2009 年 8 月 7 日
株式会社日立製作所

次世代ハッシュ関数の世界的コンペで日立の「Luffa」が第一次選考を通過

2012年に決定される次世代ハッシュ関数標準の候補の一つとして日本から唯一選出

株式会社日立製作所(執行役会長兼執行役社長:川村 隆／以下、日立)が、ベルギーのルーヴァン・カトリック大学と共同で開発したハッシュ関数*1「Luffa(ルッファ)」*2 が、このたび米国商務省国立標準技術研究所(以下、NIST)*3 主催の、世界の暗号技術標準を事実上決定する次世代ハッシュ関数コンペティション(以下、SHA-3 コンペ)*4 において、次世代ハッシュ関数の候補の一つに選出されました。今回の選考は、51 方式の中から 14 方式*5 を選出したもので、日本からの応募としては唯一「Luffa」がこの第一次選考を通過しました。今後、選出された 14 方式で第二次選考が行われ、最終的には 2012 年に次世代のハッシュ関数が決定される予定です。

情報化社会においては、さまざまな情報を保護するために、暗号技術が重要な役割を果たしています。中でもハッシュ関数は、データの改ざんや破損の検出に活用される暗号技術の土台となるもので、電子取引やデバイス認証などに広く利用されています。ハッシュ関数は、暗号化の対象となるデジタル情報を圧縮してデータの指紋とも呼ばれる特徴値を抽出する関数です。この特徴値は、異なるデータから抽出されたものが一致する可能性が極めて低いこと、またデジタル情報がわずかでも異なると特徴値が大きく変わるという性質を持つため、ハッシュ関数は、悪意ある第三者によるデータの改ざんや、意図せざるデータの破損を検出するために用いられています。

現在、最も普及が進んでいるハッシュ関数は、160 ビット長の特徴値を出力する SHA-1*6 と呼ばれる関数ですが、2005 年に、最新の暗号解析技術によって脆弱性が発見され、期待される安全性を確保できないことが明らかになりました。NIST は、256 ビット長の特徴値を出力する SHA-2*7 への移行を推奨していますが、これと並行して、2007 年 11 月に、新たな標準ハッシュ関数を選定する SHA-3 コンペを開始しました。2008 年 12 月には、世界中から応募された 64 方式のアルゴリズムの中から 51 方式を、次世代ハッシュ関数の候補として認定し、SHA-3 コンペの第一次選考を開始しました。

8 ヶ月間に渡って行われた第一次選考は、世界中の暗号研究者が 51 方式のアルゴリズムの安全性を評価する一方、開発者はアルゴリズムの改定案を提出するなど、意見交換を行いながら候補の絞込みが行われました。この結果、安全性に対する新しい評価手法が開発されるなど、技術的にも大きな進歩が見られました。今回 NIST は、世界中から寄せられた多くの評価結果を踏まえ、51 方式の中から安全性、高速性の面で優れた 14 方式を次世代ハッシュ関数標準の候補として選定し、2009 年 7 月 24 日に発表しました。そして 14 方式の中に、日本からの応募では唯一、日立がルーヴァン・カトリック大学と共同で開発したハッシュ関数「Luffa」が選ばれました。

第二次選考に進む 14 方式は、いずれも安全性、実装性などにおいて優れた特性を有しているハッシュ関数です。今後は、2010 年夏頃に最終候補となる 5 方式が選出され、さらに 2 年かけて NIST により次世代ハッシュ関数 SHA-3 が決定される予定です。

今後、日立では、SHA-3 コンペを通じてハッシュ関数の安全性や実装性などの研究を深め、社会イノベーション事業における情報セキュリティの基盤となる、暗号分野の発展に貢献していきます。

■日立が開発したハッシュ関数「Luffa」について

従来のハッシュ関数は、一定サイズのデータブロックごとにデータ攪拌(かくはん)処理と圧縮処理を行う設計思想のため、データブロックごとの処理負荷が大きくなっていました。これに対して「Luffa」は、ブロックごとに攪拌(かくはん)処理のみを行い、最終的に圧縮処理を行うことで、効率的なデータ圧縮を行う新しい「スポンジ型」構成法を採用しました。「スポンジ型」構成法は、従来のハッシュ関数に比べ高い安全性を実現できることが知られています。さらに「Luffa」では、高速処理性と軽量性を兼ね備えた基本処理部を適切に配置することで、軽量性を損なうことなく安全性と高速処理性を両立させるとともに、スケーラブルな設計を可能とし、SHA-3 で求められる 224 ビットと 256 ビット、384 ビット、512 ビットの出力サイズに対応できるようにしました。

*1 ハッシュ関数：任意のメッセージ入力に対して固定長の出力値を生成する関数。出力値が同じになる入力の発見が困難であることなどの安全性基準を満たすことが要求される。
*2 Luffa(ルッファ)は、日本において日立製作所より商標登録出願中です。
*3 NIST：National Institute of Standards and Technology の略。製品市場を事実上牽引する米国の商務省下の NIST で政府向けの標準暗号を制定する。
*4 SHA-3 コンペ：NIST が主催する次世代のハッシュ関数を選定するプロジェクトで、正式には「Cryptographic Hash Algorithm Competition」と称する。選ばれたハッシュ関数は 2012 年に SHA-3 として米国連邦標準規格 FIPS(Federal Information Processing Standard)になり、世界中の情報機器で標準的に利用されていくことになると考えられる。
SHA-3 は、Secure Hash Algorithm-3 の略。
*5 候補 14 方式：http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/index.html
*6 SHA-1：Secure Hash Algorithm-1 の略。FIPS180-2 に掲載された NIST が開発した出力サイズ 160 ビットのハッシュ関数。米国のみならず、インターネット、ISO 等で標準化されている。
*7 SHA-2：Secure Hash Algorithm-2 の略。FIPS180-2 に掲載されたハッシュ関数。224 ビットと 256 ビット、384 ビット、512 ビットの出力サイズに対応している。SHA-1 と同じ設計思想に基づいている。

■お問い合わせ先

株式会社日立製作所 システム開発研究所 企画室 [担当：塚越]
〒215-0013 神奈川県川崎市麻生区王禅寺 1099 番地
TEL：044-959-0325(直通)

以上

このニュースリリース記載の情報(製品価格、製品仕様、サービスの内容、発売日、お問い合わせ先、URL 等)は、発表日現在の情報です。予告なしに変更され、検索日と情報が異なる可能性もありますので、あらかじめご了承ください。
