情報処理最前線

共通鍵ブロック暗号 AESの経緯と今後の展望

下山 武司
通信・放送機構

カリフォルニアの朝

アメリカ西海岸の小さな町，ヴェンチュラには澄み切った青空が広がっていた．ホテルの窓からは，4，5階のビルに相当しそうな高いソテツが，駐車場に沿ってきちんと等間隔に並んで生えていた．それほど入念な手入れをしているようには思えないのだが，空の青さをバックに高い位置できれいに広がっている大きな葉を見ていると，仕事で来ているのをすっかり忘れてしまうようであった．それを思い出させたのは，思わず窓を開けてみたときに吹き込んできたカリフォルニアの朝の冷たい空気に触れたときである．

-------- -------- --------

AES会議初日の朝は，こうして迎えました．昨晩のE2作戦会議の雰囲気が抜け切らないまま眠りについたため，自分が発表するわけでもないのに，朝からなぜか緊張していたのを憶えています．ヴェンチュラはサンフランシスコとロスアンゼルスを3対1ぐらいに分けた辺りに位置するカリフォルニア海岸沿いのリゾート地です．ほとんど雨が降らず，昼は日光がさんさんと照りつけて暑いですが，夜になるとカリフォルニアの海を流れる寒流と，突き抜けるような青空がもたらす放射冷却の影響で非常に寒くなります．この朝は，一段と冷え込みが激しかったのかと思いきや，カリフォルニアで暮らしている日本人に聞いたところでは，決してそうではなかったようです．この地方にとってはごく普通の1日の始まりでした．

さてこの原稿は，タイトルから一目瞭然のことながらAESに関する話題について書かれようとしているのですが，読者の方々の中には「なにを今さら」と思われる方もいらっしゃるではないでしょうか．これまでに書かれたAESに関する記事といえば，思いつくだけでも(1)五十嵐幸雄さん（日経），勝村幸博さん（日経）によるAES会議速報[1), 2)]，(2)宇根正志さん（日本銀行）による各AES候補に関する詳細な分析結果[3), 4)]，(3)鈴木裕信さんによる旅行記エッセイ風会議報告[5), 6)]，その他，国内会議での報告など[7), 8)]，すでにいくつもの記事が世の中に出回っていまして，もはや速報性は失われてしまいました．それに加え，この記事が世に出る頃には，そろそろローマで第2ラウンドが始まる頃でして，いまさら第1回AES会議の報告なんか，と思われるのがむしろ自然かもしれません．というわけで，この記事に何か新しい情報を期待された方にはちょっとがっかりさせてしまうかもしれません．とはいえ，新しく書くことが何もなくなってしまったわけでもありませんし，「AES？　それって何？」という方もいらっしゃるでしょう．ですから，重複を恐れずどしどし書き進めるとしましょう．

暗号を取り巻く背景～ところでAESって何？

今まで説明もなくAESというものを取り上げてきましたが，ここでAESとは一体何なのかを解説します．

AESというのはAdvanced Encryption Standardの略で，アメリカのNIST（National Institute of Standard Technology）が中心となって選定が行われている次世代の共通鍵ブロック暗号のことです．

暗号は大きく分けて，公開鍵暗号と共通鍵暗号に分類できます．共通鍵暗号は，暗号文の送り手と受け手が同じ鍵（＝秘密情報）を共有していることを前提に送信される暗号の総称で，高速な暗号化処理が行えるという特徴を持っています．たとえば最近のパソコンでは数十Mbit/s程度の暗号化が実現できます．携帯電話や銀行間のデータ通信など，高速な暗号化データ送信が必要とされる分野に応用されています（**図-1**）．

一方，公開鍵暗号は，送り手と受け手が異なる鍵を用いる暗号で，送り手側の鍵（暗号化鍵）が公開されている暗号です．暗号化鍵は暗号文を作るためにのみ使えるもので，復号には使えません．暗号文を復号をするためには，暗号文を受ける側のみが持つ鍵（復号鍵）が必要となります．そのため，生成された暗号文は暗号文を盗聴した者はもちろん，送り手自身ですら暗号文のみからは平

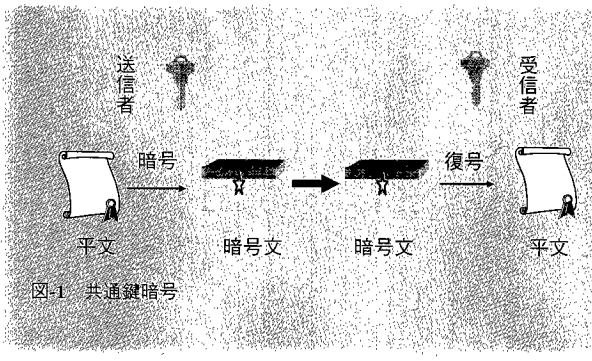

図-1　共通鍵暗号

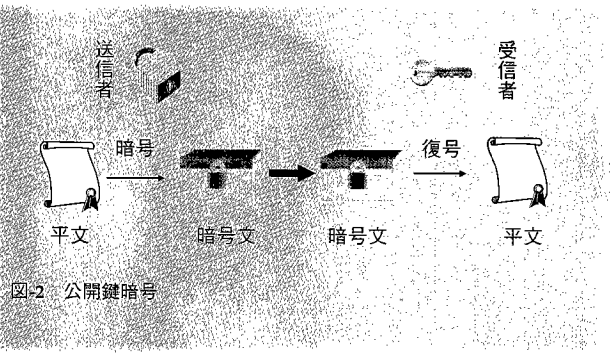

図-2　公開鍵暗号

CAST-256	Canada	Entrust Technologies, Inc.	構造はシンプル．しかし速度は遅い．
CRYPTON	Korea	Future Systems, Inc.	知名度は低いが高速．安全性は大丈夫か？
DEAL	Canada	Richard Outerbridge and L.Knudsen	DES 6回分．遅すぎる．
DFC	France	Centre National pour la Recherche Scientifique	差分・線形攻撃に対して証明可能安全性を持つ．
E2	Japan	NTT	あらゆる攻撃を検討．チップも試作．ダークホース？
FROG	Costa Rica	TecApro International S.A.	会議直前に攻撃される．
HPC	USA	Richa Schroeppel	スパイスというパラメータ付き．
LOKI97	Australia	L.Brown, J.Pieprzyki, J.Seberry	差分攻撃で解読済み．
MAGENTA	Germany	Deutsche Telekom AG	会議中に解読される．鍵スケジュールが問題．
MARS	USA	IBM	本命の1つ．ただし鍵にコリジョンあり．
RC6	USA	RSA Laboratories	RC5の経験を基に設計．最も高速．
RIJNDAEL	Belgium	J.Daemen and V.Rijmen	独特な構造を持つ．比較的高速．
SAFER+	USA	Cylink Corporation	暗号界の大御所が設計．でも魅力がない．
SERPENT	UK, Israel, Norway	R.Anderson, E.Biham, L.Knudsen	段数が多い．Bitslice法で高速実装が可能．
TWOFISH	USA	Counterpane Systems	鍵によってS-boxの構造が変化．

［AES候補に漏れた暗号］
GEM（Lance Gharat），RAINBOW（Samsung Advanced Institute of Technology），Simple（Richard Frank），TMD（Jonathan Stielbel (of Mobile Safe LLC)），Vobach Technology（Design Automations Systems, Inc.），WICKER'98（LAN Crypto, Inc.）

表-1　AESの表

文を復号することができません．この性質から，暗号化鍵は秘密にしておく必要がなく，まるで電話番号のように公開しておけるわけです（**図-2**）．

公開鍵暗号は，個人認証や鍵配送など広い応用範囲があります．おおざっぱに言って，共通鍵暗号を用いた機能は公開鍵暗号でも実現することができます．しかし公開鍵暗号は素因数分解や楕円曲線上の離散対数問題などの数学的な理論に基づいた複雑な処理を行って実現されており，高速な暗号通信にはあまり向きません．いくら公開鍵暗号が万能とはいえ，今後すべての暗号通信が共通鍵暗号から公開鍵暗号に置き換わるというようなことはないであろう，という考えが情報セキュリティ研究者の間では一般的です．

DESからAESへ〜壇上に上がった候補たち

共通鍵暗号の1つに共通鍵ブロック暗号という種類の暗号があります．共通鍵ブロック暗号というのは，平文をある決まった長さに区切られた，ブロック単位ごとに同じ鍵で暗号化操作を行うという暗号のことで，乱数表や算術演算を組み合わせて構成されています．さて，これまで共通鍵ブロック暗号の事実上世界標準としてDES（Data Encryption Standard）という暗号が使われてきました．DESは1977年に制定された暗号で，NISTの前身であるNBS（National Bureau of Standard）の公募に対して，唯一IBMによって応募されたアルゴリズムを基礎としています．その暗号化アルゴリズムの仕様が完全に公開された暗号として，画期的であった反面，制定当初から安全性に関してさまざまな議論がなされていました．1つの大きな点としては設計基準の不透明性によるものがあります．仕様が公開されているとはいえ，なぜそのように設計されているのかという設計基準に関する情報がNSA（National Security Agency）の要請により非公開とされてきた関係で，設計者だけが知り得る解読法が存在するのではないかという憶測が生まれました．またもう1つには，56ビットという鍵の長さに関する議論があります．56ビットといえば約72京個の異なる鍵があるわけで，一見すると非常に大きな数のように見えますが，計

■潜入！E2作戦会議室

第1回AES会議の会場に指定されていたホテルには，カナダのキングストンから丸1日飛行機を乗り継いで，会議前日に到着していました．

今回の海外出張はSAC'98，AES，CRYPTO'98と暗号関係の国際会議を「はしご」するもので，私にとってこのような2週間にも及ぶ長期海外出張は初めての経験でした．

会議が始まる前の晩は，2日後に発表を控えたE2の発表練習場に，持ち前のずうずうしさと社交性を乱用して，もぐり込んでしまいました．練習室として暫定的に指定されたのは，ホテル内の太田和夫さん (NTT) の部屋．この部屋にE2関係者，総勢8人+αが集まり，夜更けまで発表練習をしていました．発表者の盛合志帆さん (NTT) は，流暢な英語とよく通る声を武器に，E2を印象づけようと一生懸命．関係者+一部部外者があれこれと意見を言い合っているうちに，プレゼンテーション用に準備されたPowerPointにどんどん修正項目が加わっていきました．係になっている大久保美也子さん (NTT) は，発表当日の朝まで日本から担いできたPCを使って徹夜で修正作業をしたそうです．

見ている側にとっては，候補が絞られていく過程というのは，まるでクイズ番組でも見ているかのように，結構スリリングで面白いところがありますが，立候補している側にとっては，解読されてしまうのはむろん論外としても，誤解から生じた些細なうわさや評判でさえ命取りになりかねないとして，不利になりそうな種を早いうちに摘み取ろうと必死だったようです．傍目にはやや神経質にすら感じました．会議に参加していたVaudeny (DFCの提案者) に感想を聞いたところでも「SERPENTは大胆．E2は臆病．」と2つのAES候補に対照的な印象を持ったようです．E2の関係者にとってはAES会議中だけでなく後に続く国際会議であるCRYPTO'98が終わるまでの間，特にランプセッションまでは気の抜けない緊張状況の連続だったようです．

現在 (1998年11月末) でも朝出勤したら，Internet NewsやAES Electronic DiscussionなどのAESが関係するネットワーク討論の場を隅々まで欠かさずチェックすることが，E2関係者の日課になっているとか．

算機の進歩や，複数の計算機をネットワークを介して利用するネットワークコンピューティングと呼ばれる方法が普及してきたことで，現在では見かけほど十分安全な数ではなくなってきています．さらに1997年にはRSA社によるDES解読コンテストのように解読への動機付けを与えるようなイベントが何回か行われ，最近では単一組織が持てるレベルの計算機資源を用いるだけで，わずか3～4日で解読されてしまうようになってしまいました．また1990年以降急速に発達した差分攻撃法，線形攻撃法といった暗号解析理論の進歩も，DESの安全性をおびやかす一因となっています．

とはいえ，このような結果からDESで暗号化されたすべての暗号が直ちに解読されてしまうというわけではありません．しかし将来に渡って使い続けていく限り，いつかは本当の意味で安全な暗号ではなくなる日が来ることは容易に想像できます．

そこでDESに続く次世代の共通鍵ブロック暗号として，より安全で高速演算が可能な暗号が必要になってきたわけです．DESを選定した組織であるNISTの企画によって，DESに続く新しい共通鍵ブロック暗号を世界中から募集し，互いを競わせるというシステムによって選定するプロジェクトが始まりました．この暗号がAESと呼ばれているものです．現時点ではAESはある1つの決まった暗号を指しているわけではありません．AESが決まるのは2000年の夏頃です．NISTからの情報によるとAESに応募された暗号は全部で21個あり，そのうちの書類が不備であった6個を除いた15個が候補として壇上に上がる権利が得られました（**表-1**）．

▶第1回AES会議～そしてビデオは横浜に

第1回AES会議では，候補となった15個の暗号が正式にお披露目されました．いくつかの暗号は，会議前にすでに公表されていましたが，SERPENTのように会議前に発表されたもの（FSE'98）と名前が同じでも仕様の一部が異なったりして，必ずしも同じ暗号とは限りませんでした．

この会議中に話題となった代表的なトピックスをいくつか挙げてみます．MAGENTAが発表直後に安全性に問題あることが指摘されたり，MARSを提案したIBMの研究者がNISTの指定した暗号性能評価であるPentium-Pro 200MHzおよびBorland C++を用いた方法では，公平な評価が得られるとは限らないことを実際に数値を出して指摘したり，RivestによるRC6の概要説明発表中でRC5から7ステップの変更だけでRC6を得ることができるという主張を受けて，BihamがRC6からSERPENTを7ステップで，またSchneierがSERPENTからTWOFISHを7ステップで得る方法を示したりして，会場を大いに沸かせました．日本から提案された唯一の暗号E2は，完成度の非常に高いプレゼンテーションで聴衆を注目させるとともに，全暗号候補の中で唯一ハードウェアによる実装を写真で示し，非常に好評でした．これら会議の模様は，すべてビデオに収めてあります．ビデオは，通信・放送機構，横浜リサーチセンターが所有しています．ほかにもいくつかトピックスがあるのですが，それらについては文献1)，2)，5)，6)など，臨調感あふれる文章で書か

■7ステップ？

RC5からRC6への7つのステップ (Rivest (RSA))

1. RC5から始めます．
2. 掛け算と巡回シフトを加えます．
3. XOR入力としてBではなくtを使います．
4. 2つのRC5を並べます．
5. 出力を交換させます．
6. 暗号化の始めと終わりにホワイトニング処理を行います．
7. 安全性を保つため段数を20とします．

RC6からSERPENTへの7つのステップ (Biham (Technion))

1. RC5から始めます．
2. 7ステップを経てRC6を得ます．
3. 掛け算を取り除きます．
4. 巡回シフトを取り除きます．
5. Sボックスを加えます．
6. 伝統的なデザインを加えます．
7. ビットスライス法を適用させます．

SERPENTからTWOFISHへの7つのステップ (Schneier (Conterpain))

1. フェイステル構造を加えます．
2. Sボックスを拡張し複雑にします．
3. ビット置換を1ビット巡回シフトに置き換えます．
4. 角 (Square) を曲がります．
5. 安全 (SAFER) に運転します．
6. 野球のバットを使って鍵スケジュールをします．
7. 解析，最適化，解析，最適化...

DESからAESへの7つのステップ (Smid (NIST))

1. 自分の上司にDESはもはや安全ではないことを説得します．
2. 自分の上司にTriple-DESよりAESの方がいいことを説得します．
3. 世界の暗号研究者に自分の作った暗号を公開します．
4. 世界の暗号研究者の作った暗号を解読します．
5. 輸出規制法違反で逮捕されないよう自己防衛します．
6. 総意がまとまることを祈ります．
7. もしだめだったらAESは結局DESです．

れている会議報告がいくつかありますので，それも参照していただければと思います．今後AESが決まるまでには，提案者やその他の暗号研究者による生き残り合戦が繰り広げられるでしょう．第2回AES会議は，ローマで行われる共通鍵暗号の国際会議であるFSE'99（3月24～26日）の直前3月22，23日に，同じくローマで行われます．果たして，生き残る暗号はどれか！

MAGENTAの解読～プリンタ持って会議に行こう

今書いている文章について，これまで研究者以外の人の手で書かれたAES会議報告とは一味違ったものにしたいので，AES会議中に解読されたという暗号，MAGENTAの解読法について，少し解説するとしましょう．技術的な用語が並び多少難しく長いかもしれません．

MAGENTAはドイツ版NTTともいうべき会社のドイツテレコムのK.HuberとM.Jacobson, Jr.が提案したAES候補暗号です．配布資料によれば，すでにドイツテレコム社内では実際に使われている暗号だそうです．暗号化関数全体は6段フェイステル構造をしています．各段のラウンド関数には$GF(2^8)$上の指数関数とFFT構造を組み合わせており，差分攻撃，線形攻撃に対して十分な強度を持っています．提案発表の最後には，「知られた最良の攻撃法は全数探索法である．」と締めくくっていました．

たしかにラウンド関数はそれなりによくできていて，ここを攻撃しても解読するのは難しそうです．実際，MAGENTA発表直後に議論となったのはラウンド関数に関してではありません．というよりラウンド関数にはノータッチです．

まず，MAGENTAの解読に関して口火を切ったのはFarguson（Counterpane）でした．MAGENTAの発表終了直後のことです．彼の考えによれば2^{96}個の平文暗号文組みがあれば鍵を求めることができるというのです．2^{96}個という数は，全数探索するよりも少ない量ですので，もし彼の考えが正しければ，理論的な意味ではこの時点で「解読できた」ということになるわけです．それを聞いたBihamらが，もっと改良できるかもしれないと言い始めました．

MAGENTAの発表セッションが終わった後，提案者のJacobsonと，先程の人たちを含む世界のトップ暗号研究者6人Biham，Biryukov，Ferguson，Knudsen，Schneier，Shamirが，会場の中央に1カ所に集まり，あれこれ言い合っている間に，どうやらMAGENTAは解読されてしまったようです．問題は，鍵スケジュールという部分にありました．彼らによる攻撃法を用いれば，MAGENTAが採用したのと同じ鍵スケジュール構造が使

われた暗号は，MAGENTAに限らずどんなラウンド関数を使っていようとも解読できてしまうというわけなのです．

MAGENTAの鍵スケジュールとは，暗号化鍵128ビットKを64ビットずつK_1とK_2に分け，6段のラウンド関数のうち1，2，5，6段目にはK_1を，間の3，4段目にはK_2を用いるというきわめて単純な構造をとってます．この単純な構造が命取りになりました(図-3)．

以下，彼らによる攻撃法を説明しましょう．

彼らが見つけた攻撃法は2種類あります．1つは2^{64}個の選択平文暗号文組みと2^{64}回の暗号化操作を使って解読する方法［解読1］，もう1つは2^{33}個の既知平文暗号文組みと2^{97}回の暗号化操作を使って解読する方法［解読2］です．いずれの解読法も3段目のラウンド関数に着目しています．

まず記号の説明をしておきましょう．ラウンド関数をEとし，64ビット拡大鍵をK_1，K_2とします．X_iはi段目の128ビット出力とし，X^TをXの上位64ビット，X^Bを下位64ビットとします．

［解読1］

1．任意の平文X_0について，未知の鍵Kで暗号化された暗号文X_6を生成します．
2．2^{64}個の鍵候補K_1'について，以下を行います．
(a) X_0から2段目出力候補X_2を計算します．
(b) $X_2^T = X_2'^T$を満たすX_2'を任意に選びます．
(c) X_2'をK_1'で復号し，平文X_0'を得ます．
(d) X_0'を未知の鍵Kで暗号化してX_6'を得ます．
(e) X_6とX_6'を候補鍵K_1'で復号し，X_4とX_4'を得ます．
(f) X_2，X_4およびX_2'，X_4'のXORで3段目のEの出力を比べます．
(g) もし等しくなければ，K_1'を鍵候補からはずして次の候補に移ります．
3．上記をパスした鍵候補リストを作ります．

本当の鍵であれば鍵候補リストに残りますし，偽の鍵は別の平文を用いてチェックすることで簡単に弾くことができるはずです．これで拡大鍵K_1を求めることができました．拡大鍵K_2に関しては何も言ってませんが，共通鍵ブロック暗号の分野では，これだけでも解読されたと認められることになっています．1つの拡大鍵でも求められたということは，鍵に関する情報がたとえ一部といえども漏れてしまったことに変わりありませんから(この意味での解読を専門家の間ではInformation deductionと呼んでいます)．

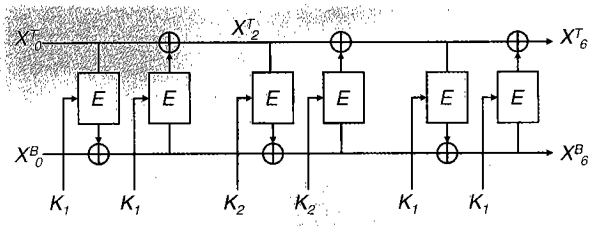

図-3 MAGENTAの暗号化アルゴリズム

［解読2］

続いて2^{33}個の既知平文暗号文組を用いた解読を示します．この解読法はBirthday paradoxと呼ばれる手法を用いています．

1．2^{64}個の鍵候補K_1'について以下を繰り返します．
(a) 2^{33}個の平文X_0についてX_2を計算します．
(b) X_2^Tが一致する平文対を探します．
(c) それぞれの暗号文X_6からK_1'を用いてX_4を計算します．
(d) それぞれのX_2，X_4のXORから3段目Eの出力を比較します．
(e) 一致しなければK_1'を棄却し次の鍵候補について調べます．
2．上記を満足した鍵候補リストを作ります．

解読2も解読1と同様にして，拡大鍵K_1を求めることができます．

このようにしてMAGENTAは，理論的には解読することができたわけです．しかし，ここで言っておかなければならないのですが，MAGENTAはあくまでも全数探索と比較した場合に，それより少ない計算量で鍵の一部の情報を得ることができたという意味でしかありません．DESのように3～4日計算機をまわせば文字どおり「暗号文から平文を解読」できるというわけではないのです．現実的にいえば，MAGENTAで暗号化された暗号文を現在の計算機能力を用いて解読することはまだまだ難しいはずです．たとえAES候補としては脱落しても，誰かがMAGENTAを使っていたとして不思議はありません．こういうことは誰も書かないので，あえて書いておきました．以上でMAGENTAの解読アルゴリズムの説明を終わります．さて，最後に会議2日目の出来事を．

AES会議の2日目の朝もビデオ設置のための最前席を確保しておこうと，早めに会場に行きました．会議場の入口には昨日と同様，部屋へ入るとき必ず目に止まる位置に横長の会議机が置いてありました．この机には，近々行われる国際会議の案内やAES会議で発表者が用いたOHPのコピーなどが並べられています．こういった机は研究集会ではよくあるもので，並べられた資料のほとんどは参加者が事前に用意してきたドキュメントです．と

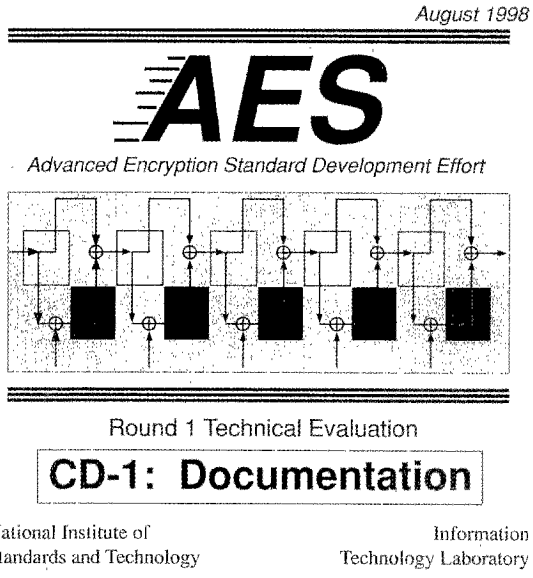

図-4　AES会議で配布されたCD-ROM（ソースコードは含まない）

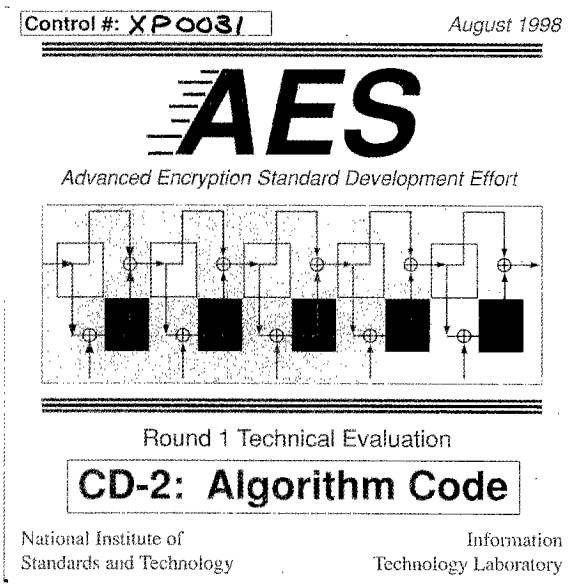

図-5　輸出許可を得て送られてきたCD-ROM（全AES候補のソースコードを含む）

ころがこの日の机の上には，なんと昨日議論になったMAGENTAの解読法に関する論文がすでに置いてあるではありませんか．「え？　もう論文を作って，しかも印刷までしてしまったの？」．今回の会議には自国からPCを持って来た人が，少なからずいましたし，私もはるばる日本からビデオカメラを持って来ている手前，人のことをとやかく言えたぎりではないのですが，プリンタまで持ち込んでいた人がいたとは....

▶AES候補の性能比較？

第1回AES会議に参加しますと，NISTから候補暗号のドキュメントをまとめた予稿集と，それらを電子的に収めたCD-ROMが手渡されました．表紙にはCD-ROM1と書いてあります（図-4）．さて，AES候補となっている各暗号の提案者らは，NISTの指定する性能評価を行い，かつそのデータを裏付けさせるため，暗号のC言語で書かれたソースコードが提出されています．AES選定の根拠となるデータ作成はできる限り公の場でも行えることをうたっていますので，NISTに提出されている各暗号のソースコードもいずれは公開されることは想像がついていました．ということは，早くもこのCD-ROMの中に各暗号のソースコードも含まれているのでは？　いいえ．含まれていませんでした．このCD-ROMに含まれていたのは各暗号の提案論文や性能評価表のみでした．

ご存知の方がいらっしゃるかもしれませんが，暗号というのは国際貿易上は武器の一種であると見なされています．ですから勝手に国外に持ち出すことができません．国外への持ち出しには，アメリカ商務省の輸出許可が必要となるのです．ちなみに，アメリカ国内のインターネットサイトで，暗号のソースコードがそのまま置かれている場所がありますが，そのソースコードを日本にいる人が勝手にダウンロードすることは，形式的には武器輸出に関する法律違反になるようです．

ということで，会議中はまだ輸出許可の下りていない段階でしたし，NISTという立場もあり，安易にソースコードの配布はできなかったのでしょう．会場で配布されたCD-ROMにはソースコードは含まれていませんでした．しかし輸出許可さえとれば，後日ソースコードが入ったCD-ROMを手に入れることができました．許可申請は実はそれほど難しくはありません．日本人でも手に入れた方がすでに何人かいらっしゃるようです．表紙にはAES CD-ROM2という名前と輸出管理番号が記されています（図-5）．

さて，ソースコードの入ったCD-ROMも手に入ったことですし，いよいよ各暗号の紹介と安全性や演算効率に関する解析結果に移りたいと思いますが，残りページ数が心許なくなってしまいました．これについては後日誰かにお任せということで．

▶今後の展望～本当の勝者は誰？

果たしてどの暗号がAESとして選ばれるのかはNISTのみぞ知ることになりますが，ではAESが1つに絞られた後は社会にどれくらいの影響を及ぼすかについては，諸説入り乱れていてはっきりしません．仕様が公開された共通鍵ブロック暗号がDESしかなかった時代とは異なり，現在では確認されているだけで70個もの共通鍵ブロック暗号があるのです．当然のことながら，異なるブロック暗号で暗号化された暗号文は，たとえ同じ鍵を用いたとしても正しく復号されることはありません．お互いの暗号文に互換性のない暗号がたくさんあっても仕方がなく，できれば統一した方がいいとする見方もあるでしょうし，いろいろな暗号を選択できる方が，ユーザにとって好まし

いとみる見方もあるでしょう．

前者の場合，過去にも何度かアメリカを中心とした標準化の動きがありました．DESを標準にしようとした計画，SKIPJACKを標準にしようとした計画，いずれも失敗に終わっています．AESが決まってもしばらくは様子見を決め込む予定の企業もあるようですし，当面はTriple-DESで十分であり，AESはその次と考える向きもあります．DESでさえ，アプリケーションによっては今後も問題なく使っていけるという意見さえ存在しています．このような状況ですので，たとえAESが決まったとしても，直ちに暗号が統一されてしまうことはない，とする見方が研究者の間では一般的です．ある電機メーカの暗号研究者の意見では，AESの候補はどれもソフトウェアによる演算効率にばかり目を向けていて，ハードウェアに向いたものは1つもない，そうです．私はハードウェアに関してはまったくのシロウトですので，真偽のほどは分かりませんが，もしそうなら，少なくとも暗号チップの分野にAESが参入するのは，少し遅れることになるのかもしれません．

一方後者の場合，数あるうちから自ら選択できる自由がある反面，どれを選ぶかについて考えた場合には，各共通鍵ブロック暗号の持つ安全性や効率性，適用するアプリケーションの性質等を吟味しなければ決定することはできません．また一口に暗号の安全性といっても，さまざまな尺度がありまして，暗号研究者でさえも簡単に理解できるものばかりとは限りません．また選択の参考となる文章を探してみたとしても，どのような暗号がどのような性質を満たしているのか，いないのか，暗号に対するアプリケーションごとに必要な要件とは何なのか，といった事項がまとめられた文書というものはまだ少なく，あったとしてもごく一部の応用しか適用できないか，非公開文章であることが多いようです．他とはっきりと異なった性質を持っていれば別ですが，結局のところ，研究者以外にはどれがどのように違っているのか判定するのが難しく，暗号の選択には専門家の意見を聞かざるを得ないのが現状ではないでしょうか．その場合は結局他人に任せることになり，自由に選べているのかどうか．

さて，AESの15候補中の本命といえば，RC6とMARSでしょう．政治的に考えてアメリカ製以外の暗号がAESに選ばれることは考えられない，と断言する研究者がいますが，そうでなくてもこの2つの暗号はよくできているというもっぱらの評判です．MARSを設計したIBMにはDESの設計にかかわったCoppersmithが名を連ねてまして，標準ブロック暗号のディフェンディングチャンピオンとしての面目がかかっています．そのプレッシャーたるや相当なものがあったのではないかと想像します．RC6を設計したRSA社は，公開鍵の分野で現在スタンダードとされているRSA方式を開発し，公開鍵暗号の分野では誰もが認めるトップランナーの1つです．この勢いで，共通鍵暗号の分野でも標準を勝ち取ろうとねらっています．

さてさて，AESに選ばれることはアメリカだけでなく世界標準暗号としての栄冠を勝ち取ることを意味し，非常に名誉であることは確かです．しかしその反面AESに選ばれてしまったら最後，開発者が持つ権利であるはずのロイヤリティを放棄しなくてはなりません．これは応募時にNISTに誓約書を提出しているため覆すことができません．開発者にとってこれは，大変な痛手であることに変わりはないはずです．AESに選ばれることは，果たしてそれに見合うだけの価値があるのかどうか．

一方で，AES最終選考の5候補に残っただけでも十分価値があるという意見もあります．暗号効率の面で他を圧倒してしまうほど高速な暗号は見当たりませんし，最終選考中に完全に解読されてしまったりすることも考えにくいです．そのため，最終選考では暗号同士の明らかな優劣というのはそれほどなく，選別者の主観によるところが大きいのではないかと考えられています．E2を開発したチームのリーダである太田さん（NTT）の話では，E2に関していえば5候補に残ることができればそれで十分でありAESに選ばれるとは思っていないそうです．結局のところAESの本当の勝者は，最終選考に残ったけれどもAESに選ばれなかったことで，安全性や効率性にお墨付きを得られた上にロイヤリティ収入を得ることができる，残りの4候補なのかもしれません．果たして勝利の女神は誰に微笑むのでしょう？

--- --- ---

カリフォルニアの朝，まだ肌寒い中散歩へ出かけて海を眺めたときにふと頭をよぎりました．

「そうか．海だったんだ．」

参考文献

1) 五十嵐幸雄: 次世代暗号AESの栄冠はだれにDESの後継争い始まる／第一回目の選定会議開催, 日経エレクトロニクス, pp.41-46 (1998.9.21).
2) 勝村幸博: 次世代暗号AES/DESに代わる米国標準暗号－15候補の中から1つが選ばれる, 日経インターネットテクノロジー, 10月号, pp.108-115 (1998).
3) 宇根正志, AES (Advanced Encryption Standard)について, 97-J-16 (Nov. 1997). http://www.imes.boj.or.jp/jdps/97-J-16.pdf
4) 宇根正志: 最近のAESを巡る動向について, 98-J-21 (Sep. 1998). http://www.imes.boj.or.jp/jdps98/98-J-21.pdf
5) 鈴木裕信: レポート AES/CRYPTO 98, Software Design, pp.70-73 (Nov. 1998).
6) 鈴木裕信: AES Conference/CRYPTO 98 訪問記, Bit, Vol.30, No.12, pp.34-39 (Dec. 1998).
7) 川村信一: AES参加報告, 信学技法, ISEC98-41, pp.39-43 (Nov. 1998).
8) 金子敏信 (座長): 次期暗号標準AESをどう考えるか, 1998年電子情報通信学会基礎・境界ソサイエティ大会講演論文集PA-3, pp. 252-260 (Oct. 1998).

（平成10年12月14日受付）