2012 年 10 月 1 日
株式会社日立製作所

日立の省電力暗号技術「Enocoro」が国際標準規格へ採択

株式会社日立製作所(執行役社長:中西 宏明/以下、日立)が 2007 年に開発した省電力ストリーム暗号*1「Enocoro(エノコロ)」が、このたび ISO/IEC での最終承認を経て、国際標準規格 ISO/IEC 29192*2 の一つに採択されました。

「Enocoro」は、データ暗号のデファクト・スタンダードである AES*3 と比べて、1/10 程度の消費電力で暗号化処理を実現します。これにより、重要インフラ*4 を支える小型制御機器やセンサに対応する基本的なセキュリティ機能を、低コストで提供することができます。本暗号は、独立行政法人情報通信研究機構(理事長:宮原 秀夫/以下、NICT)の委託研究「大容量データの安全な流通・保存技術に関する研究開発」(2005~2007 年度)の開発成果を発展させたものです。

近年、パソコンや携帯電話だけでなく、家電、自動車など多様な機器がインターネットへ接続され、センサや RFID*5 といった無線通信機能を搭載した小型機器を介して、様々な情報がインターネット上でやり取りされています。一方、コンピュータウイルスなどに代表されるインターネット上の情報漏えいリスクは益々増大していることから、CPU やメモリなどの情報処理リソースが限られた小型機器においても安全性の向上が必要であり、機器間の認証や通信データの暗号化と、低コストの実装を両立できる省電力型の暗号技術が求められています。そこで国際標準化機構 ISO/IEC は、小型機器向け暗号の国際規格として ISO/IEC 29192 の策定を進め、このたび、ストリーム暗号に関するパート ISO/IEC 29192-3 を発行、ストリーム暗号「Enocoro」が国際標準規格として採択されました。

日立は、1989 年に MULTI-2 を開発して以来、継続して暗号技術の研究と標準化を進めてきました。近年では、2005 年にストリーム暗号 MULTI-S01*6 と MUGI*7 が、2006 年には、公開鍵暗号 HIME(R)*8 が国際標準規格に採択されています。このたび、「Enocoro」が採択されたことにより、日立が開発した 4 つの暗号アルゴリズムが標準化されたことになります。日立では「Enocoro」をはじめとする暗号技術を用いて、安全なネットワーク社会を実現する技術の研究に継続して取り組み、ネットワーク化が進む重要インフラや産業システムのセキュリティ向上に努めていきます。

*1 ストリーム暗号:秘密鍵から生成したランダムなビット列(鍵ストリーム)を使ってデータを 1 ビットずつ暗号化する方式。

*2 ISO/IEC 29192 (Lightweight cryptography):リソースが限られた計算機環境に適した暗号に関する規格。規格書は、パート 1:「総論」、パート 2:「ブロック暗号」、パート 3:「ストリーム暗号」、パート 4:「公開鍵暗号技術を使うメカニズム」の 4 部からなる。2012 年 1 月 10 日にパート 2、同 5 月 29 日にパート 1 が発行された。

*3 AES (Advanced Encryption Standard):2001 年に米国が規格化した共通鍵暗号の一方式であり、事実上の世界標準暗号。米国の NIST (National Institute of Standards and Technology:国立標準技術研究所)の主催した 3 ヵ年に渡る公開評価を経て選定された。

*4 「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」(2009 年 2 月 3 日内閣官房情報セキュリティセンターの情報セキュリティ政策会議)において、「重要インフラ」とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を

及ぼすおそれが生じるものと定義されている。同計画では、情報通信、金融、鉄道、航空、電気、ガス、水道、物流、医療、自治体サービスの10分野が防護すべき対象として掲げられている。

*5 RFID (Radio Frequency IDentification):無線通信可能なIDタグ。

*6 MULTI-S01 (MULTImedia encryption algorithm, Stream cipher No.01):日立が2000年に開発したストリーム暗号の運用モード。従来のストリーム暗号はデータ秘匿機能のみであったが、MULTI-S01ではデータ改ざん検知機能も実現した。2005年7月にISO/IEC標準として採択されている。

*7 MUGI (MUlti GIga cipher):日立が2001年に開発したストリーム暗号。2003年3月に電子政府推奨暗号リストに掲載され、2005年7月にISO/IEC標準として採択されている。

*8 HIME(R) (High Performance Modular-squaring-based public-key Encryption):暗号化に必要な鍵(暗号化鍵)と暗号化されたデータの復元に使用する鍵(復号化鍵)が異なる公開鍵暗号方式の一方式。日立が2001年に開発し、2006年5月にISO/IEC標準として採択されている。

■「Enocoro」の詳細

「Enocoro」には、鍵長80ビット用のEnocoro-80と、鍵長128ビット用のEnocoro-128v2の2種類のアルゴリズムがあります。「Enocoro」は、ISO/IEC標準であり、高速性に優れたストリーム暗号「MUGI」をベースに、内部状態を保持するレジスタの数を大幅に削減することで、ハードウェア回路の小型化を実現しました。また、SPN*9 2層構成の攪拌関数を新たに採用することで、従来よりも強力にレジスタ上のデータの攪拌を可能にし、安全性向上と消費電力低減の両立を図っています。具体的には、鍵長128ビットのEnocoro-128v2は同等の安全性を持つAES-128の軽量実装に比べると2～10倍の処理速度を達成しており、より少ない計算処理でデータを暗号化することができます。FPGA (Field Programmable Gate Array)を使って1ビットのデータを暗号化する際に消費する電力を実測した結果、AESでは1.16nWs(ナノワット秒)、Enocoro-128v2では0.103nWsとなり、Enocoro-128v2がAESと比べて1/10程度の消費電力で同じ量のデータを暗号化できることを確認しました*10。

*9 SPN (Substitution-Permutation Network):参照表を使った文字の置き換えと線形変換を交互に繰り返す攪拌方式で、AESでも採用されている。「MUGI」はFeistel構造と呼ばれる攪拌方式を採用し、Feistel構造1層で構成している。Feistel構造は、1977年に米国が規格化したDESなどの共通鍵暗号方式で広く採用されている、暗号の攪拌方式の一つ。

*10 具体的な数値は評価環境によって異なる。

■関連情報

・「Enocoro」に関するホームページ(日立製作所ホームページ内)
http://www.hitachi.co.jp/rd/yrl/crypto/enocoro/index.html

■商標注記

・Enocoro、MUGI、HIME(R)は日立の登録商標です。

■照会先

株式会社日立製作所 横浜研究所 企画室 [担当:吉田]
〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地
電話 045-860-3092(直通)

以 上