２００３年7月7日
全3ページ

NEWS　RELEASE

株式会社デンソークリエイト
〒460-0003 名古屋市中区錦 2-15-20（三永伏見ビル）
TEL 052-229-1177 FAX 052-229-1171

◆ソフトウエア新製品発表◆

デンソークリエイトは、米政府標準の暗号技術を高速かつコンパクトに実現したソフトウエアを発売

株式会社デンソークリエイト（代表取締役社長:伊藤健三、本社愛知県名古屋市、以下デンソークリエイト）は、AES（Advanced Encryption Standard）暗号プログラム *iotaCRYPT/AES*（イオタクリプト・エー・イー・エス）を７月９日に発売します。

現在､コンピュータセキュリティへの関心が高まっています。デンソークリエイトは、開発者が利用しやすいように､C 言語版と java 言語版の暗号プログラムをライブラリおよびソースコードで提供します。本製品は､Windows だけではなく､組込みソフトウエア環境でも利用できるため､応用範囲が広がります。

◇

製品概要

米政府で次世代暗号標準として採択された安全性の高いＡＥＳ暗号アルゴリズムを基に、独自の実装方法を用いて高速化かつ省メモリ化を実現した暗号化プログラムです。

製品特長

- **安全なアルゴリズム**
  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採択され、2001 年 12 月に FIPS（Federal Information Processing Standard: 米国連邦情報処理標準）として発行されたアルゴリズムを採用しています。従来の DES（Data Encryption Standard）暗号に代わり、現時点で最高水準の強度を持つ暗号アルゴリズムです。
- **高速かつコンパクト**
  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省メモリに実現しました（慶応義塾大学理工学部数理科学科　神保雅一教授と共同研究）。
  - ROM サイズ： C スタティックライブラリ 3Kbyte～15Kbyte
    Java クラスライブラリ 2.5Kbyte
  - 速度性能：オリジナル AES プログラムの 30 倍以上の高速化を実現
    （下記「性能比較例」欄参照）

- **ソフトウエア実装による用途の拡大**
  ソフトウエアのみで実現しているため、特殊なハードウエアが不要です。汎用機器の利用により、システムのコスト低減が可能となります。
- **ライブラリまたはソースコードでの提供**
  ライブラリだけでなく、ソースコードでご提供することにより、とくに組込み用途に対して、柔軟に対応できるようにしています。たとえば、お客様側でのご事情により再コンパイルが必要となる場合、お客様ご自身での対応が可能になります。
- **各種組込み環境への柔軟な対応**
  ライブラリ製品には、お客様の環境をお聞きした上で、個別組込み対応版としてご提供します。自動車や携帯電話などの組込みソフト開発において、１０年以上の経験と実績を持つデンソークリエイトが対応します。また、本製品を適用したアプリケーション開発や組込み機器へのセキュリティ対策のご相談も承ります。
- **導入サポート**
  本製品をご使用いただくための導入セミナーとサポートサービスをご用意しています。出張サービスにより、製品ご使用のためのインタフェース仕様やサンプルプログラムの講習および製品移植のための技術的な相談にお応えします。
- **低価格で提供**
  ＡＥＳ暗号プログラムを単体で、低価格（￥10 万～）でご提供します。商用利用のためのランタイムライセンスも、お値打ちな設定（￥20 万～）となっています。

◇

性能比較例

＜暗号化・復号化の速度＞

オリジナル AES プログラムの **30 倍以上**の高速化を実現しています。

- 測定環境：T-Engine (SH3, 内部クロック 96MHz)
- 測定方法：1 ブロック(128bit)を 10,000 回暗号化および復号化実行した速度を計測

		iotaCRYPT/AES *(C スタティックライブラリ)* **(msec)**		**オリジナル AES プログラム※ (msec)**	
		暗号化	復号化	暗号化	復号化
	128bit	162	167	5,350	7,170
	192bit	190	196	6,460	8,700
	256bit	218	224	7,570	10,180

※：オリジナル AES プログラム　http://csrc.nist.gov/CryptoToolkit/aes/rijndael/

◇

デンソークリエイトは、高い品質を要求される自動車分野での組込みソフトウエア開発に多くの実績を持っています。今後とくに、家電など組込み分野でのネットワーク化が進むと、組込みソフト開発におけるセキュリティ要求も高まってきます。これに対して、本製品および関連するセキュリティ技術をベースとした、ソフトウエアでの受託開発やセキュリティ対策実現方法のコンサルテーションなど、顧客の要求に幅広く応えるサービスを展開していきます。

◇

※ 記載の会社名、製品名は、それぞれの会社の商標または登録商標、サービス名称です。

お客様からのお問い合わせ先

株式会社デンソークリエイト http://www.dcinc.co.jp/
新事業推進・イオタクリエイト
TEL：03-3780-7081（東京フロント）
052-229-1192（名古屋本社）
e-mail：info@dcinc.co.jp
本製品に関する情報：http://www.dcinc.co.jp/Service/Security/

報道関係者からのお問い合わせ先

株式会社デンソークリエイト
新事業推進・イオタクリエイト　塩谷 敦子
〒150-0021 東京都渋谷区恵比寿西 2-2-6 恵比寿ファイブビル
TEL：03-3780-7081　　e-mail：shiya@dcinc.co.jp

以上