（報道発表資料）

2003年7月28日

日本電信電話株式会社
株式会社日立製作所
三菱電機株式会社

# 世界初！　暗号技術で日本を代表する企業3社が実装技術を共同で開発

～楕円曲線暗号（ECDSA署名）実装技術の共同研究開発プロジェクト～

日本電信電話株式会社（本社：東京都千代田区、代表取締役社長：和田紀夫／以下、NTT）、株式会社日立製作所（本社：東京都千代田区、執行役社長：庄山悦彦／以下、日立）、三菱電機株式会社（本社：東京都千代田区、執行役社長：野間口有／以下、三菱電機）の3社は、共同研究開発プロジェクトにより、楕円曲線暗号（ECDSA署名）（＊1）の実装方式を開発し、「CRESERC（クレサーク）」と名づけました。

本技術は、NTT、日立、三菱電機の3社がプロジェクトチームを組み、楕円曲線暗号（ECDSA署名）の安全かつ高速な実装技術を共同で研究開発したもので、暗号技術で定評のある代表的な複数の企業が、ハイレベルの技術を持ち寄って共同で実装技術を開発した例としては、世界でも初めての事例です。

**＜共同研究開発の経緯＞**

現在、「e-Japan重点計画」で挙げられている電子政府（＊2）やユビキタス（＊3）環境の実現に向け、安全な通信環境を確保し高度情報流通社会を支える基盤となる技術の確立が急がれています。

その中核となるのは、暗号技術と電子認証（＊4）技術ですが、ことに実際の運用に耐え得る「安全かつ高速な実装技術」は、極めて重要な研究開発課題となっています。

しかしこれまで、実装技術は「安全性」と「処理速度」のトレードオフというジレンマとの戦いでした。そこで、NTT、日立、三菱電機の3社は、共同研究開発プロジェクトを立ち上げて検討を行い、このたび、既存製品と同等の「処理速度」を確保しつつ、世界最高レベルの「安全性」を実現する実装技術の開発に成功しました。

2003年3月には、欧州連合（EU）がNESSIE（＊5）プロジェクトとして進めていた次世代暗号方式の選定作業で、NTTと三菱電機が共同開発した「Camellia」（＊6）ならびに三菱電機の「MISTY1」（＊7）、NTTの「PSEC-KEM」（＊8）が、推奨暗号として選定されています。また、国際標準化機構

ISOでも、早ければ2004年春の確定を目途に進めている暗号標準の審議過程において、上記「Camellia」と「MISTY1」、「PSEC-KEM」の他、日立の「MULTI-S01」（＊9）と「MUGI」（＊10）が、国際標準暗号候補に残っています。さらに、これら暗号アルゴリズムは共に、総務省および経済産業省の電子政府における調達のための暗号評価プロジェクト（CRYPTREC）でも推奨暗号として選定されています。

このような暗号アルゴリズムの評価・選定、標準化活動は1990年代末より米国政府、EU、 ISO、日本国政府などにより活発に行われてきましたが現在はほぼ完了し、21世紀前半で標準的に用いられる暗号アルゴリズムが定まりつつあります。その中でも、上記の日本製暗号はいずれも処理速度が速いことやチップとして製品化しやすいことが評価されており、日本企業の暗号技術が世界の主流として普及する公算が高まっています。一方、ISO やCRYPTRECでは、今後は暗号アルゴリズムの「実装の安全性」の評価が重要であるとの認識の下に、その評価項目や評価基準制定のための検討を進める予定となっております。

このように「暗号実装の安全性」に対する認識が高まる中、NTT、日立、三菱電機の3社により共同研究開発された「楕円曲線暗号実装方式CRESERC（クレサーク）」は、この分野において世界でもトップレベルの実装技術として、電子政府やユビキタス関連システムなど情報セキュリティ技術が必要となるさまざまな応用分野に導入されることが期待されています。

**＜3社の役割分担＞**

本共同研究開発において、NTT、日立、三菱電機の3社は、共通の得意分野である楕円曲線暗号理論をベースに、各社の優位技術を活用して以下のような役割分担でプロジェクトを推進してきました。

◇ NTT　… 基本演算の高速安全実装技術
◇ 日立　… 楕円曲線演算の安全実装技術
◇ 三菱電機 … 楕円曲線演算の高速実装技術

**＜今後の方向性＞**

今後、3社は本共同研究開発成果である「楕円曲線暗号実装方式CRESERC（クレサーク）」に基づき、各社の優位技術を活かしたプロダクトを、電子政府向けシステムやユビキタス関連のセキュリティ製品に導入していく予定です。

**＜用語解説＞**

＊1　楕円曲線暗号

楕円曲線上の演算規則を利用した新しい公開鍵暗号技術。暗号強度を確保し

つつ、短い鍵長で高速にデータを暗号化できるため、RSA暗号に次ぐ次世代公開鍵暗号として注目されている。ECDSA（Elliptic Curve Digital Signature Algorithm）は、楕円曲線暗号による電子署名のアルゴリズムであり、NESSIEやCRYPTRECでも推奨暗号として選定されている。

＊2　電子政府

　コンピュータシステムやインターネット技術を活用して、行政実務処理をはじめとするさまざまな処理を電子化した行政機構のこと。

＊3　ユビキタス（Ubiquitous）

　もともとは、ラテン語で「いたるところに偏在する」という意味。インターネットなどの情報ネットワークに、いつでも、どこからでもアクセスできる環境を指す。

＊4　電子認証

　電子署名と公開鍵証明書（電子証明書）を用いて、電子の世界で印鑑と印鑑証明書を実現する技術。

＊5　NESSIE (New European Schemes for Signatures, Integrity, and Encryption)

　2000年から3年間の期間で実施された欧州連合（EU）認定の次世代暗号選定のためのプロジェクト。

＊6　Camellia

　NTTと三菱電機が共同で開発した128ビットブロック暗号アルゴリズム。詳細仕様が公開されている。

＊7　MISTY1

　三菱電機が開発した64ビットブロック暗号アルゴリズム。詳細仕様が公開されている。

＊8　PSEC-KEM

　NTTが開発した公開鍵暗号アルゴリズム。詳細仕様が公開されている。

＊9　MULTI-S01

　日立製作所が開発した256ビット鍵長ストリーム暗号アルゴリズム。詳細仕様が公開されている。

＊10　MUGI

　日立製作所が開発した128ビット鍵長ストリーム暗号アルゴリズム。詳細仕様が公開されている。

【本件に関するお問い合わせ】

ＮＴＴ情報流通基盤総合研究所
企画部　広報担当　飯塚、佐野、遅塚
TEL：0422-59-3663
E-mail：koho@mail.rdc.ntt.co.jp

株式会社日立製作所
コーポレート・コミュニケーション本部　広報部　紺野
TEL：03-3258-2056
E-mail：atsushi_konno@hdq.hitachi.co.jp

三菱電機株式会社
広報部　鎌田
TEL：03-3218-2172
E-mail：Yutaka.Kamada@hq.melco.co.jp

NTT ニュースリリース