主役登場

国産初のデファクト暗号という大輪の花を咲かせよう

神田　雅透

NTT情報流通プラットフォーム研究所
主任研究員

セキュリティプロトコルを専門にしていた私が「FEAL（Fast data Encipherment ALgorithm）の後継暗号を設計しないか」というプロジェクトリーダのたった一言に乗って共通鍵暗号の研究を始めたのは1995年のことです．当時，商用的にはFEALがNTTの主力暗号として現役だったとはいえ，共通鍵暗号に対する解読技術が世界的に急進展していた時期であり，その矢面に立っていたのが米国政府標準暗号（当時）であるDES（Data Encryption Standard）とFEALでした．とりわけFEAL-8については，開発当初からくすぶり続けていた脆弱性の指摘がますます大きくなってきており，早晩新しい暗号が必要になるに違いないと予測されたため，まずは独自に最新の暗号設計技術を蓄積するという名目で横浜国立大学との共同研究を始めました．

転機が訪れたのは，1997年に米国商務省国立標準技術研究所がDESの後継暗号AES（Advanced Encryption Standard）を公募で選ぶプロジェクトを始めたときです．それまでの「暗号は武器の一種であり，国際標準暗号は決めない」時代から「情報化社会を支える基盤技術として安全な暗号を国際標準暗号にする」時代へと移行していく契機となりました．

もともと暗号は各種サービスを安全に提供するための道具という縁の下の力持ちというべき基盤的技術ゆえに，どんな暗号を使っていようとも一般にはサービスの外見上は何も変わりません．その結果，「技術的に優れているかどうか」ではなく，「知っているかどうか」あるいは「すぐに使えるかどうか」が暗号の大きな選択基準となっている場合が少なくありません．いわば，暗号の「ブランド力」が使われるかどうかの分かれ目になります．その点からみると，AESが国際標準暗号となればそのブランド力はとてつもなく大きくなり，単なる一企業の自社暗号では太刀打ちできないことは明らかです．

そうした状況の中で，NTTが開発した暗号を広く普及させるとすれば，従来のように国際学会などで発表するだけでなく，実際にいろいろな国際標準規格に採用され，AESと肩を並べる暗号であると世界に認められる必要があります．そこで，技術的にはNTTが持つソフトウェアでの暗号設計ノウハウと三菱電機が持つハードウェアでの暗号設計ノウハウを結集してAESと同等以上のものを開発し，国際標準暗号にすることを大目標として，三菱電機と共同で開発した暗号が「Camellia（カメリア）」です．そのことは名前にも現れており，日本原産の花「椿」が世界中に広まって「Camellia」になったのと同じように，初めから国産暗号が世界中に広まることを期待して名づけました．

実際に，今までの標準化活動を通じて，CamelliaはAES同等の性能を有する国際的に唯一の暗号との地位を獲得し，とりわけISO/IEC（International Organization for Standardization/International Electrotechnical Commission）国際標準暗号や国産暗号初のインターネット標準暗号などに選定されるなど，「Camelliaブランド」という，国産暗号としては初めてデファクト暗号になりうる種をつくり出すことに成功しました．

ただ，今はあくまで種の状態であり，これが花開くかどうかは，これからどれだけ利用されるかにかかっています．とりわけ，今後数年間で日本市場において広く使われるようになるかどうかが極めて重要な分かれ道となるはずなので，セキュリティプロデューサ・研究所一体となって普及活動を強力に進めていき，数年後にはCamelliaブランドの大輪の花を咲かせたいと思います．