公募方式による米国の新暗号方式AESの選定

ネットワークでのデータの送受信、侵入に対するデータの保全など、コンピュータにおける暗号の重要性はこれまでになく高まっている。米国では、1970年代から標準であったDESに代わる新暗号AESの選定が進んでいる。この選定過程における暗号アルゴリズムの公募、およびオープンな評価のプロセスについて述べる。

DESの終焉

1977年に米国政府の標準として採用された暗号方式、DES（Data Encryption Standard）は、56ビットの鍵長を持つ秘密鍵暗号方式（鍵の総数は2^{56}＝７京以上）で、開発当初はすべての鍵を調べ尽くす手法でも解読には2000年（１回１マイクロ秒かかるとして）を要すると言われていた。しかし、コンピュータ技術が進歩し、またネットワークを介した複数コンピュータの同時並行処理が容易である今日、その暗号強度の信頼性は急速に低下しつつある。米国のRSAデータセキュリティ社が1999年に懸賞付きで課したDES解読問題が、高速専用解読機とインターネット上の多数のコンピュータを統合して鍵をすべて調べ尽くす手法で、１日に満たない時間で破られたことは、その事実を如実に示している。

この安全上の問題点をカバーすべく、DES処理を３回反復して強度を高めるTripleDESが1999年に規格化された。しかし、もともと単段で作動する設計のアルゴリズムを繰り返しているため処理効率は最良ではなかった。また、この方式に固有の近道攻撃法（鍵の全数探索によらない解読法）が存在することなどの弱点もわかっており、一時しのぎという性格が強い。このため、データの送受信・保存の要求に対応する安全性・速度・柔軟性に優れた新暗号方式が求められていた。

新暗号方式AES

このような経緯から、アメリカ商務省の機関である米国標準技術局（NIST：National Institute of Standards and Technology）は、DESの後継となる暗号アルゴリズムの公募を1997年９月に開始した。これがAES（Advanced Encryption Standard）である。

AESの基本要件は、「秘密鍵に基づく128ビット単位のブロック処理暗号であり、128、192、または256ビットの鍵を使用すること」である。さらに、処理速度、メモリー使用量、柔軟性なども選定基準として提示された。原理的に処理速度の遅い公開鍵暗号は除外されているが、鍵長は大幅に拡大された（DESが仮に１秒で破れてもAES解読には149兆年かかる）。

これらの要求性能は、高速処理と実装時の柔軟性を満足させた上で、鍵長の容易な拡張を意図したものである。今日のコンピュータ上で必要とされる暗号処理の要望に叶うものと言える。

公募プロセスの特徴

軍用・外交用の暗号と異なり、DESやAESのアルゴリズムは完全に公開することが前提となっている。公開アルゴリズムは、実装コストや互換性の面で有利となるのはもちろんであるが、さらに、その内容が暗号研究者から吟味され尽くすことになり、強度上の不安が少なくなるという側面を持つ。

NISTでは、今回のAESの選定プロセスにおいて、公開による吟味という手法をできる限り推し進め、公募の各段階において広く外部から意見を募る方法を採っている。

1997年１月に選定の計画を発表した後、募集に先立って、プロジェクトの進め方や基準についての反応を３ヶ月にわたって募集し、さらにワークショップを開いて要求性能、選定プロセスの基準を検討した。これを反映した最終の募集要項が９月に発表され、公募が開始された。

1998年６月に応募を締め切った後、７月までに書類選考により21候補中15候補が残された。15候補の開発者は翌月に第１回のカンファレンスに招かれ、それぞれ方式の発表を行っている。会議の主目的は各候補の説明であるが、世界でもトップクラスの暗号研究者が参加しており、各方式が厳しく検討された。方式発表のプレゼンテーションが終わった途端に出席者から解読法が示され、その場で事実上選外となった候補も出ている。

さらに２回の公開カンファレンスが開かれ、その間には候補方式の設計者や会議参加者のみならず、外部からも広くコメントが寄せられた。これらの追加情報は随時NISTのホームページで公表され、自由な閲覧に供されている。内容は、設計者が自候補を擁護するもの、外部の解析者が示した弱点、さらにそれらへの反論、実装方法の考察などである。

これらの情報や強度・処理速度などの各種解析の結果を踏まえ、NISTでは候補を段階的に絞り込んだ結果、2000年10月にベルギーの開発者による「Rijndael」（「レインダール」「レインドール」または「ラインダール」）が採用されることが発表された。発表後のまとめとして連邦標準の草案が2001年２月に提示され、それに対する最後のコメント受付が５月末まで実施されている。連邦標準としての最終公表は今夏を予定している。

日本での暗号アルゴリズム公募

日本の暗号研究・開発レベルは、国際的に見ても低くないが、公募された方式が標準に制定されたことはない。しかし、経済産業省の委託で情報処理振興技術協会が2000年から実施している電子政府向け暗号技術の評価において、方式を公募し、評価（攻撃）結果も公開で募るという手法が採られた。米国の例で有効性が実証された公募・公開のプロセスを徹底し、よりセキュリティの高い情報の送受信・保護が実現されることが望まれる。

（NRIアメリカ　鶴田正剛）