・パラドックスと呼ばれる。

る)、以下に示すように、Single DES と同じブロック長を保ったまま安全性を保つためにいくつかの対応策が提案された。

（2）インナーCBC モード

ブロック長が 64bit と短い Triple DES を利用したまま暗号文一致攻撃および辞書攻撃に対する安全性を高める方法としては、Triple DES のインナーCBC モードを利用することが考えられる（図 2 参照)。Triple DES のアウターCBC モード（一般に TCBC モードと呼ばれているもの）に対しては、同じ鍵で暗号化された暗号文が一致する場合（$C_i = C_j$)、Triple DES 処理のうち一つめの DES 処理（K_1 での暗号化処理）への入力も一致してしまう（$C_{i-1} \oplus P_i = C_{j-1} \oplus P_j$)。この特性から、暗号文が一致した場合には平文に関する何らかの情報を与えてしまうため、アウターCBC モードは暗号文一致攻撃や辞書攻撃に対する安全性は高くないと考えられている。これに対して、インナーCBC モードは、Triple DES の各 DES 処理間にフィードバックを設けることで暗号文から簡単に平文に関する情報が判明しないようにすることにより安全性を高めようとしている。また、インナーCBC モードには、各 DES 処理を並行して行うことにより、Single DES とほぼ変わらない処理速度が実現できるというメリットも存在する。



アウターCBC モード　　インナーCBC モード

図２　Triple DES のインナー／アウターCBC モード

しかし、Triple DES のインナーCBC モードに対しては、Biham がいくつかの解読法を提案している（Biham[1998])。これらの解読法は、選択暗号文攻撃[11]により、インナーCBC モードに存在する DES 処理間のフィードバックを制御することで、各々の鍵を独立に差分解読法や全数探索法で解読する方法である。その中で解読に必要な計算量が最も少ないのは 2^{59} であり、Single DES に対して全数探索を行った場合の計算量を数倍上回るのに止まる。このように、

[11] 攻撃者にとって望ましい暗号文を指定し、これに対応する平文が得ることができた場合の鍵を求める解読法。

インナーCBC モードは、解読者が DES 処理間へのフィードバック値を直接制御できることがその安全性の低さに繋がっている。

（3）CBCM モード

インナーCBC モードには、上記のような解読者が DES 処理間へのフィードバック値を直接制御できるという問題が存在するため、暗号文一致攻撃、辞書攻撃に対して Triple DES の強度を高めるために、1995 年に、IBM の Coppersmith、Johnson、Matyas が CBCM モードを提案した（Coppersmith, Johnson, and Matyas[1996]）。CBCM モードの仕組みは図 3 参照。

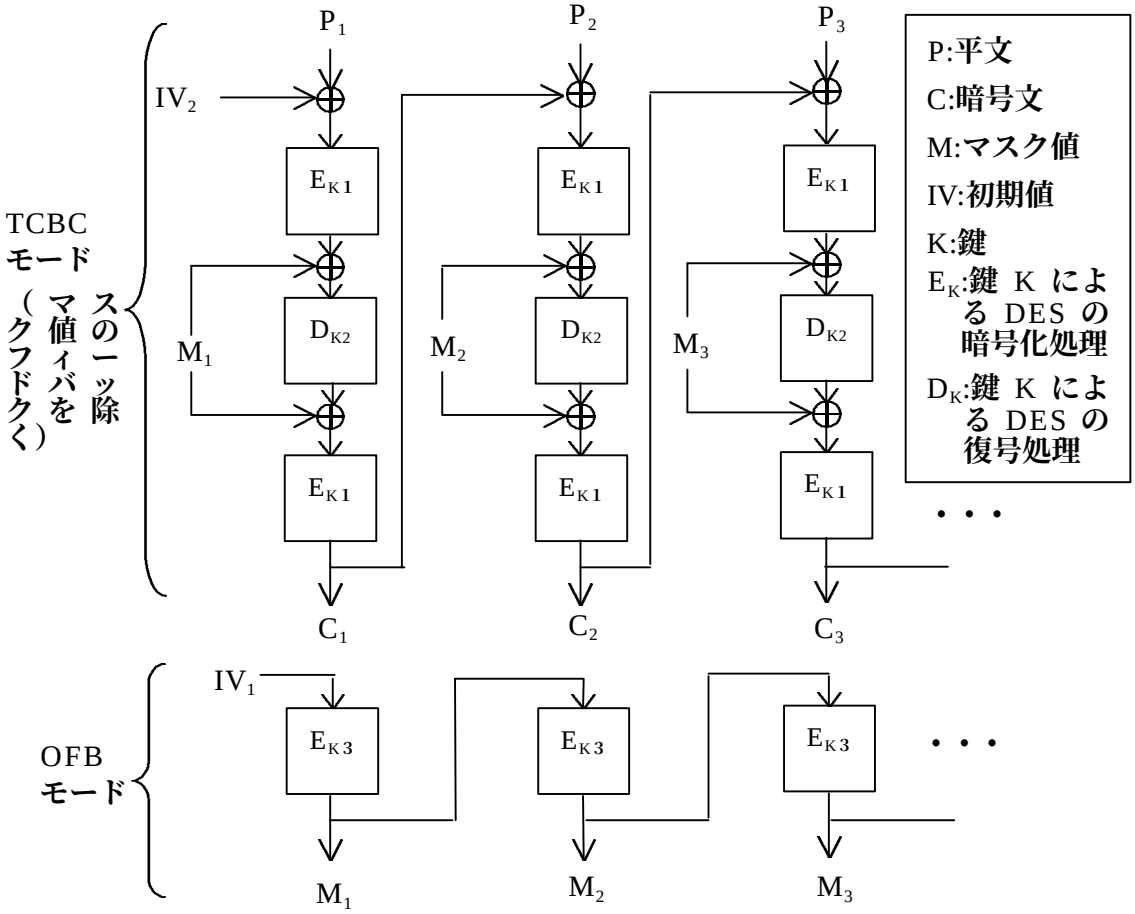


図３ CBCM モード

前述のとおりインナーCBC モードでは解読者が DES 処理間のフィードバック値を直接操作することにより解読が行われたことに対応して、CBCM モードでは、Single DES のブロック長を変えずに暗号文一致攻撃、辞書攻撃への安全性を保ったまま、OFB モード（Single DES）で計算したマスク値を TCBC モード（Triple DES）内での DES 処理間にフィードバックすることにより、解読者がフィードバック値を直接操作できないようにすることで安全性を高めようとしている。

5. Triple DES CBCM モードへの暗号解析

CBCM モードは、米国国内の標準化機関である ANSI（American National Standards Institute）配下で米国金融業界内での標準化を行っている ANSI X9 による Triple DES の利用モードに関する標準である X9.52 の原案に含まれていたが、標準化作業がほぼ終了していた 1997 年に、暗号学者の Biham と Knudsen が当モードに対する攻撃法を発表したため（Biham and Knudsen[1998a]）、X9.52 から当モードを除外して標準化することとなった。このように本攻撃法の発表は Triple DES の標準化の動向に大きな影響を与えることとなったため、以下では攻撃法の内容を紹介する。本攻撃は選択暗号文攻撃であり、K_1、K_2、K_3の順に鍵を導出している。

<K_1の導出>

① 図 4 のとおり、一つの暗号文 C_1（64bit）を任意に選択し、CBCM モードの結果、暗号文 C_1が 2^{64}個連続して得られ、各々の C_1に対応する平文（$P_{1,1}$～$P_{1,2^{64}}$）も入手できたとする。同様に、任意に選択した 2^{64} 個の暗号文 C_2 に対して、平文 $P_{2,1}$～$P_{2,2^{64}}$が入手できたとする。

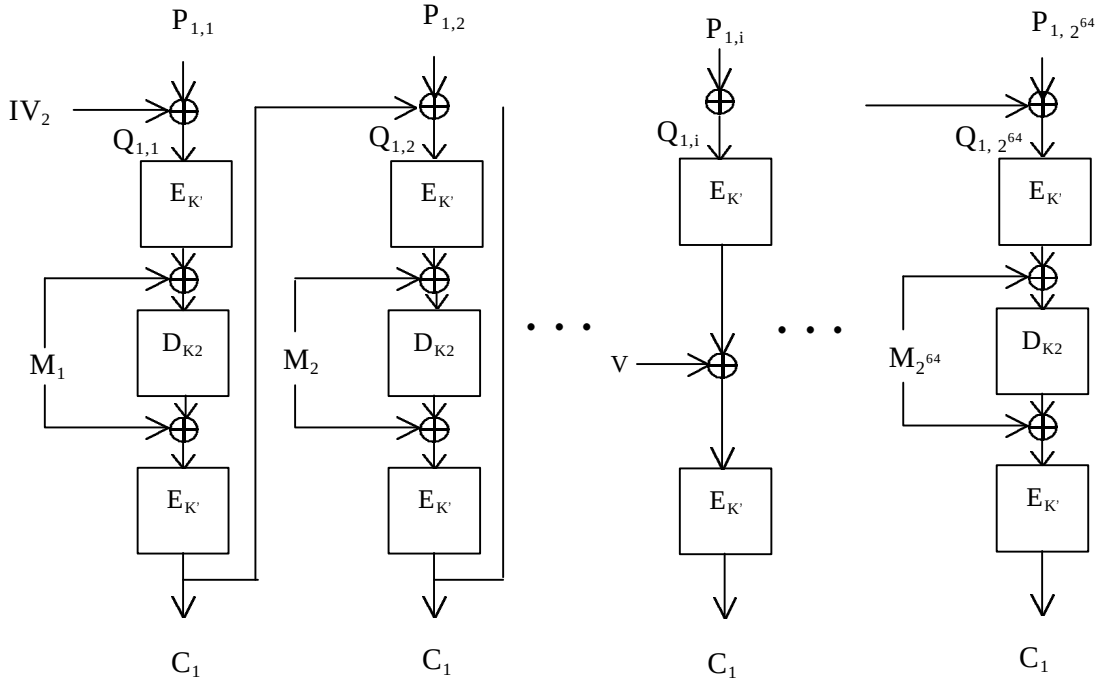


図４ K_1の導出（１）

② K_1の適当な候補を選びこれを K'とする。

③ 適当な V（ブロックサイズ 64bit のデータ）をランダムに選択する。

④ ②、③で選択した K'、V に対して、$Q_{1,i} = D_{K'}(D_{K'}(C_1) \oplus V)$を満たす i 列目を見つける。ここで、$Q_{1,i}$は、その i 列目における Triple DES の 1 つめ

の DES 処理への入力データである。

$Q_{1,i} = D_{K'}(D_{K'}(C_1) \oplus V)$ を満たす i 列目を探す理由

Triple DES の 2 つめの DES 処理の出力値を x とし、これと当該 DES 処理への入力値と排他的論理和をとった場合、その結果は $x \oplus E_{K2}(x)$ と表わされる x の関数であり（図 5 参照)、これを v（x）とする。v（x）の値は 2^{64} 個の値を取り得る x によって決定されるが、v（x）の値がとり得る範囲はバースデー・パラドックスのため 2^{64} 個よりも小さくなるものの、2^{64} 個の中に占める割合は比較的高い（約 63%）ことがわかっている。したがって、ランダムに V を選択しても、$V = x \oplus E_{K2}(x)$ を満たす x が、2^{64} 列の中には少なくとも一つ存在する確率が高い（63%)。これにより、本式を満たす i 列目においては、K_2 を無視して K_1 のみの導出を行うことが可能となる。

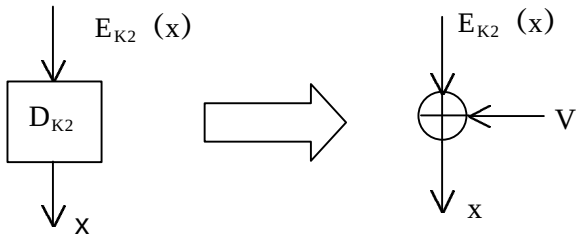


図５ K_1 の導出（２）

⑤ 同様に、同じ K'、V に対して、$Q_{2,j} = D_{K'}(D_{K'}(C_2) \oplus V)$ となる j 列目を見つける。

⑥ i と j が見つかった場合には、$D_{K'}(C_1) \oplus D_{K'}(C_2) = E_{K'}(Q_{1,j}) \oplus E_{K'}(Q_{2,i})$ が成立するかどうかを確認し、この式が成立すれば K'が正しい K_1 である。図 6 のとおり、K'が正しい K_1 であれば、本式が成立するはずである。成立しなければ別の V を選択し③~⑥のプロセスを繰り返す。

⑦ 全 V について③から⑥を繰り返しても⑥の式が成立しない場合には、異なる K'を選択し②から⑦のプロセスを繰り返す。

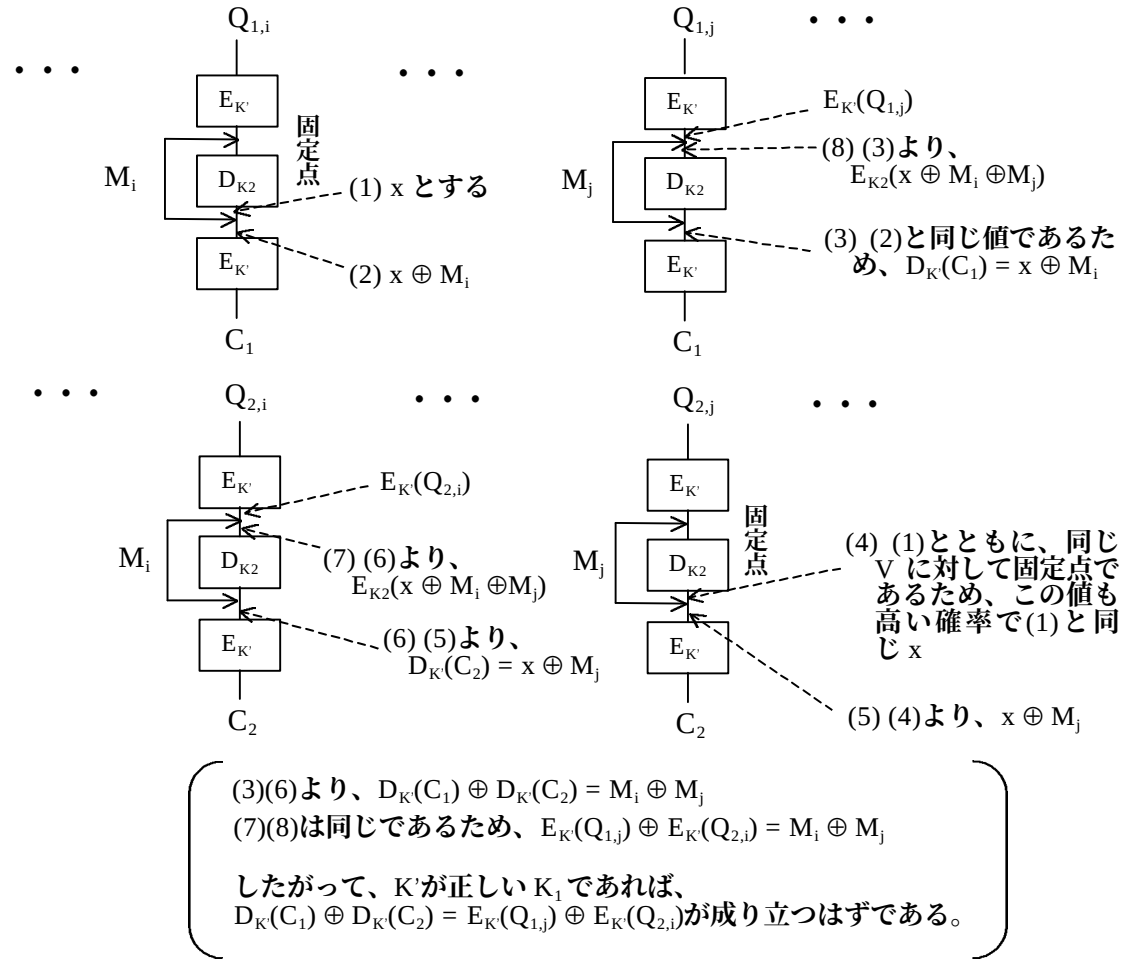


図６　K_1の導出（３）

<K_2の導出>

① K_2の適当な候補を選びこれを K"とする。

② ランダムに a（ブロック長 64bit）を選択し、2 つめの DES 処理への入力値であるとする。K"に対して $b = a \oplus D_{K"}(a)$ を計算し、$b = E_{K1}(Q_{1,i}) \oplus D_{K1}(C_1)$ となる i と K"を求める（K_1は導出済であるため、$E_{K1}(Q_{1,i}) \oplus D_{K1}(C_1)$は既知）。

③ ②で i と K"が見つかれば $M_i = a \oplus E_{K1}(Q_{1,i})$ という関係式より対応する M_i を求める。

④ ③の結果より、$Q_{2,i} = D_{K1}(M_i \oplus E_{K"}(M_i \oplus D_{K1}(C_2)))$ が成立するかどうかを検証し、成立すればその場合の K"が正しい K_2 である。成立しなければ、新しい a を選択し、②から④を繰り返す。

⑤ 全 a に対しても正しい K_2 が見つからない場合は新しい K"を選び①から⑤を繰り返す。

<K_3の導出>

① 2^{33}個の a_i(i=1,…2^{33})をランダムに選択し $b_i = a_i \oplus D_{K2}(a_i)$（i=1,…$2^{33}$）を計算する。

② ①の結果をもとに、
$b_i = E_{K1}(Q_{1,m}) \oplus D_{K1}(C_1)$
$b_j = E_{K1}(Q_{1,m+1}) \oplus D_{K1}(C_1)$
を満たす、a_i、a_jを見つける。
2^{33}個の a_i を選択したのは、バースデー・パラドックスと同様に、$(2^{64})^{1/2}=2^{32}$以上のデータを取得すれば、連続する $Q_{1,m}$、$Q_{1,m+1}$が得られる確率が約 0.5 を超えるためである。

③ ②を満たす a_i、a_jが見つかれば、
$M_m = a_i \oplus E_{K1}(Q_{1,m})$
$M_{m+1} = a_j \oplus E_{K1}(Q_{1,m+1})$
を計算し、$M_{m+1} = E_{K3}(M_m)$ を満たす K_3を全数探索法により見つける。

本攻撃に必要な条件をまとめると、必要テキスト量は 2^{65}（C_1 および C_2）、攻撃全体に係る必要最低限の計算量は、K_1、K_2、K_3 を導出するのに必要な計算量[12]が各々2^{57}、2^{56}、2^{56} であるため、その総和の 2^{58} である。したがって、本攻撃法に必要な計算量は、Single DES を全数探索法により攻撃する場合の数倍に止まる。

本攻撃法は、上で説明したとおり理論的には十分成り立ち得るが、2^{65} 個の暗号文を指定しそれに対応する平文を得られるという前提の下に行われる選択暗号文攻撃であり、現時点では、現実的な脅威となる可能性はさほど高くないと考えられる。しかし、実装環境如何では現実的な脅威になることもあり得るほか、標準全体のレピュテーションが落ちることを嫌い、CBCM モードが ANSI X9 による標準から除外されたのではないかと考えられる。

インナーCBC モードのみならず、CBCM モードについても攻撃法が提案されたということは、Triple DES 内の DES 処理間にフィードバックを行うことの危険性を示唆しているものと評価することができよう。DES 処理間のフィードバックを取り入れた利用モードの場合、それが攻撃者によって直接制御可能かどうかに関わらず、何らかの情報を与え、3 つの DES 処理の鍵を独立して攻撃できるようになる危険性が高いと考えておくべきであろう。

[12] ランダムに V や a を選んだ中で、1 つの鍵候補の検証を行うために必要な計算量を 1 単位とする。

６. Triple DES の標準化の進捗状況

現在、Triple DES は、多くの金融機関のコンピュータシステムにおいて採用されつつあることを背景として、様々な標準化機関において標準暗号として認定され始めている。そのうち主要標準化機関による Triple DES の標準の名称について表 2 に簡単に纏める。

表２　主要標準化機関による Triple DES の標準

標準化機関	ANSI	ISO/TC68	NIST
トリプル DES の利用モードの標準名	ANSI X9.52	未定	FIPS 46-3
シングル DES の標準名	ANSI X3.92	ISO 8731-1、9564-2、10126-2	FIPS 46-2
シングル DES の利用モードの標準名	ANSI X3.106	ISO 8372 (ISO/IEC JTC1 SC27*の標準)	FIPS 81
位置付け	米国金融業界の標準	金融業界の国際標準	米国政府機関における標準

*ISO と IEC（International Electro-technical Commission）が共同で設立した、情報技術の国際標準化を担当する技術専門委員会（JTC1:Joint Technical Committee 1）配下で汎業界的な情報セキュリティ技術の国際標準化を担当する分科委員会。

Triple DES の標準化に関する具体的な動きは以下のとおり。

（1）ANSI

ANSI X9 下の情報セキュリティ技術分科会（X9F）配下の暗号ツール作業部会（X9F1）は、X9.52 として Triple DES（ANSI X9 による各種標準では Triple Data Encryption Algorithm<以下 TDEA>と呼称）の標準案を作成し、1998 年 8 月から 10 月までの public comment 期間を経て標準として認定した。

Triple DES の基礎となる Single DES 自体は以前から Data Encryption Algorithm という名称で X3.92 として標準化されており、その利用モードも X3.106 として標準化されている。X9.52 は、基本的には Single DES を前提とした X3.106 を拡張して Triple DES の利用モードを標準化したものである。

X9.52 で標準化されている利用モードは表 3 に示した 7 つであるが、4 つの利用モード（表 3 中の①、②、④、⑥）については、前述のとおり 3 つの DES 処理の鍵を全て同一のものとすることにより、各々対応する Single DES の利用モード（表 3 の説明欄に記述）と互換性が保たれている。また、Triple DES は、Single DES を 3 回繰り返す暗号方式であるため、基本的には Single DES の 3 倍の処理時間を要するが、表 3 中の③、⑤、⑦の 3 モードでは、3 つの DES 処理を並行して行えるようにすることにより、Single DES と変わらない処理速度で暗号化・復号を行うことを可能になる。これらの利用モードを実装する

のにあたっては、基本的には Single DES の利用モードと同じ考え方で選択できるものと考えられるが、その際の一般的な留意点を表 3 に記述した。

なお、ANSI X9 では、現在、X9.52 の実装に当たって、利用モードを選択する際の留意点に関する標準である X9.65 ”TDEA Implementation Standard / Guideline”を作成している。本標準では、各利用モードの利用分野や Triple DES に対する攻撃法の紹介等を行っている。

表３　Triple DES の利用モード

利用モード	説　明	採用に当たっての留意点
① TDEA Electronic Codebook Mode（TECB）	X3.106 における ECB の拡張。	• 同一の鍵に対して同じ平文からは必ず同じ暗号文が得られるため、1 ブロックより長いデータの暗号化や複数ブロックの暗号化に同じ鍵を使用する場合には不適。 • 送信された暗号文に発生した bit エラーは他ブロックに影響しない。
② TDEA Cipher Block Chaining Mode（TCBC）	X3.106 における CBC の拡張。	• 暗号化する平文と前ブロックの暗号文の排他的論理和をとるため、同一の鍵に対して同じ平文から異なる暗号文が生成される。したがって、連続した複数ブロックの暗号化に適する。 • 前のブロックと排他的論理和をとるため、正しい順番で復号することが重要。
③ TDEA Cipher Block Chaining Mode – Interleaved（TCBC-I）	平文ブロックを 3 分割し 3 つの TCBC モードを同時処理。	• 基本的には②の同様の性質。 • Single DES とほぼ同じ処理スピードを実現可能。 • Single DES と互換性なし。
④TDEA Cipher Feedback Mode（TCFB）	X3.106 における CFB の拡張。	• 処理するデータを分割して、送信データのサイズを小さくすることが可能(多くは1ビットまたは8ビット)。 • 同期がずれても自己回復可能なので、同期のずれやすい通信路等に適する。
⑤TDEA Cipher Feedback Mode – Pipelined（TCFB-P）	3 つの DES の同時処理を実現（3 つの初期値を設定)。	• 基本的には④と同様の性質。 • Single DES とほぼ同じ処理スピードを実現可能。 • Single DES と互換性なし。
⑥TDEA Output Feedback Mode（TOFB）	X3.106 における OFB の拡張。	• 送信暗号文に bit エラーが発生しても他のブロックには影響しないため、無線通信等エラー伝播を避ける必要がある場合に適する。 • ④と同様、処理するデータを分割して、送信データのサイズを小さくすることが可能。
⑦TDEA Output Feedback Mode – Interleaved（TOFB-I）	3 つの DES の同時処理を実現（3 つの初期値を設定)。	• 基本的には⑥と同様の性質。 • Single DES とほぼ同じ処理スピードを実現可能。 • Single DES と互換性なし。

（2）ISO

ANSI X9 における X9.52 の標準化を受け、国際標準化機構（ISO）の金融専門委員会（ISO/TC68）の下で「セキュリティ管理と一般銀行業務」を担当する分科委員会（ISO/TC68/SC2）において、現在 Triple DES の国際標準化が進められている。Single DES の安全性低下が急速に認識されつつある状況下、ISO/TC68 としても金融業界の業務上の要請に応えるために、米国国内標準である X9.52 の内容をそのまま国際標準化することにより迅速に標準を作成することが予定されている。つまり、標準原案の策定や審議といった通常の標準化作業の段階を経ずに、X9.52 を直接国際標準最終案（FDIS：Final Draft International Standard）として TC68/SC2 に提出し、その承認後、直ちに国際標準（IS：International Standard）に採択するという標準化の手続きが今後行われる予定である。ただし、標準化の時期は現時点では未定である。

また、Triple DES の標準化に伴い、従来 Single DES が標準暗号であることを前提として記述されている、①CD/ATM、POS 端末と銀行のホストコンピュータ間での PIN の暗号化（ ISO 9564 ）、②鍵の管理（ ISO 8732 ）、③データの暗号化（ ISO 10126 ）、④MAC（ ISO 8731 ）、等の各種標準においても Triple DES を対象とするように変更されていくものと予想される。ちなみに、①の ISO 9564 については、現在国際標準案（DIS：Draft International Standard）として提案された改定案に対する投票段階にあるが、PIN の暗号化に使用する暗号アルゴリズムは実質的に Triple DES に変更される予定である[13]。

（3）FIPS

ANSI X9 における X9.52 の標準化を受け、1999 年 1 月に NIST より Triple DES を米国政府標準暗号とするというアナウンスが行われた。同時に公表された案について同年 4 月 15 日までのコメント受付期間を経て FIPS として標準化される予定である。Single DES は FIPS 46-2 として規定されていたが、Triple DES の場合はこれを更新するものとして FIPS 46-3 として規定される予定であり[14]、その内容は X9.52 をもとにしている。

FIPS46-3 案の主なポイントは、①Triple DES は FIPS として認可された共通鍵暗号アルゴリズムとなること、②Single DES は基本的に既存システムに

---

[13] 現在のドラフトでは、明示的には標準中に Triple DES とは指定されていないが、鍵の長さを最低 112bit と規定することにより、Single DES の利用を排除し、Triple DES への移行を促進しようとしている。

[14] そもそも、FIPS46 は 5 年毎に見直しが行われているが、前回見直し時の 1993 年に、次回（1998 年）見直し時には安全性の強化を企図して暗号アルゴリズムの変更を検討すると表明されていた。

おいてのみ使用を許可し、Single DES を使用する既存システムのメンテナンスを行う場合、実現可能であれば Triple DES を Single DES モード（3 つの鍵を全て同じにする）で使用すること、③Single DES 使用政府機関に対しては、各システムが必要とするセキュリティレベル及び他の対応手段の有無等に応じて慎重な計画の下にトリプル DES に移行することを奨励していること、の 3 点である。

FIPS は米国政府機関に対する標準であり、その他の機関は必ずしも今回の措置により Single DES が利用できなくなるわけではない。しかし、欧米の金融機関では、Single DES の「信用状」として機能していた FIPS46-2 の認定終了を先取りして、Single DES から Triple DES や目的に応じて公開鍵暗号方式に移行しつつある。

７．まとめ

全数探索法に対する Single DES の安全性低下に伴い、当面 Triple DES がその後継として使用されることは確実な状況であり、実際に Single DES から Triple DES への移行も金融業界を中心に始まりつつある。これに伴い、Triple DES を標準の共通鍵暗号アルゴリズムとする動きも様々な標準化機関において行われつつあり、その標準化の過程で鍵長の伸長による全数探索法への対応のみならず、暗号文一致攻撃や辞書攻撃に対して Single DES のブロック長を変更しないまま安全性を高めるためにインナーCBC モードや CBCM モード等様々な方法が提案されてきた。

しかし、それらの対応に関しても各々解読法が存在することが提案されたことから、暗号文一致攻撃や辞書攻撃に対してはブロック長を伸ばさずに対応することは困難であることが判明してきた。このため、Triple DES は現時点では全数探索法に対しては十分な安全性を有していると考えられているものの、NIST が現在選考中の次世代米国政府標準暗号（AES：Advanced Encryption Standard）[15]により長いブロック長のデータを利用できるようになるまでの橋渡しを行うものとして考えられている[16]。

もっとも、現時点においては、Triple DES は最も信頼性の高い共通鍵案号アルゴリズムと考えられており、金融取引用の通信ネットワークにおいては、今後も Triple DES が幅広く利用されていくものと考えられる。ただし、その際には、Single DES の場合と同様、暗号文一致攻撃や辞書攻撃が可能となるほどの大量の暗号文を同一の鍵で生成しない等の対応を利用者側で行うことが必要となろう。

また、Triple DES には第 6 章で紹介したような様々な利用モードが存在し、各々特徴が異なる。このため、Triple DES を使用する場合には、業務やコンピュータシステムの性質にあわせて適切な利用モードを選択していくことが必要である。

以　　上

---

[15] AES の最終選定時期は現時点で不明であり、早くても 2000 年入り後と考えられている。その選定後も、安全性に対する高い信頼を得て一般に利用可能となるまでには数年かかるものと予想されている。

[16] FIPS46-3 案によれば、AES はより長期的な視野に立ったより高いレベルでのセキュリティの実現を目指しているため、AES の認定後も、Triple DES は FIPS 認定暗号アルゴリズムとして共存し、徐々に AES に移行していくことになると指摘している。

【参考文献】

岩下直行・谷田部充子、「金融分野における情報セキュリティ技術の国際標準化動向」、IMES Discussion Paper Series No. 98-J-29 日本銀行金融研究所、1998 年 11 月

宇根正志・太田和夫、「共通鍵暗号を取り巻く現状と課題　―DES から AES へ―」、IMES Discussion Paper Series No. 98-J-27 日本銀行金融研究所、1998 年 11 月

松本勉・岩下直行、「金融分野における情報セキュリティ技術の現状と課題」、IMES Discussion Paper Series No. 98-J-25 日本銀行金融研究所、1998 年 11 月

American National Standards Institute, "X9.52 – 1998, Triple Data Encryption Algorithm Modes of Operation", 1998

American National Standards Institute, "WORKING DRAFT X9.65 – 1999, Triple Data Encryption Algorithm（TDEA）Implementation Standard / Guideline", 199X

E. Biham, "Cryptanalysis of Multiple Modes of Operation," Journal of Cryptology, Vol. 11, No. 1, pp. 45-58, 1998

E. Biham and L. R. Knudsen, "Cryptanalysis of the ANSI X9.52 CBCM Mode," Advances in Cryptology – Proceedings of EUROCRYPT '98, Lecture Notes in Computer Science, Vol. 1403, pp. 100-111, Springer-Verlag, 1998a

E. Biham and L. R. Knudsen, "DES, Triple-DES and AES," RSA Laboratories' CryptoBytes, Vol. 4, Number 1, 1998b

E. Biham and A. Shamir, "Differential Cryptanalysis of the Full 16-Round DES," Advances in Cryptology – Proceedings of CRYPTO '92, Lecture Notes in Computer Science, Vol. 740, pp. 487-496, Springer-Verlag, 1993

D. Coppersmith, D. B. Johnson, and S. M. Matyas, "A proposed Mode for Triple-DES Encryption," IBM Journal of Research and Development, Vol. 40, No. 2, pp. 253-262, 1996

Electronic Frontier Foundation, Cracking DES, O'Reilly & Associates, 1998

K. Kusuda and T. Matsumoto, "A Strength Evaluation of the Data Encryption Standard," Institute for Monetary and Economic Studies, Bank of Japan, DPS No. 97-E-5, 1997

S. Lucks, "Attacking Triple Encryption," Proceedings of Fast Software Encryption '98, Lecture Notes in Computer Science, Vol. 1372, pp.239-253, 1998

M. Matsui, "Linear Cryptanalysis Method for DES Cipher," Advances in Cryptology – Proceedings of EUROCRYPT '93, Lecture Notes in Computer Science, Vol. 765, pp. 386-397, Springer-Verlag, 1994

A. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996

R.C. Merkle and M. Hellman, "On the Security of Multiple Encryption," Communications of the ACM, Vol. 24, No. 7, pp. 465-467, 1981

National Institute of Standards and Technology, "Data Encryption Standard（DES）," Federal Information Processing Publication（FIPS PUB）46-2, 1993

National Institute of Standards and Technology, "DRAFT Data Encryption Standard（DES）," Federal Information Processing Publication（FIPS PUB）46-3,

1999

P. C. van Oorschot and M. J. Wiener, “A known plaintext attack on two-key triple encryption,” Advances in Cryptology – Proceedings of EUROCRYPT ’90, Lecture Notes in Computer Science, Vol. 473, pp. 318-325, Springer-Verlag, 1990