# Ⅴ-2. 次世代ハッシュ関数の動向に関する調査研究

Study on trend of the next generation hush function.

| キーワード | 暗号、次世代標準ハッシュ関数、ハッシュ関数攻撃 |
|---|---|
| Key Word | crypto, advanced hash standard, attacks on cryptographic hashes |

## 1. 調査の目的

インターネット等を介した電子商取引システムや電子政府システム等、様々な情報システムで広く利用されているが、ハッシュ関数はそうしたシステムの安全性確保のための中核技術として不可欠な暗号技術である。しかし、近年、従来利用されてきたハッシュ関数に対して新たな攻撃方法が発見されたことにより、安心して利用できる安全な次世代のハッシュ関数を開発・標準化の動きが活発化している。

本調査研究においては、将来の安心・安全な情報システムに不可欠な、次世代ハッシュ関数の技術動向に関して国内外における調査を実施した。

## 2. 調査研究成果概要

### (1) 調査の内容

#### ①次世代ハッシュ関数に関する取組動向についての調査

【国内における取組動向】

ハッシュ関数のデファクトスタンダードである SHA-1 脆弱性の発表を受け、我が国においても様々な対応が実施されている。主として注目されるのは、独立行政法人による公的な研究助成や関連イベントの開催などによるハッシュ関数の危殆化への技術的な取組や関連分野への適切な情報交流機会の提供といった支援的な取り組みである。

これらの取り組みは、ハッシュ関数におけるネックとなっている安全性評価手法からアルゴリズム開発レベル、実環境における対応策まで広範にわたって研究開発が実施されているが、成果が出るのはこれからといった状況である。

【国外における取組動向】

暗号技術の実質的なイニシアティブを握る米国商務省国立標準技術研究所 (NIST) や IETF 等の国際標準化機関の動向は、概ね以下の通りである。

- SHA-1 の脆弱性について明確になり次第、適切なハッシュへの移行 (当面の移行すべきハッシュ関数は SHA-2)
- 移行に伴うプロトコル等の仕様修正などの検討を適宜推進
- SHA-2 のさらに次に位置づけられる SHA-3 を選定する公募コンテストの実施(NIST)

#### ②次世代ハッシュ関数に関する最新の設計技術動向についての調査

次世代ハッシュ関数に関しての基本見解としては、「SHA-1 は、厳密な数学的には安全性に問題があるが、現実の利用の中で直ちに使えなくなる程ではない」というスタンスが一般的である。そして、現時点での SHA-1 の現実的な代替アルゴリズムは SHA-2 ファミリであるが、研究が十分でない可能性がある。

また、過去 3 年間の技術動向を調査した結果、2006 年が次世代ハッシュ関数に関する研究発表が盛んであった (2005 年に SHA-1 の弱点が指摘された翌年)。そして、具体的な次世代ハッシュ関数の提案については、発表後 2 年以内に弱点が指摘されており、現時点で明確に有力候補と判断できる提案はないことが明らかになった。

そして、今後については、NIST の次世代ハッシュ関数の公募 ("SHA-3") が、ロードマップの一つの

目安になるが、具体的なアルゴリズムが出てくるまではどう対応するかの明確な判断はできない状況にある。

### ③次世代ハッシュ関数の利用が想定されるシステムについての調査

【次世代ハッシュ関数の利用が想定されるシステム用途】

次世代ハッシュ関数の利用が想定されるシステム用途であるが、以下の理由から用途そのものは現状のハッシュ関数が利用されている状況から、大きな変化はないものと推測される。

- システム用途となるセキュリティ・アプリケーションの構成がインターネットを介して様々な構成要素間の相互運用性を維持したまま発展する必要があること
- ドラスティックな用途や仕様変更は、相互運用性確保にそぐわないこと（例：RFC で暗号アルゴリズムを分離するようになったのは、比較的最近）

次世代ハッシュ関数へのニーズとしては、どの程度の期間の安全性を保持するかという時間的な観点でシステムニーズを整理することが有効な方法の一つである。

将来的なハッシュ関数の実利用を念頭におき、SHA1 や SHA-2 ファミリーなどの従来型の衝突困難性ハッシュ関数（CRHF）、近年実用レベルへの発展が期待されている汎用一方向性ハッシュ関数（UOWHF）による用途別の特性をそれぞれ以下に示す。

UOWHF：処理速度や利用環境条件よりも本質的な安全性証明を求めるような用途

CRHF：本質的な安全性よりも処理速度や利用環境条件を求めるような用途

【次世代ハッシュ関数の要件】

次世代ハッシュ関数については、安全性強度、安全性評価、ソフトウェア・ハードウェア実装性能などの点において、以下の方向性をもった要件が適切であると考えられる。

| | 要件 1　CRHF 型<br>（処理性能や実装環境を優先） | 要件 2　UOWHF 型<br>（証明可能安全性の付与を優先） |
|---|---|---|
| 安全性強度 | 出力長が 256 ビット相当 | 出力長が 256 ビット相当 |
| 安全性評価 | ハッシュ関数が達成すべき安全性要件の明確化と定量的な安全性評価を実施可能な方式であること | ハッシュ関数が達成すべき安全性要件の明確化と理論的な証明可能安全性を有すること。 |
| 実装性能 | SHA-2 ファミリーと比較した際に、以下の点を満たすこと。<br>➢ 多様な CPU 環境下で処理速度、もしくはメモリ使用量の面で優位性を示す点があり、高いレベルでバランスの取れた性能を有する<br>➢ 速度最適実装と面積最適実装においても、処理速度、もしくは、回路規模の面で優位性を有する | 利用される実システム上の環境において、第三者が納得できる利用上問題のない適切な実装性能を保有すること。 |