2012 年 2 月 14 日

KDDI 株式会社
KDDI 研究所

高速ストリーム暗号アルゴリズム「KCipher-2（ケーサイファー　ツー）」が ISO 国際標準規格に採用

KDDI 株式会社(本社: 東京都千代田区、代表取締役社長: 田中 孝司、 以下 KDDI)、株式会社 KDDI 研究所（本社：埼玉県ふじみ野市、代表取締役所長：中島康之、以下 KDDI 研）は、KDDI 研が開発した高速ストリーム暗号(注 1)アルゴリズム「KCipher-2」の標準化を進めてきました。このたび、ストリーム暗号の標準規格 ISO(注 2)18033-4 の最終承認を経て、国際標準規格として採用されました。

「KCipher-2」は、KDDI 研と九州大学が共同で設計し、KDDI 研によって商用化された高速ストリーム暗号アルゴリズムです。KCpher-2 は、携帯電話機等の小型で処理能力が限られた機器や大容量データの高速処理向けに開発された、暗号化と復号に同じ鍵を使用する共通鍵暗号方式です。

共通鍵暗号方式で米国標準の AES(注 3)と比べて、最大 10 倍の速さで暗号化と復元を実現します。

また、複数の大学や専門機関による安全性評価においても、脆弱性が発見されていないことが報告されています。

KDDI と KDDI 研は今後、「KCipher-2」の高速・軽量という特徴を生かし、マルチメディアコンテンツ配信やデータセンターなど大容量のデータを扱う分野や、携帯電話や IC カードなどリソースが限られた中で高速な処理を求められる分野に積極的に展開していきます。

以　上

（注 1）入力データ（平文もしくは暗号文）をビット単位ごとに暗号化、復号を行う方式。軽量な処理に加え、暗号化と復号化の処理が同一となるため、実装コストが小さい。携帯電話の GSM 通信の暗号化や、SSL 暗号通信に用いられるなど、古くから実用的なアルゴリズムとして使用されている。

（注 2）International Organization for Standardization（国際標準化機構）の略。

（注 3）Advanced Encryption Standard の略。暗号モジュールに関するセキュリティ要件の仕様を規定する米国連邦標準規格 FIPS(Federal Information Processing Standardization)によって規定されているブロック暗号。

本件に関するお問合せ先
株式会社KDDI研究所 営業企画グループ
TEL:049-278-7545　E-mail : inquiry@kddilabs.jp