NEWS RELEASE

NTT

日本電信電話株式会社

２００６年４月１３日

128ビットブロック暗号「Camellia」のオープンソースを公開
～多くの国際標準規格に採用された次世代国産暗号を広く使いやすいものに～

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」）は、2000年に三菱電機株式会社（本社：東京都千代田区、執行役社長：下村 節宏、以下「三菱電機」）と共同開発した128ビットブロック暗号※1アルゴリズム「Camellia（カメリア）」のNTT製ソースコード（C言語版・Java版）を、オープンソースとして、本日（2006年4月13日）よりホームページ上にて公開いたします。主要な国際標準暗号・推奨暗号に選定された国産暗号がオープンソースとして提供されることは初めてのことであり、Camelliaを、日本発の暗号技術として安全な高度情報流通社会を支える国際的な基盤技術に広めていくとのNTTの方針に基づいて実施するものです。

なお、このソースコードは、従来ホームページ上で公開していた参照コードよりも約3倍（当社比）高速なものであり、オープンソースコミュニティに対して順次提供していく暗号エンジンとなる予定のものです。

Camelliaホームページ　　：http://info.isl.ntt.co.jp/crypt/camellia/index.html
オープンソース掲載ページ：http://info.isl.ntt.co.jp/crypt/camellia/source.html

背景とオープンソース公開の意義

Camelliaは、世界最高レベルの安全性と実用性に優れた暗号方式として世界的に高く評価されており、ISO/IEC国際標準暗号※2をはじめ、欧州連合推奨暗号※3や電子政府推奨暗号※4などの国際的な暗号の標準化規格・推奨規格に選定されています。また、国産暗号としては初めてインターネットでの主要な暗号通信プロトコルであるSSL/TLS、IPsec、S/MIME、XMLにおける標準規格（IETF Standard Track RFC※5）の暗号方式にも採用されました。

今回NTTは、主要な国際標準暗号・推奨暗号に選定されたCamelliaを日本発の暗号技術として安全な高度情報流通社会全般を支える国際的な基盤技術に広めていくとの方針のもと、基本特許無償許諾契約を締結しなくてもCamelliaを自由に利用できる環境を提供することといたしました。

その一環として、本日（2006年4月13日）よりCamelliaのNTT製ソースコー

ドを、マルチプルライセンス形式※注）のオープンソースとして無償で公開いたします。これにより、Camelliaを搭載する製品開発や試験運用・利用にあたっての利用者の作業負担が大幅に軽減され、更なるCamelliaの普及・促進が図られるものと期待しております。

※注）　マルチプルライセンス形式：ソースコードとしては同一のものですが、オープンソースとしての利用（ライセンス）条件が異なる複数のオープンソースを用意してあります。

Camelliaの特長

Camelliaは、2000年にNTTと三菱電機が共同で開発した128ビットブロック暗号（鍵長128, 192, 256ビットの3種類が利用可能）であり、世界最高レベルの安全性を確保するとともに、PCかICカードかといったプラットフォームに依存しない高速なソフトウェア実装と、128ビットブロック暗号としては世界最小かつ最高水準の処理効率を有するハードウェア実装が可能であるなど、優れた実装性能をも兼ね備えた暗号方式です。

これらの特長に関しては、数年にわたる世界中の暗号研究者らによる十分な第三者評価検証も行われており、現在主流の64ビットブロック暗号Triple DESと比較すると、安全性が非常に高いうえに、処理速度が4～5倍高速であることが確認されています。この結果、AES※6と同等の安全性と処理性能を有する世界でも唯一の128ビットブロック暗号として、事実上の日本を代表する暗号であると国際的に認知されています。

実際に、安全性の観点から、様々な暗号の標準化規格・推奨規格でAESとCamelliaの両方が選定されています。

今後の展開について

オープンソースの公開を契機として、OpenSSLやLinuxをはじめとするオープンソースコミュニティに対してもCamelliaのオープンソースを提供し、早期にCamelliaが標準搭載されるよう、働きかけを行ってまいります。また、Camellia搭載製品のラインアップ充実・展開を図るために、Camelliaを搭載する製品を開発・事業化する企業・法人様に対して技術支援や導入支援などのサポートも提供してまいります。

今後ともCamelliaをより一層広く利用していただけるよう、SSL/TLSなどを利用するセキュリティ製品への組み込みをはじめとして、Camellia搭載の製品・サービスの開発を積極的に進めるとともに、真に安心・安全な情報化社会の実現に貢献すべく、研究開発を推進していきます。

基本特許無償許諾契約の取り扱いについて

Camellia基本特許を共有するNTTと三菱電機は、従来Camelliaを搭載する製品を開発・事業化する企業・法人様を主な対象に基本特許無償許諾契約に基づく特許無償化を行ってきました。しかしながら、今般、NTTと三菱電機の合意に基づき、今後は、Camelliaの利用者におかれては、基本特許無償許諾契約を締結せずともCamellia基本特許を無償にてご利用いただけることといたしました。

なお、ご要望があれば、従来同様、NTT・三菱電機との三社による基本特許無償許諾契約に基づく実施許諾を受けることも可能です。

Camelliaの歴史

2000年3月	暗号アルゴリズム Camellia発表
2001年4月	基本特許無償化を発表
2003年2月	日本の電子政府推奨暗号に認定
2003年2月	NESSIEにおいて欧州連合推奨暗号に公式認定
2003年2月	TV-Anytime ForumでのDRM暗号に採用
2004年1月	IETF S/MIME用標準暗号に採用 [RFC3657]
2005年4月	IETF XML用標準暗号に採用 [RFC4051]
2005年5月	ISO/IEC国際標準規格に採用 [ISO/IEC18033-3]
2005年7月	IETF SSL/TLS用標準暗号に採用 [RFC4132]
2005年12月	IETF IPsec用標準暗号に採用 [RFC4312]
2006年4月（今回）	オープンソース公開

＜用語解説＞

※1　128ビットブロック暗号

データを128ビットのブロック長（データのまとまりの長さ）ごとに暗号化する共通鍵暗号の1つ。共通鍵暗号とは、データの暗号化と復号に同じ秘密鍵を用いる暗号方式であり、高速な処理ができるため、大量のデータを扱う通信メッセージやファイルの暗号化や携帯端末の認証などに多く使われている。

なお、ブロック暗号には、CamelliaやAESなど1990年代後半以降に作られた128ビットブロック暗号と、Triple DESやMISTY1など1990年代半ば以前に作られた64ビットブロック暗号（64ビットのブロック長）がある。

※2　ISO/IEC国際標準暗号

国際標準化機構／国際電気標準会議ISO/IECが初めて選定した国際標準暗号方式。

ISO/IEC9979（暗号方式登録制度）に替わって、第三者機関（NESSIE、CRYPTREC等）による安全性や処理性能の評価報告を基に、ISO/IEC18033として初めて国際標準暗号が規格化された。次世代標準となる128ビットブロック暗号では、Camellia、AES、SEEDのみが採用された。

※3　欧州連合推奨暗号

2000年から2003年にかけて欧州連合が実施したNESSIE（New European Schemes for Signatures, Integrity, and Encryption）プロジェクトにおいて、高い安全性と処理性能を有する方式として選定された暗号技術。応募された暗号技術39個を含む総計44個の暗号技術のなかから17個が選定された。

日本の暗号としては、Camellia（128ビットブロック暗号・NTT/三菱電機）、MISTY1（64ビットブロック暗号・三菱電機）、PSEC-KEM（公開鍵暗号・NTT）が選ばれた。

※4　電子政府推奨暗号

2000年から2003年にかけて評価・審議された暗号技術評価委員会CRYPTREC（CRYPTography Research & Evaluation Committees）において、電子政府システムでの利用に資するかどうかの観点から安全性に特に問題がないと判断された暗号技術。応募された暗号技術52個を含む総計66個の暗号技術のなかから31個が選定された。

※5　Standard Track RFC（Standard Track Requests For Comments）

インターネット標準（Internet Standard）になるための仕様として公開される公式ドラフト文書。

IETFが発行するすべての文書にRFCの番号が付与されるが、それらは、インターネット標準規格としてIETFが規格審議・承認・管理を行うStandard Track RFCと、情報提供を目的として公開されるNon-standard Track RFCに分類される。

※6　AES（Advanced Encryption Standard）

2001年に米国商務省国立標準技術研究所NIST（National Institute of Standards and Technology）により制定された米国政府標準の128ビットブロック暗号で、「高度暗号化規格」とも呼ぶ。1997年から2000年にかけて行われたAESプロジェクトにおいて安全性および処理性能で最も優れていると判断された、J. DaemenとV. Rijmenが提案したRijndaelをベースに規格化された。

＜参考図＞

・図1　ブロック暗号標準化の現状

【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　遅塚、佐野、中村
TEL：0422-59-3663
E-mail：koho@mail.rdc.ntt.co.jp

NTT ニュースリリース