2009 年 1 月 15 日
株式会社日立製作所
国立大学法人神戸大学
国立大学法人福井大学
独立行政法人情報通信研究機構

より安全な情報通信のための次世代暗号技術の開発に成功

～米国商務省が実施する次世代暗号のコンペに応募し、候補として正式に認定～

株式会社日立製作所(執行役社長:古川　一夫／以下、日立)と国立大学法人神戸大学(学長:野上　智行／以下、神戸大)、国立大学法人福井大学(学長:福田　優／以下、福井大)は、より安全な次世代ハッシュ関数[*1]「Lesamnta(レザンタ)」[*2]を共同で開発しました。さらに、この「Lesamnta」は、世界の暗号技術標準を事実上決定する米国商務省国立標準技術研究所(以下、NIST)[*3]の次世代暗号コンペティション(以下、SHA-3 コンペ)[*4]において、次世代ハッシュ関数の候補として正式に認定されました。

なお、本成果は、独立行政法人情報通信研究機構(理事長:宮原　秀夫／以下、NICT)からの委託研究「次世代ハッシュ関数の研究開発(2007～2008 年度)」によるものです。

■背景

ネットワークを介して様々なサービスが実現される情報通信社会では、通信機器や IC カードの不正利用を防止する技術や、文書データの改ざんを検知する技術が重要となっています。それらの技術にはハッシュ関数が利用されていますが、現在最も広く用いられているハッシュ関数 SHA-1[*5]は、暗号解析技術の進展にともない、その安全性が低下していることが報告されています。そこで、NIST は、新しいハッシュ関数を選定するために、次世代ハッシュ関数選定のためのプロセス SHA-3 コンペを 2007 年 11 月から開始し、候補となるハッシュ関数を公募しました。

このような背景の下、日立と神戸大、福井大は、安心・安全な社会の実現に向けて、次世代ハッシュ関数「Lesamnta」を共同で開発しました。

■成果

今回「Lesamnta」を SHA-3 コンペに応募したところ、NIST による書類審査の結果、応募された 64 種類のアルゴリズムの中から「Lesamnta」を含む 51 種類のアルゴリズムが、2008 年 12 月、次世代ハッシュ関数の候補アルゴリズムとして正式に認定されました。

「Lesamnta」は、実装の容易さや処理速度といった要件を配慮しつつ、安全性を最も重視したアルゴリズムです。「Lesamnta」では、日立が RFID[*6]向けに開発したハッシュ関数 MAME[*7]の設計指針を継承しながら、従来のブロック暗号研究で培った安全性評価等の技術を活用し、高いデータ攪拌性[*8]を有する複数の基本関数を、安全性と効率性とを考慮して最適配置することで各種暗号解読への耐性を実現しています。さらに、様々な製品やシステムで容易に実装できるようバイト単位の処理を基本としています。

その結果、「Lesamnta」は、NIST での評価基準の一つでもあるハッシュ関数 SHA-2[*9]と比較して、十分に高い安全性を有するとともに、各種プラットフォームで容易に実装することが可能です。

■今後の展望

今後は、NIST の主催する公開研究会等において安全性や性能等の面から候補の比較が行われ、2012 年に NIST により次世代ハッシュ関数 SHA-3 が選定される予定です。

なお「Lesamnta」の詳細を、2009 年 1 月 20 日(火)から 23 日(金)まで滋賀県の大津市で開催される「2009 年 暗号と情報セキュリティシンポジウム」で 21 日(水)に発表する予定です。

■用語解説

*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等の安全性基準を満たすことが要求される。

*2 Lesamnta(レザンタ):日本における日立の登録商標です。

*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:Secure Hash Algorithm-3 の略。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。

*5 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。

*6 RFID:Radio Frequency Identification の略。ID 情報を内蔵した小型の無線タグと、それを用いた ID 化技術の総称である。

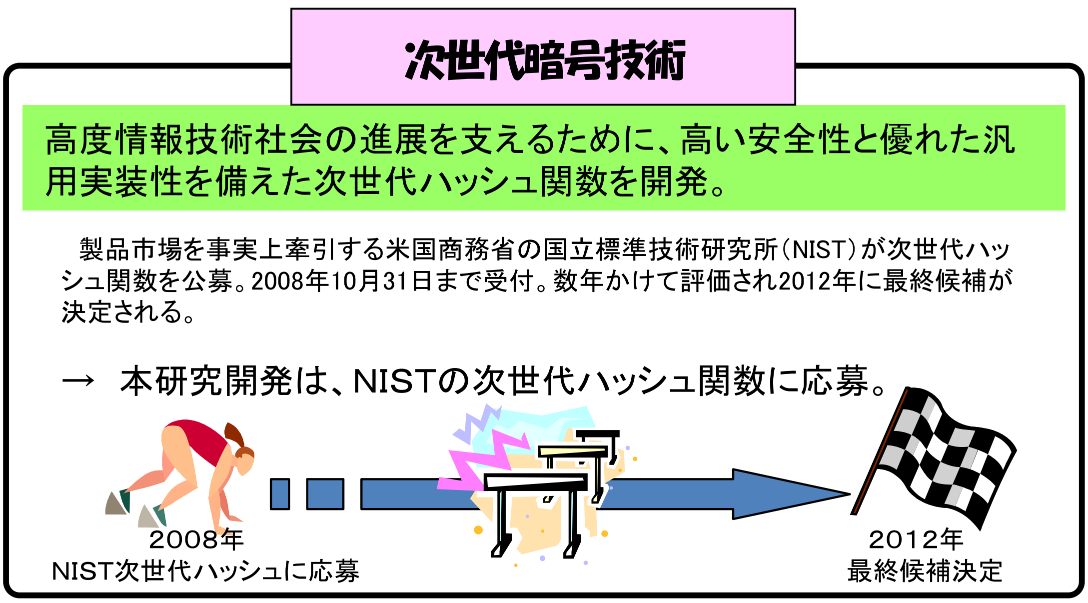
*7 MAME:日立が 2007 年に発表した RFID 向けハッシュ関数であり、特にハードウェアでの実装規模が小さい。

*8 データ攪拌性:関数に入力されたデータをランダムなデータへと変換する性質。安全性の高いハッシュ関数となるためには、この性質が強いことが重要である。

*9 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 25 6 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。

■補足資料

(1)SHA-3 コンペの概要



SHA-3 コンペとは、高い安全性と優れた汎用実装性を備える次世代ハッシュ関数の標準を規定する、NIST 主催の国際プロジェクトです。暗号技術の選定コンペティションとしては、1997 年に行われたブロック暗号の世界標準である AES(Advanced Encryption Standard)の選定に続くものです。SHA-3 コンペで選定されるハッシュ関数は米国政府標準にとどまらず、AES と同様に世界中の情報機器で標準的に利用されていく予定です。

SHA-3 コンペに公募し、正式な候補として認定されるためには、要求される評価水準を十分にクリアする必要があり、今回、正式な候補が公表されました。日立はこれまで、安心・安全な社会の実現に向けて暗号技術の開発を進めてきましたが、神戸大、福井大との産学連携によって今回の候補認定に至ったことは、その一つの成果となるものです。今後、学会などのオープンな場での議論及び評価が重ねられ、数段階の選定ステップを経て、今回認定された「Lesamnta」を含む 51 種類の候補の中から、2012 年に SHA-3 の標準ハッシュ関数が決定される予定です。

（2）ハッシュ関数 Lesamnta の概要

「Lesamnta」は、SHA-2 より高い安全性を持つハッシュ関数です。SHA-2 とは異なり、理想的なハッシュ関数との区別が困難であることが明示されており、また、SHA-2 の主要な課題とされている SHA-1 の既存の解読法に対する安全性を有していることから、より安心・安全に利用されることが期待できます。また、「Lesamnta」は、優れた汎用実装性を持っています。シンプルかつコンパクトな設計であるため、8 ビット CPU 上では実装規模を小さく実装でき、また、AES と共通する部品を取り入れることにより、AES の組み込まれた次世代の 32 ビット・64 ビット CPU 上では極めて高速に処理することが可能になります。この汎用実装性により、様々な情報機器において幅広い目的で、かつ便利に利用されることが期待できます。

■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　雅人］
Tel:044-959-0325

国立大学法人神戸大学　工学研究科電気電子工学専攻　情報通信研究室［担当:桑門　秀典］
Tel:078-803-6091

国立大学法人福井大学　工学研究科電気・電子工学専攻　情報通信システム研究室［担当:廣瀬　勝一］
Tel:0776-27-9738

以上