iotaCRYPT/AES 製品仕様

プログラム特徴

- 独自の実装方法（特許出願中：特願 2001-394109）を用いて AES の暗号化と復号化を高速かつコンパクトに実現（名古屋大学大学院情報科学研究科　神保雅一教授と共同研究）

  - 独自変換テーブルの開発によって、Triple DES に比べ 16 倍以上の高速化を実現しました（〔性能計測例〕の項参照）。
  - 独自変換テーブルは、ROM または RAM 領域において配置指定の選択ができます※1。これにより、各領域制限に応じ省容量化が可能です。

※1：Java 版 AES 暗号プログラムでは、独自変換テーブルは RAM 領域配置のみとなります。

実装仕様

- FIPS PUB197※2 に準拠
- ブロックサイズ 128bit 固定長
- 鍵長 128bit、192bit、256bit をサポート
- 動作モードは ECB※3, CBC※4 をサポート
- C 言語および Java にて実装

※2：FIPS PUB197
Federal Information Processing Standards Publication 197
November 26, 2001　Announcing the ADVANCED ENCRYPTION STANDARD (AES)
http://cs-www.ncsl.nist.gov/publications/fips/fips197/fips-197.pdf 参照

※3：ECB(Electronic Code Book)モード
平文（暗号化される前の文）のデータをブロックに分割して、各ブロックにてそれぞれ暗号化を行い、再び結合させることにより全体の暗号化を実現する方式

※4：CBC(Cipher Block Chaining)モード (C 言語版のみの実装となります)
すでに暗号化したブロックと、次の平文のブロックとの XOR（排他的論理和）をとり、暗号化する方式

製品パッケージに含まれるもの

- C 言語ソースコード製品(***iotaCRYPT/AES C,　C for T-Engine***)
  - 使用許諾契約書（当社管理上、事前にご契約いただいた上で、製品を出荷させていただきます）
  - C 言語ソースコード一式
  - 取り扱い説明書（コンパイル･リンク方法、API 他）

- Java ソースコード製品(***iotaCRYPT/AES Java***)
  - 使用許諾契約書（当社管理上、事前にご契約いただいた上で、製品を出荷させていただきます）
  - Java ソースコード一式
  - インタフェース仕様
  - サンプルプログラム※5
  - 簡易テストプログラム※6

※5：サンプルプログラム
・AES 暗号ライブラリを使用してファイルを暗号化<->復号化するプログラム。
・J2SE にて動作確認済みです。

※6：簡易テストプログラム
全ての鍵長（128bit，192bit，256bit）の暗号化<->復号化が正しく行われることを、ある固定の 1 データに対して実施し確認するプログラム。

DENSO CREATE

製品の種類

製品名	製品概要	動作確認環境	許諾ライセンス数
◆C 言語ソースコード製品◆			
iotaCRYPT/AES C	Cソースコード		50
iotaCRYPT/AES C for T-Engine	T-Engine 版 Cソースコード		50
◆Java ソースコード製品◆			
iotaCRYPT/AES Java	Java ソースコード		50
◆その他製品◆			
iotaCRYPT/AES ランタイムライセンス	商用利用のためのライセンス（ライブラリまたはソース製品をご購入の上、商用利用の際に必要となります）		100 or 無制限

※：ライブラリおよびソースコード製品を、お客様製品に組込んで販売されるなど、商用利用目的の場合は、別途 *iotaCRYPT/AES* ランタイムライセンスのご購入が必要です。

API 概要

- Primitive API（C 言語製品・Java 製品）

関数またはメソッド	概要
暗号化	ブロック単位(1 ブロック＝128bit)の平文を暗号化する
復号化	ブロック単位(1 ブロック＝128bit)の暗号文を復号化する
拡張キーの生成	3 種類の長さの暗号鍵(128bit、192bit、256bit)から、拡張キー※8 を生成する
拡張キーのクリア	生成した拡張キー※7 を格納している領域を解放する

※7：拡張キー
AES のアルゴリズムにおいて、必要となる鍵。

- Standard API （C 言語製品のみ。Java 製品に関してはお問い合わせください）

関数	概要
ECB モード暗号化	複数ブロック(16 バイト単位)の平文を ECB モードで一括暗号化する
ECB モード復号化	複数ブロック(16 バイト単位)の平文を ECB モードで一括復号化する
CBC モード暗号化	複数ブロック(16 バイト単位)の平文を CBC モードで一括暗号化する
CBC モード復号化	複数ブロック(16 バイト単位)の平文を CBC モードで一括復号化する
パディング付加/削除	指定のブロック長単位で、入力ブロック列にパディングを施す/削除する

動作検証

- FIPS※2 にて定義されている TESTVECTORS※8 のテストデータを使用した動作検証済み。
- 独自変換テーブルの検証のために、プログラム内の全ての条件分岐および全テーブルデータを使用したテストを実施。その結果、FIPS PUB197※2 にて参照されるサンプルプログラムと実行結果が等しいことを確認済み。

※8：FIPS PUB197※2　Appendix C － Example Vectors 参照

性能計測例

- 暗号化・復号化の速度
  - C 言語スタティックライブラリ
    - ✧ 測定環境：T-Engine (SH3, 内部クロック 96MHz)

		iotaCRYPT/AES (Mbyte/sec)		Triple DES (Mbyte/sec)	
		暗号化	復号化	暗号化	復号化
鍵長	128bit	7.90	8.05	0.475 (鍵長：56bit)	0.475 (鍵長：56bit)
	192bit	6.74	6.74		
	256bit	5.82	5.82		

※本測定環境では、RAM サイズ最小版・ROM サイズ最小版ともに、暗号化復号化の実行速度は同じです。

  - Java クラスライブラリ
    - ✧ 測定環境：DELL OptiPlex GX150
      (ペンティアムⅢ 内部クロック 1GHz, メモリ 256Mbyte), Windows2000

		iotaCRYPT/AES (Mbyte/sec)	
		暗号化	復号化
鍵長	128bit	9.7	9.6
	192bit	8.6	8.6
	256bit	7.9	7.9

メモリ計測例

	ROM サイズ(Kbyte)	RAM サイズ(Kbyte)
C 言語スタティックライブラリ（RAM サイズ最小化版）	27～29 程度	0.0
C 言語スタティックライブラリ（ROM サイズ最小化版）	13～20 程度	15 程度
Java クラスライブラリ	2.5(Jar ファイル)	12.5(概算)

※測定環境は、性能比較例と同一です。
※RAM サイズは、静的変数領域として使用するサイズを計測しています。RAM サイズには、拡張キー分の容量は含まれません。
※C 言語製品において、RAM 最小化版の ROM サイズおよび ROM 最小化版の RAM サイズには、独自変換テーブル分の容量が含まれます。
※Java ライブラリ製品の RAM サイズには、独自変換テーブル分の容量が含まれます。

参考情報：AES 暗号とは

- NIST（National Institute of Standards and Technology: アメリカ国務省･標準技術局）の次世代「共通鍵暗号」標準化プロジェクトで 2000/10 に、Rijndael のアルゴリズムが採択され、2001/12 に FIPS（Federal Information Processing Standard: 米国連邦情報処理標準） ※2 として発行
- 日本の総務省および経済産業省が、「電子政府推奨暗号リスト」に掲載
  http://www.soumu.go.jp/joho_tsusin/security/pdf/cryptrec_01.pdf
- 鍵の長さ 128bit、192bit、256bit の 3 通り（DES 暗号は実質 56bit）により、より強固な暗号鍵を生成できる
- ラウンド変換と呼ばれる処理を繰り返し実行することで、暗号処理としての安全性が保証される
  （理論上では、DES のクラック時間を 1 秒に例えると AES では 149 兆年かかる）
- 強度、速度の両面において、現時点で最高水準の暗号アルゴリズム
- 今後、従来の DES および Triple DES からの移行が見込まれる

■お問い合わせ

株式会社デンソークリエイト　E-mail： info@dcinc.co.jp　URL：http://www.dcinc.co.jp/

本社　新事業推進・イオタクリエイト
〒460-0003 **愛知県名古屋市中区錦** 2-15-20
TEL (052)229-1192　FAX (052)229-1171

東京フロント
〒150-0021 **東京都渋谷区道玄坂** 1-21-2 **新南平台東急ビル** 6F
TEL (03)3780-7081

　(04.6.1版)