IMES DISCUSSION PAPER SERIES

# AES（Advanced Encryption Standard）について

宇根正志

Discussion Paper No. 97-J-16

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES
BANK OF JAPAN

日本銀行金融研究所

〒100-91 東京中央郵便局私書箱 203 号

IMES Discussion Paper Series 97-J-16
1997 年 11 月

# AES（Advanced Encryption Standard）について

**宇根正志***

**要旨**

AES は、現在最も広く利用されている暗号アルゴリズムである DES（Data Encryption Standard）の後継として、米国政府が策定しようとしている次期米国政府標準暗号の名称である。本年 1 月、米国政府は、AES のアルゴリズムを公募によって選定する方針を発表した。これは、近年のコンピューター処理能力の向上に伴って、DES の強度が徐々に低下してきており、今後より強度の高い暗号アルゴリズムが標準暗号として認定される必要が高まっているとの認識が強まっているためである。その後、米国政府は、暗号研究者や暗号ユーザーからのコメントを織り込み、本年 9 月、AES のアルゴリズムの要件、評価基準や今後の選定スケジュールを決定、公表している。

本稿では、AES のアルゴリズムの要件・評価基準決定に至るまでの経緯を、インターネット等から入手した資料を基に整理し、AES の公募方法に関する暗号研究者や暗号ユーザーのコメントを紹介する。米国では、DES が金融ネットワークの安全性確保のために広く利用されており、金融分野における新標準暗号選定への関心は非常に高い。このため、中央銀行（FRB）や銀行協会（ABA）等は、こうした新標準策定作業に積極的に関与している。今回決定された AES の要件・評価基準にも、FRB 等のコメントの多くが採用されている。

今後、AES が DES に代わって米国政府標準暗号として認定されると、金融業務を含めた様々な分野で採用される可能性が高い。こうした観点からも、AES の認定を巡る動きについては、引き続き注視していく必要があるものと考えられる。

**キーワード：**AES、DES、NIST、共通鍵ブロック暗号、米国政府標準暗号

JEL classification: L86、Z00

* 日本銀行金融研究所研究第２課（E-mail: masashi.une@boj.or.jp）

本論文を作成するに当たっては、横浜国立大学の松本勉助教授、NTT 情報通信研究所の岡本龍明特別研究員と太田和夫主幹研究員、三菱電機情報技術総合研究所の反町亨氏から有益なコメントを頂戴した。

## 1. AES 検討開始に至るまでの経緯

現在、米国政府標準暗号[1]に認定されている DES は、鍵長 56 bit、ブロック長 64 bit の共通鍵ブロック暗号であり、世界で最も広く利用されている暗号アルゴリズムである。DES のアルゴリズムは、NBS[2]が 1973 年に実施した米国政府の標準暗号アルゴリズムの公募において、IBM 社から提案されたアルゴリズムが原形となっており、NBS 等による審査を経て 1977 年に米国政府標準暗号に認定された。

その後、様々な暗号研究者によって DES の解読法に関する研究が行われ、「差分解読法」[3]や「線形解読法」[4]などの方法が提案されたが、DES の安全性にとって致命的となる解読法は未だに見つかっていない。また、候補となるすべての鍵を試してみる「全数探索法」は、解読に必要な計算時間が膨大で現実的な脅威とはならないとされていた。こうした長年にわたる DES 強度評価の蓄積によって DES の安全性に対する信頼が高まり、DES は金融をはじめとした幅広い分野において、通信データの暗号化手段として普及してきた。

しかし、近年のコンピューター処理能力の向上に伴って、DES の安全性は徐々に低下してきている[5]。このため、近い将来、DES よりも安全性の高い暗号アルゴリズムが標準暗号として認定される必要があるとの見方が強まっている。NIST は、1993 年の標準暗

---

[1]米国政府標準暗号は、米国連邦政府内で利用されるコンピューターシステムに関する標準規格 FIPS（Federal Information Processing Standards）の一部であり、DES は FIPS 46-2 に指定されている。なお、FIPS は NIST によって作成されており、「ソフトウェアに関する標準・ガイドライン」や「ハードウェアに関する標準・ガイドライン」など 7 つのカテゴリーに分類される。DES が規定されている FIPS 46-2 は、「コンピューターセキュリティに関する標準・ガイドライン」に分類されている。

[2] NBS（National Bureau of Standard）は、米国内における科学技術全般の標準規格を策定する政府機関であった。1988 年から、NIST（National Institute of Standards and Technology）と名称変更されている。

[3] 差分解読法は、1990 年に暗号研究者の Biham（イスラエル科学技術研究所＜通称テクニオン＞）と Shamir（イスラエル・バイツマン研究所）が考案した解読法で、ある特定の差分を持つ一組の平文のペアに対して、特定の差分を持つ暗号文のペアが生じる確率が高くなる場合に、それらの平文と暗号文のペアに基づいて暗号鍵を推測する方法である。

[4] 線形解読法は、1993 年に三菱電機・情報技術総合研究所の松井充氏（共通鍵ブロック鍵暗号 MISTY の考案者の１人）が考案した方法で、平文と暗号文のいくつかの bit の排他的論理和が暗号鍵のいくつかの bit の排他的論理和と等しくなる確率が 0.5 から乖離する場合に、この乖離を最大にする線形の近似式を構成して暗号鍵を推測する方法である。

[5] 例えば、線形解読法によって、12 台のワークステーションを使って 50 日で解読できたという研究結果が報告されているほか、タイムメモリートレードオフ法（予め暗号文と鍵の対応が分かるような索引表を作成しておき、暗号文入手後短時間で鍵の探索を可能にする解読法）を利用することにより、専用解読装置の開発費用を除けば、数時間程度での解読が現実的な費用で実施できる可能性も別の研究結果によって示されている。

号の再評価（re-certification）[6]において、「1998 年に行われる次回の標準暗号見直しの際には、DES よりも高い安全性を有する暗号アルゴリズムについて調査し、DES に代わる新しい標準暗号を認定するかどうか検討したい」（FIPS 42-6 の但書）と表明し、標準暗号としての DES の見直しが今後必要となるとの考え方を示した。

DES に代わる暗号方式としては、Triple-DES と呼ばれる暗号方式が利用されている。Triple-DES は、これまで欠陥が発見されていない DES のアルゴリズムを、異なる３つまたは２つの暗号鍵で３回繰り返して暗号化する方法である。ANSI X9[7]では、この Triple-DES を新たな金融業務用の標準暗号（ANSI X9.52）として認定することを現在検討している。もっとも、Triple-DES は、DES を３回繰り返して暗号化するため処理速度がやや遅いほか、当面危険性はないとはいえ、Triple-DES 特有の解読法（Merkle-Hellman 選択平文攻撃等）の存在が知られていること等から、数年～10 年後に新しい暗号標準が一般に利用可能となるまでの「つなぎ」となる暗号方式と位置付ける向きが多いようである。

こうした中、米国政府（NIST[8]）は、1997 年 1 月に、1998 年の標準暗号見直しに合わせて DES に代わる共通鍵ブロック暗号（標準化後、AES<Advanced Encryption Standard>と呼ばれる予定）を公募すると発表し、同年 9 月にはアルゴリズムに必要とされる条件、評価基準やアルゴリズムの選定スケジュール等を内容とする募集要項を発表した。この発表により、DES に代わる標準暗号の選定が事実上スタートしたといえる。

今後、AES が DES に代わって米国政府標準暗号として認定されると、金融業務を含めた様々な分野で採用される可能性が高い。こうした観点からも、AES の認定を巡る動きについては、引き続き注視していく必要があるものと考えられる。

## 2. AES の候補となるアルゴリズム募集に関する発表

NIST は、1997 年 1 月２日に AES のアルゴリズムを募集する方針を発表するとともに、① AES の候補となるアルゴリズムが満すべき要件（Minimum Acceptability Requirements）、②評価基準（Evaluation Criteria）と、③今後の審査手順を発表した[9]。

---

[6] NBS は、1977 年に DES を標準暗号として認定した時に、DES が強度等の観点から標準暗号として適格かどうかを 1983 年から 5 年ごとに再評価（re-certification）することとしており、これまで 3 回（1983 年、1988 年、1993 年）の再評価が行われ、いずれも DES が標準暗号として認定されている。

[7] ANSI（American National Standards Institute）は、米国内の技術標準を策定する民間の標準化機関であり、ISO（International Organization for Standardization）の米国代表である。X9 は、金融機関における情報システム技術の標準規格を策定する委員会である。

[8] NIST については、注 2 を参照。

[9]発表内容は、NIST[5]に掲載されている。

### (1) AES が満たすべき要件

NIST は、「AES として認定するアルゴリズムは、候補となる各アルゴリズムに対する暗号研究者等専門家の評価を考慮して決定される」とした上で、満足すべき要件として以下の４つを提案した。

① AES は共通鍵ブロック暗号[10]とする。
② AES の鍵長は可変とする[11]。
③ AES はハードウェアにもソフトウェアにも実装可能とする[12]。
④ AES はロイヤリティ・フリーとする[13]。

### (2) AES の評価基準

AES の評価基準として以下の７点が挙げられており、NIST は、各項目の詳細については今後専門家からのコメントを踏まえて決定するとしている。

① 安全性（解読の困難性）
② 処理速度
③ アルゴリズム実装に必要となるメモリー容量
④ ハードウェアやソフトウェアへの実装可能性
⑤ アルゴリズムの構造の単純性
⑥ 鍵長やブロック長などのアルゴリズムの柔軟性
⑦ 実装する場合のライセンス取得の必要性

また、アルゴリズムの応募の際には、C 言語によって書かれたアルゴリズムのソースコードのほか、現在知られている攻撃方法に対するアルゴリズムの強度評価の結果や、

---

10 共通鍵ブロック暗号は、共通鍵暗号とブロック暗号の両方の性質を兼ね備えた暗号方式である。共通鍵暗号とは、暗号化と復号化に同じ鍵を利用する暗号方式であり、ブロック暗号とは、暗号化するデータをある一定の長さのブロックに分割し、すべてのブロックを同じ鍵で暗号化する方式である。

11 DES をはじめ多くのブロック暗号は、鍵長とブロック長が固定されている。この要件は、実装するアプリケーションに応じて鍵長を変更することができるように、アルゴリズムを設計することを意味している。

12 この要件は、AES が、専用チップによって暗号化・復号化の高速処理が可能となるアルゴリズムであると同時に、プログラムと汎用チップによって安価に実装することも可能となるアルゴリズムでなければならないということを意味している。

13 この要件は、AES のアルゴリズムを使用する場合に特許使用料等を支払う必要がないことを意味している。したがって、AES のアルゴリズムに特許が存在する場合、その特許所有者は AES の利用に対する特許使用料を請求しないことを表明しなければならない。なお、DES に関しては、DES の特許（U.S. Patent Number 3,962,539＜出願日 1975 年 2 月 24 日＞）を所有していた IBM 社がロイヤリティ・フリーでの DES の使用を容認すると表明したことについて、FIPS 46-2 に明記されている。

ハードウェアやソフトウェアで実装した場合の処理速度やメモリー容量に関する資料等を提出するように求められている。

### (3) AES の公募・審査手順

AES の公募・審査手順については、① NIST が発表した要件と評価基準に対するコメントを 1997 年 4 月 2 日まで募集する、②寄せられたコメントを参考にして、AES の技術的要件等を検討するワークショップを開催する、③最終的に決定された AES の基準等を基に、AES の候補となるアルゴリズムを公募する、というスケジュールの概略を発表した。

## 3. NIST 発表の AES の要件・評価基準に対する暗号学者や技術者等の反応

NIST が 1 月 2 日の発表内容に対して一般からコメントを募集した結果、暗号学者、技術者や金融関係者等から 25 通のコメントが寄せられた[14]。本節では、これらのコメントの内容を整理する。

### (1) 寄せられたコメントの内容

#### ①「AES として認定するアルゴリズムは、候補となる各アルゴリズムに対する暗号研究者等専門家の評価を考慮して決定される」点について

いずれのコメントも肯定的な見方であり、「インターネット上でアルゴリズムを公開すべきである」とか「アルゴリズムの強度等を研究者に検証してもらうべきである」とのコメントがあった。

＜コメント＞

- AES の候補となるアルゴリズムの詳細をインターネット等を利用して世界中に公開し、数多くの暗号研究者の評価をアルゴリズム選定の参考にすべきである。その場合には米国の暗号輸出規制に抵触する可能性があるが、候補となるアルゴリズムについてはその規制の例外として取り扱うべきである（Ronald Rivest[15]、MIT コンピューターサイエンス研究所教授）。
- AES の候補となるアルゴリズムの詳細な仕様を公開し、暗号研究者や技術者による評価を参考にしてアルゴリズムの選定を行うべきである（TIS 社[16]）。

---

[14] コメントの全文は、NIST[6]に公開されている。

[15] Ronald Rivest 氏は、RSA 暗号の発明者の一人である高名な暗号学者。共通鍵ブロック暗号の RC5 の発明者でもある。

[16] TIS（Trusted Information System）社は、米国 Maryland 州 Glenwood を本拠とする情報セキュリティ製品の有力なベンダー。暗号ソフトウェアの開発サポート、ファイヤーウォール製品の製造・販売やコンサルタント業務を行っている。

②「AES を共通鍵ブロック暗号とする」点について

多くのコメントがこの項目について触れず、鍵長やブロック長についてコメントを寄せており、その意味で肯定的な見方が多かった。ただし、「ブロック暗号よりも高速処理が可能なストリーム暗号[17]を最初から除外するのは不自然である」とのコメントもあった。

＜コメント＞

- ブロック暗号よりも高速処理が可能となるストリーム暗号も、候補に含めてもよいのではないか（Bruce Schneier、情報セキュリティコンサルタント）。

③「AES の鍵長は可変とする」点について

「この要件では、鍵長が一定である Triple-DES が対象外となってしまうため、要件を変更すべきである」とのコメントがあったほか、鍵長の上限や下限を設定するという要件に変えた方がよいとのコメントがあった。

＜コメント＞

- 鍵長を長くすると処理速度の低下を招くため、暗号の強度との間のトレードオフをどのように設定するかを検討する必要がある。それを踏まえて利用可能な鍵長の上限もしくは下限を設定すべきである（Bill Stewart、Netcom 社[18]）。
- 鍵長の上限を 256 bit とし、ブロック長の基準についても明確にすべきである。ブロック長は少なくとも 128 bit 以上とすべきであろう（Ronald Rivest、MIT コンピューターサイエンス研究所教授）。
- 鍵に付加されるパリティ・ビットは、ネットワーク間での相互接続性を損なう可能性があるほか、鍵の冗長性を増加させ解読を比較的容易にする可能性があるため、AES の要件で規定する鍵長にはパリティ・ビットを含めるべきではない（Cindy Fuller[19]、米国銀行協会）。
- 鍵が可変的なアルゴリズムをハードウェアにおいて実装するためには、鍵長の上限と間隔を決定しておく必要がある。例えば、鍵長の上限として、128～256 bit が妥当であると同時に、鍵長の間隔を 32 bit にして、128 bit、160 bit、...、224 bit、256 bit というように利用可能な鍵長の間隔を予め設定しておくことが必要であろう（反町亨[20]、三菱電機・情報技術総合研究所）。

---

17 ストリーム暗号は、暗号化するデータの各ブロック（1～数 bit 単位）に対応する鍵の系列（鍵ストリーム）を生成し、暗号化するデータの各ブロックとそれに対応する鍵ストリームの排他的論理和を計算することにより暗号化する方式である。データの処理速度に関しては、一般的には、専用チップを利用することによってブロック暗号よりも高速処理が可能になるといわれている。

18 Netcom 社は米国 California 州 Sun Jose を拠点としているインターネット・プロバイダー。

19 Cindy Fuller 氏は、米国銀行協会の職員で、ISO/TC68（国際標準化機構の金融専門委員会）と ANSI X9 の事務局長を務めている。

20 反町亨氏は、三菱電機・情報技術総合研究所において、暗号アルゴリズムの開発に従事している研究者。

④「AES **はソフトウェアにもハードウェアにも実装可能とする」点について**

「アルゴリズムを実装するアプリケーションを明確にすべきである」とか、「１つのアルゴリズムを AES として認定するのではなく、様々なアプリケーションに利用可能なように複数のアルゴリズムを AES として認定してもよいのではないか」といったコメントが寄せられた。

＜コメント＞

・ブロック暗号には様々な用途が存在するが、AES をどのようなアプリケーションに利用するのかを明確にした方がよい（Matthew Robshaw、RSA Laboratories[21]）。

・アルゴリズムをソフトウェアとハードウェアのどちらで実装するにせよ、ある一定水準以上の処理能力を要件として設定しておくことが重要である。例えば、ハードウェアで実装する場合、暗号化処理速度は 1Gb/s（Giga bit per second）以上となるアルゴリズムが望ましい（Thomas McDermott、NSA 情報システムセキュリティ部）。

⑤「AES **はロイヤリティ・フリーとする」点について**

多くのコメントが「AES に認定されるアルゴリズムがロイヤリティ・フリーとなることが好ましい」としている。

＜コメント＞

・AES に認定されるアルゴリズムはロイヤリティ・フリーとし、誰もが自由に利用できるようにすべきである（Thomas McDermott、NSA 情報システムセキュリティ部）。

⑥**アルゴリズムの評価基準について**

AES の候補となるアルゴリズムの評価基準については、「７つの評価基準を安全性、コスト、システムの柔軟性の３つに整理すべきである」といったコメントがあったほか、これらの評価基準について技術的側面から様々なコメントが寄せられた。

＜コメント＞

・AES の評価基準にどのようにプライオリティを付けるのかを明確に示すべきである。また、安全性とコストとの間のトレードオフをどう解決するのかも考慮する必要がある（Matthew Robshaw、RSA Laboratories）。

・AES の評価基準としては、安全性、コストとシステムの柔軟性の 3 つを重視すべきである。安全性に関しては様々な解読法に対するアルゴリズムの強度を評価し、

---

[21] RSA Laboratories は、RSA Data Security 社の研究所で、暗号研究や暗号ソフトウェアの開発、コンサルタントを行っている。RSA Data Security 社は、米国 California 州 San Francisco を本拠とする有力暗号ベンダーであり、公開鍵暗号方式の RSA 暗号や、共通鍵暗号方式の RC2、RC4 や RC5 を実装した暗号製品を供給している。

コストに関しては実装する場合に必要となる CPU やメモリー容量をベンチマークとするほか、システムの柔軟性については、どのようなアプリケーションに利用可能なのかを判断材料とすべきである（Cindy Fuller、米国銀行協会）。

・ソフトウェア上でのアルゴリズムの処理速度の測定は、比較的処理速度の遅い 8 bit のマイクロプロセッサーを利用して行うべきである。デスクトップパソコンの処理速度は年々向上しており、現時点で最高速のパソコン上で処理した場合にアルゴリズムによって速度に差が生じているとしても、近い将来その差は無視しうる程度のものになると考えられる。したがって、IC カードにも実装することを考慮して、8 bit のマイクロプロセッサーを利用するのがよいと考えられる（Bruce Schneier、情報セキュリティコンサルタント）。

**⑦　その他**

その他のコメントとしては、「AES に認定されるアルゴリズムは輸出可能とすべきである」とか、「DES から AES への移行が円滑に行われるように適切に対処するべきである」といったコメントがあった。また、AES の認定が終了するまでは Triple-DES を一時的に政府標準暗号として認定すべきだ、とのコメントもみられた。

＜コメント＞

- AES は世界規模での利用が可能となるアルゴリズムとして位置付けるべきであり、輸出可能となるような措置を講ずるべきである（TIS 社）。
- 海外からのアルゴリズムの応募も受け入れるべきである（Ronald Rivest、MIT コンピューターサイエンス研究所教授）。
- DES から AES への円滑な移行が可能となるように、移行スケジュール等の調整を念入りに行うべきである（Cindy Fuller、米国銀行協会）。
- DES の標準暗号見直しの期限である 1998 年末までに AES となるアルゴリズムを選定するのは時間的に困難であるため、AES の選定が完了するまでは Triple-DES を政府標準暗号として認定しておくとよい（Bruce Schneier、情報セキュリティコンサルタント）。

## 4. AES の要件・評価基準に対する FRB のコメント

このように新標準暗号に関する議論が高まる中で、暗号ユーザーである金融機関、とりわけ FRB も多大な貢献を行っている。FRB は、1997 年１月２日に NIST が発表した AES の要件・評価基準に対し、Raymond Romero 氏の名前で、以下の 8 項目のコメントを表明しており、AES の選定に協力する旨を発表している。これらのコメントは、ほぼすべて最終的な募集要項に盛り込まれた形となっている。

―― 現在、FRB は、金融機関との間で交換されるデータの暗号化アルゴリズムを DES から Triple-DES に移行するための検討を行っており、仮に Triple-DES を採用した場合、DES から AES への移行期間中は Triple-DES を利用する考えを明らかにしている（1997 年 4 月 2 日に対外公表、プレスリリースは別添参照）。

＜FRB のコメント＞

① ブロック長は 128 bit 以上に設定すべきである。

② 鍵長はその下限のみを規定して Triple-DES も候補となるように変更すべきである。

③ パリティ・ビットは、暗号文の冗長性を増加させ解読を比較的容易にする可能性があるほか、他のシステムとの相互接続性が確保されない場合もあるため、パリティ・ビットを鍵長に含めない扱いとすべきである。

④ アルゴリズムの特許については、ISO 等の国際標準化における特許の取り扱い方法（原則として、ロイヤリティ・フリーな技術でなければ標準化しない）を参考にすべきである。

⑤ アルゴリズムの評価基準は、より重要度の高い順に、安全性、システムの柔軟性、コストの３つに整理すべきである。

⑥ AES を様々なアプリケーションに利用可能にするために、複数のアルゴリズムを AES として認定するという選択肢も考慮すべきである。

⑦ DES から AES への移行について、コストをあまりかけずに円滑に実施できるように NIST は配慮すべきである。特に、移行期間中において DES または Triple-DES を利用する金融機関も存在すると予想されることから、NIST は DES に対して十分なサポートを引き続き行うべきである。

⑧ AES のアルゴリズム選定のための具体的なスケジュールを明示すべきである。

## 5. AES の募集要項の発表

NIST は、上記のコメント等を踏まえて、1997 年 9 月 12 日に AES の募集要項[22]を正式に発表し、① AES の候補となる暗号アルゴリズムが満足すべき要件（Minimum Accessibility Requirements）、②評価基準（Evaluation Criteria）、③知的所有権の扱いや、④今後の選定スケジュール、等について明らかにした。

### （1）AES が満たすべき要件

AES の候補となるアルゴリズムが満たすべき要件として、以下の４つが挙げられている。

① 共通鍵暗号であること。

② ブロック暗号であること。

③ 鍵長は 128 bit、192 bit と 256 bit が利用可能であること。

④ ブロック長は 128 bit が利用可能であること。

### （2）AES の評価基準

AES のアルゴリズムの評価基準として、安全性、コスト、その他のアルゴリズムの特

[22] AES の募集要項は、NIST[7]に公開されている。

徴、が挙げられており、この順番で評価基準の優先順位が付けられている。

**①　安全性（解読の困難性）**

安全性は最も重要な評価基準として位置付けられる。安全性の高さを判断する方法として、(i) 同一の鍵長とブロック長の下で解読の困難性について他の候補のアルゴリズムと比較する、(ii) そのアルゴリズムによって暗号化されたデータと、平文データをランダムに転置したデータとの間の類似性を評価する、(iii) そのアルゴリズムの安全性のベースとなっている数学的な根拠を評価する、(iv) アルゴリズムの評価プロセスの中で指摘された安全性に関する問題点があれば、それも評価項目として考慮する、といった方法が挙げられている。

**②　コスト**

コストについては、(i) ライセンス要件、(ii) 処理速度、(iii) 実装に必要なメモリー容量を考慮して評価するとされている。

ライセンス要件については、AES として認定されるアルゴリズムはロイヤリティ・フリーの取り扱いが可能かどうかが評価対象となる。処理速度に関する評価は、ソフトウェアで実装する場合とハードウェアで実装する場合の両方のケースにおいて行われるが、技術的評価第一ラウンドにおいては鍵長とブロック長をそれぞれ 128 bit とした場合の処理速度が測定され、技術的評価第二ラウンドにおいては鍵長 128 bit とブロック長 128 bit の組み合わせ以外の組み合わせで処理速度が測定される。この 2 つのラウンドにおける測定結果が評価対象となる。また、実装に必要となるメモリー容量については、ハードウェアに実装する場合には必要となるゲート数[23]が、ソフトウェアに実装する場合には RAM の容量が評価対象として利用される。

**③　その他のアルゴリズムの特徴**

その他の評価基準とされるアルゴリズムの特徴として、(i) 様々なアプリケーションへの利用可能性、(ii) ハードウェアやソフトウェアへの適用性、(iii) 構造の単純性、が挙げられている。

様々なアプリケーションへの利用可能性については、例えば、ATM ネットワークや衛星通信等のアプリケーションでも利用可能かどうか、ストリーム暗号、メッセージ認証コード（MAC）、疑似乱数生成装置やハッシュ関数等にも利用可能かどうか等について評価される。ハードウェアやソフトウェアへの適用性に関しては、そのアルゴリズムがハードウェアにのみ実装可能である場合等、用途が制限されていないかどうかについ

[23] ゲートは、電子回路のパーツの１つで、入力端子に与えられた入力信号を論理演算によって処理し、その結果を出力端子から出力する機能をもつ。

て評価される。

### (3) アルゴリズムに関する知的所有権の取り扱い

AES として認定されたアルゴリズムは、ロイヤリティ・フリーの扱いとされる。この方針に沿って、NIST は、アルゴリズムの特許所有者やアルゴリズムを実装したアプリケーションの特許所有者に対して、「アルゴリズムが AES として認定された場合、そのアルゴリズムの使用はロイヤリティ・フリーとする」旨を明記した約定書の提出を要求している。

### (4) 今後のアルゴリズム評価・選定スケジュール

今後のアルゴリズムの評価・選定のスケジュールは以下の表１の通り。

**表１：今後のアルゴリズム評価・選定スケジュール**

| フェーズ | 作業内容等 |
|---|---|
| ① 候補となるアルゴリズムの募集（締め切り日：1998 年 6 月 15 日） | 提出資料に不備がないかどうかをチェックし、暗号輸出規制と整合的な形ですべてのアルゴリズムを公開し、一般からのコメントを募集する。 |
| ② 第一回 AES 候補コンファレンス（日程：1998 年夏、具体的な日程は未発表） | 候補の暗号アルゴリズムの提案者がアルゴリズムの説明を行い、コンファレンス参加者からコメントを得る。 |
| ③技術的評価第一ラウンド | NIST は、第一回のコンファレンスで得たコメントを参考にして候補のアルゴリズムの強度および弱点等を評価し、満たすべき要件を満足しているかどうかをチェックする。アルゴリズムの絞り込みも行う。 |
| ④第二回 AES 候補コンファレンス（第一回コンファレンスの約６か月後開催予定） | NIST による技術的評価第一ラウンドの評価に関して議論するほか、候補アルゴリズムの一層の絞り込みを行う際の留意点について検討する。 |
| ⑤技術的評価第二ラウンド | NIST は、安全性、処理速度やアルゴリズムの知的所有権に関してより詳細に検討を行い、候補のアルゴリズムを５つ以下に絞り込む。NIST は、絞り込まれた候補アルゴリズムを公表し、それらに対するコメントを募集する。 |
| ⑥第三回 AES 候補コンファレンス（技術的評価第二ラウンドの結果発表の６～９か月後に開催予定） | 技術評価第二ラウンドの NIST の選定に対し、一般からのコメントを集約するとともに、アルゴリズムの一層の絞り込みについて検討する。 |
| ⑦ NIST による最終選定 | NIST は、AES の候補となるアルゴリズムを決定し、一般からのコメントを募集する。 |

DES から AES への移行について、NIST は、「DES の標準暗号見直しが行われる 1998 年 12 月までには、AES の選定プロセスは終了しないと考えられる。したがって、アル

ゴリズムの移行をいかに円滑に進めるかについては、今後関係者と協議しつつ決定する」としている。また、技術的評価の２つのラウンドの概要は以下の通り。

① 技術的評価第一ラウンド

評価第一ラウンドでは、主に（i）鍵長とブロック長の組み合わせの利用可能性、（ii）提出されたアルゴリズムの処理結果の正確性、（iii）処理速度が検証される。

鍵長とブロック長の組み合わせの利用可能性については、鍵長、ブロック長とも 128 bit に設定し、実際にデータの暗号化が可能かどうかが検証される（これら以外の組み合わせでの利用可能性は第二ラウンドで検証される）。また、アルゴリズムの処理結果の正確性については、予め提出されたサンプルデータを実際にそのアルゴリズムのプログラムを使って暗号化し、その暗号化データと予め提出されたサンプルデータの暗号化データが一致するかどうかが確認される。処理速度の検証では、鍵長、ブロック長をそれぞれ 128 bit に設定した場合、暗号鍵のセットアップ、暗号鍵の変更や、暗号化・復号化にそれぞれどの程度の時間がかかるのかが測定される。

── NIST がアルゴリズムの評価に利用するパソコンは、200MHz の Intel Pentium Pro Processor と 64MB RAM を搭載し、OS として Windows95 がインストールされている IBM PC 互換機とする。またコンピューター言語としては、C 言語と Java が利用される。

② 技術的評価第二ラウンド

評価第二ラウンドでは、鍵長とブロック長の組み合わせが 192-128 bit と 256-128 bit の場合の（i）利用可能性と（ii）処理速度が検証される。処理速度に関しては、アルゴリズムのセットアップ、暗号鍵のセットアップ、鍵の変更、暗号化および復号化の処理速度を計測し、評価する。

## 6. 今後の展望

NIST が発表した募集要項によって、AES の候補となるアルゴリズムは共通鍵ブロック暗号に限定されたほか、その鍵長、ブロック長についても明らかにされた。そこで、現在 ISO の暗号アルゴリズム登録制度[24]に登録されている１４の暗号アルゴリズムのう

[24] ISO の暗号アルゴリズム登録制度は、情報セキュリティ技術の標準化を担当する ISO/IEC JTC1/SC27（以下、SC27）が、暗号化機能を有する製品の流通性を高めるために、1991 年にその登録手続きを ISO/IEC 9979 Information technology - Security techniques - Procedures for the registration of cryptographic algorithms に定めたことから発足した。アルゴリズムを登録するためには、アルゴリズムの ISO エントリー名、固有の名称、適用範囲（データの秘匿、認証等）、入出力のパラメーター等９つの必須項目と４つの選択項目を登録機関（現在、英国

ち、アルゴリズムの詳細な仕様が公開されている方式の中で、候補となるアルゴリズムの要件を満足するものがあるかどうかを調べてみる（表２参照）。まず、登録アルゴリズムの中で詳細な仕様が公開されている共通鍵ブロック暗号は７つ存在するが、その中で鍵長が 128 bit 以上のアルゴリズムは、IDEA、MULTI2、FEAL と MISTY1 の４つである。しかし、いずれもブロック長が 64 bit となっており、現時点で ISO に登録されているアルゴリズムのうち、AES の要件をすべて満足するアルゴリズムは存在せず、仮にこれらのアルゴリズムを利用するとしても改造を加える必要があると考えられている。

**表２：ISO に登録されている暗号アルゴリズム**

| | 暗号<br>アルゴリズム名 | アルゴリズムの公開の有無 | 登録日 | 提案者（開発者） | 鍵長とブロック長 | |
|---|---|---|---|---|---|---|
| | | | | | 鍵長 | ブロック長 |
| 共通鍵ブロック暗号 | IDEA | 公開 | 1993 年 5 月 10 日 | スイス・Ascom・Tech 社 | 128 bit | 64 bit |
| | DES | 公開 | 1994 年 9 月 5 日 | 米・NCS[25]（IBM 社） | 56 bit | 64 bit |
| | CDMF | 公開 | 1994 年 10 月 29 日 | 米・IBM 社 | 40 bit | 64 bit |
| | Skipjack | 非公開 | 1994 年 10 月 31 日 | 米・NSA | 80 bit | 64 bit |
| | RC2 Symmetric Block Cipher | 非公開 | 1994 年 10 月 31 日 | 米・RSA Data Security 社 | 可変 | 64 bit |
| | MULTI2 | 公開 | 1994 年 11 月 14 日 | 日・日立製作所 | 256 bit | 64 bit |
| | FEAL | 公開 | 1994 年 11 月 14 日 | 日・NTT | 128 bit | 64 bit |
| | SXAL/MBAL | 公開 | 1995 年 10 月 23 日 | 日・ローレル・インテリジェント・システム社 | 64 bit | 可変 |
| | MISTY1 | 公開 | 1996 年 11 月 27 日 | 日・三菱電機 | 128 bit | 64 bit |
| | ENCRiP | 非公開 | 1997 年 2 月 12 日 | 日・日本電気 | 64 bit | 64 bit |
| その他 | B-Crypt | 非公開 | 1992 年 8 月 19 日 | 英・British Telecom 社 | （ストリーム暗号） | |
| | LUC Public-Key Cryptosystem & Digital Signature | 公開 | 1994 年 7 月 20 日 | ニュージーランド・LUC Encryption Technology 社 | （公開鍵暗号） | |
| | RC4 Symmetric Stream Cipher | 非公開 | 1994 年 10 月 31 日 | 米・RSA Data Security 社 | （ストリーム暗号） | |
| | BARAS | 非公開 | 1995 年 8 月 18 日 | フランス・ETSI[26] | （詳細不明） | |

（注）シャドーのかかっているアルゴリズムは、詳細な仕様が公開されている共通鍵ブロック暗号である。

また、これらの既存のアルゴリズムとは別に、例えば DES の原形を開発した IBM 社

---

National Computing Centre）に報告する必要がある。ただし、アルゴリズムの詳細な仕様を報告する義務がないため、データ処理過程が十分公開されていないアルゴリズムも登録の対象となるほか、登録機関等によるアルゴリズムの強度評価は登録手続きに盛り込まれていない。

[25] NCS（National Communications System）は、米国防総省の下部組織の１つで、主として災害等の非常時における政府の情報通信ネットワーク確保のために、政府の情報通信インフラの整備や関連技術の標準化等の役割を担っている。

[26] ETSI（European Telecommunications Standards Institute）は、418 のヨーロッパ各国の標準化組織や企業によって構成される、情報通信技術に関する標準化団体。

等が新しい暗号アルゴリズムを応募する可能性もある。

NIST が発表したアルゴリズム選考スケジュールによれば、応募されたアルゴリズムの１つが AES として正式に認定されるまでに、１年以上の時間が必要となることがわかる。しかし、AES が、アルゴリズムの強度に対する高い信頼を得て、実際に幅広い分野で利用されるようになるためには、AES の標準化終了後さらに数年はかかると考えられる。こうした AES を巡る動きについては、将来金融分野におけるデータ暗号化手段にも大きな影響を与えると考えられるため、今後も注目していく必要があろう。

以　上

## 参考文献


[1]Kusuda, K. and T. Matsumoto, “A Strength Evaluation of the Data Encryption Standard,” IMES Discussion Paper Series 97-E-5, Institute of Monetary and Economic Research, Bank of Japan, August 1997.

[2]Menezes, A. J., P. C. Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[3]Morita H., “Registration and Standardization of Cryptographic Algorithms in the SC 27 Committee,” Workshop on Design and Evaluation of Cryptographic Algorithms, Nov 27, 1996.

[4]National Institute of Standards and Technology, “Data Encryption Standard（DES）,” Federal Information Processing Standards Publication（FIPS PUB）46-2, December 13, 1993.

[5]National Institute of Standards and Technology, “Announcing Development of a Federal Information Processing Standard for Advanced Encryption Standard,”（URL: http://csrc.nist.gov/encryption/aes/aes_fr1.txt）, January 2, 1997.

[6]National Institute of Standards and Technology, “AES Comments（e-mail）,”（URL: http://csrc.nist.gov/encryption/aes/comments.txt）, April, 1997.

[7]National Institute of Standards and Technology, “Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard（AES）,”（URL: http://csrc.nist.gov/encryption/aes/aes_9709.htm）, September 12, 1997.

[8]Schneier, B., *E-mail Security*, John Wiley & Sons, Inc., 1995.

（別添）

# FRB による Triple-DES 評価に関するプレス・リリース

For Release:
April 2, 1997

Contact:
Joe Elstner, St. Louis - (314) 444-8902
Sandra Conlan, San Francisco - (415) 974-3231
Gwen Byer, Richmond - (804) 697-8105

## Federal Reserve is Evaluating Triple DES

ST. LOUIS--The Federal Reserve is evaluating an advanced application of the Data Encryption Standard (DES), known as Triple DES, to protect data that are transmitted electronically between the Federal Reserve Banks and between the Federal Reserve and financial institutions. Federal Reserve officials said that if the new standard proves effective, an announcement about actual implementation can be expected in early 1998.

The Federal Reserve is an active participant in the X9 committee of the American National Standards Institute (ANSI), which is completing a standards document for Triple DES. "Our active role in developing improved data security techniques, of which Triple DES is one component, helps provide assurance that transactions with the Federal Reserve will continue to be safe and secure from cryptographic crime," said Bruce J. Summers, director of automation resources for the Federal Reserve. "This year we will be testing Triple DES and working on an implementation plan, coordinating with vendors of encryption products and our customers."

The Federal Reserve currently uses DES to secure electronic information and will spend the next several months completing its analysis of Triple DES. "Triple DES significantly increases data security because it invokes DES three times," Summers said. "With each iteration, it is possible to use a different encryption key value, which results in a longer overall key value that is far more

resistant to attack." Certain Triple DES operating modes are also compatible with the Fed's current DES implementations, which will ensure a smoother transition for Federal Reserve customers.

The Fed is also following a National Institute of Standards and Technology (NIST) project to develop an advanced encryption standard to eventually replace DES. Summers believes that, while the Fed should closely monitor such activities and study other options being developed, it must be at the forefront of data security implementations and be prepared to use Triple DES to provide continued security until a new standard is ready. "Our evaluation of Triple DES is a continuation of the Fed's efforts to ensure that the highest levels of security are applied to Federal Reserve operations and payment services," said Summers.