NEWS RELEASE

NTT

日本電信電話株式会社

2006年11月8日

国産唯一の次世代国際標準暗号「Camellia」を オープンソースコミュニティOpenSSL Projectが採用

～オープンソースライブラリとして組込・配布も自由にでき 世界的な普及促進に弾み～

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」）が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）」が、国際的なオープンソースコミュニティであるOpenSSL Projectが開発するSSL/TLS※2プロトコル用暗号ツールキットOpenSSL toolkitに採用されました。

NTTでは、安心・安全な高度情報化社会を支えるために、主要な国際標準暗号・推奨暗号に選定されたCamelliaを国際的な基盤技術として広めていくとの方針のもと、2006年4月13日にオープンソース化を実施してCamelliaを自由に利用できる環境を提供するとともに、オープンソースコミュニティに対してもCamelliaのソースコードを提供するなど、採用に向けた活動を行ってまいりました。

その結果、本年9月にリリースされたOpenSSL 0.9.8c版にCamelliaが搭載されました。

OpenSSL toolkitにCamelliaが採用されたことは、米国政府標準暗号AES※3と同等の安全性と処理性能を有する世界唯一の暗号方式としてのCamelliaの位置づけがより確かなものになったものといえます。今後、Camelliaが搭載されたOpenSSL toolkitが世界中のWWWサーバなどに組み込まれ、また世界有数のオープンな暗号ライブラリとしても利用されるようになることによって、Camelliaの利用や製品開発が世界規模でより一層広がるものと期待しております。

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
OpenSSL Projectページ　　：http://www.openssl.org/

＜背景とOpenSSLでの採用の意義＞

Camelliaは、世界最高レベルの安全性と処理性能を備えた次世代暗号方式として、ISO/IEC国際標準暗号※4をはじめ、欧州連合推奨暗号※5や電子政府推奨暗号※6などの国際的な暗号方式の標準化規格・推奨規格に選定されるなど、事実上の日本を代表する暗号方式として国際的に認知されています。また、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※7）の暗号方式にも採用されています。

NTTでは、世界的に高く評価されているCamelliaのメリットをより多くの人々に享受していただけるよう、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無償で公開し、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しております。さらに、オープンソースコミュニティに対してもCamelliaのソースコードを提供するなど、採用に向けた活動を行っています。

OpenSSL toolkitの機能には、SSL/TLSのデファクトスタック、暗号エンジン、PKIアプリケーション開発ツールキットという3つの側面があります。

このなかで、共通鍵暗号の暗号エンジンとして、現世代暗号ではTriple DES、RC4等複数の暗号が搭載されていますが、次世代暗号ではAESのみがOpenSSL 0.9.7版からサポートされているという状況でした。今回CamelliaがOpenSSL 0.9.8c版から搭載されたことで次世代暗号としても複数の暗号を利用できる環境*注）が整い、より安心・安全な高度情報化社会の実現に貢献できるものと考えています。

表　OpenSSL toolkitに搭載されている暗号

ブロック暗号		ストリーム暗号（現世代）
64ビットブロック暗号（現世代）	**128ビットブロック暗号（次世代）**	
DES、Triple DES、DESX、Blowfish、RC2、RC5、CAST5（CAST-128）、IDEA	**AES、Camellia**	RC4

注）現在のOpenSSL 0.9.8x版において、標準コンパイルオプションのままではCamelliaは自動でインストールされません。次回のメジャーバージョンアップ時に、標準インストールされるようになる予定です。

現在世界中にあるWWWサーバの60%以上でOpenSSL toolkitが組み込まれており、今後はこれらすべてにCamelliaが順次搭載されるようになります。また、OpenSSL toolkitを利用した様々な製品開発などでもCamelliaが標準的に選択できるようになるなど、Camelliaの利用や製品開発が促進されると期待されます。

＜仕様公開・オープンソース化の意義＞

Camelliaはその仕様を当初から公開しており、すでに世界中の暗号研究者によってアルゴリズムの安全性評価や性能評価が多数行われています。それらの評価結果は、報告書や国際暗号学会等で公表されており、Camelliaが世界最高レベルの暗号方式であることの技術的裏づけとして国際規格、推奨規格に選定される根拠となっています。

今後、OpenSSL toolkitに搭載されたCamelliaのオープンソースコードが世界中に配布されることにより、プログラム実装においても世界中の技術者による評価・改良・組込が行われ、より使いやすい暗号に成長していくものと期待しています。

また、実際の製品においては実装上の脆弱性が信頼性・安全性の脅威ともなりますが、アルゴ

リズムを公開することと同様、暗号エンジンをオープンソースとして公開することにより、その実装についても世界中の技術者によって監視されることになるため、実装上の安全性が高まる効果も期待されます。

＜Camelliaの特長と歴史＞

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）です。世界最高レベルの安全性の確保はもとより、PCでもICカードでも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が可能で、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もできるなど、優れた処理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と同等の安全性と処理性能を有する世界で唯一の128ビットブロック暗号として、事実上の日本を代表する国産暗号として国際的にも認知されています。

Camelliaは、高度情報化社会の健全な発展を図るべくオープンソースに基軸を置くというNTTの基本的な方針のもと、以下のような経緯をたどって現在に至っています。

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	オープンソース公開
2006年9月	**OpenSSLで採用（openssl-0.9.8c以降から採用）**

＜今後の展開＞

NTTでは、Camelliaをより一層広く利用していただけるよう、今回のOpenSSL toolkitへの採用だけにとどまらず、LinuxやFreeBSDなどを扱うオープンソースコミュニティなどに対してもCamelliaの採用に向けた活動を継続してまいります。

また、Camelliaを搭載した製品・サービスの開発を自らも積極的に進めるとともに、Camellia搭載製品の開発や事業化、導入などを希望される企業・法人様との連携も図ってまいります。

＜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　SSL/TLS (Secure Socket Layer /Transport Layer Security)

SSLは、ネットスケープ社が開発した暗号通信プロトコルであり、インターネット上で送受信されるデータを暗号化し、安心して通信が行えるようにする仕組み。TLS は、SSL3.0の次期バージョンとして名称変更を行ったうえでIETFにより標準化された。

現在のIEやFirefoxなどのブラウザにはSSL/TLSが標準で搭載されているため、ECサイトやネットバンキングなどのサービスを利用する際、暗証番号やクレジットカード番号、個人情報などの送信のためにSSL/TLSを使うケースが一般的である。最近では、利用者が意識しなくても、暗号通信が必要な場面で自動的にSSL/TLSが使われるように設定しているサイトも多くなってきている。

※3　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。

※4　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。

※5　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。

※6　電子政府推奨暗号

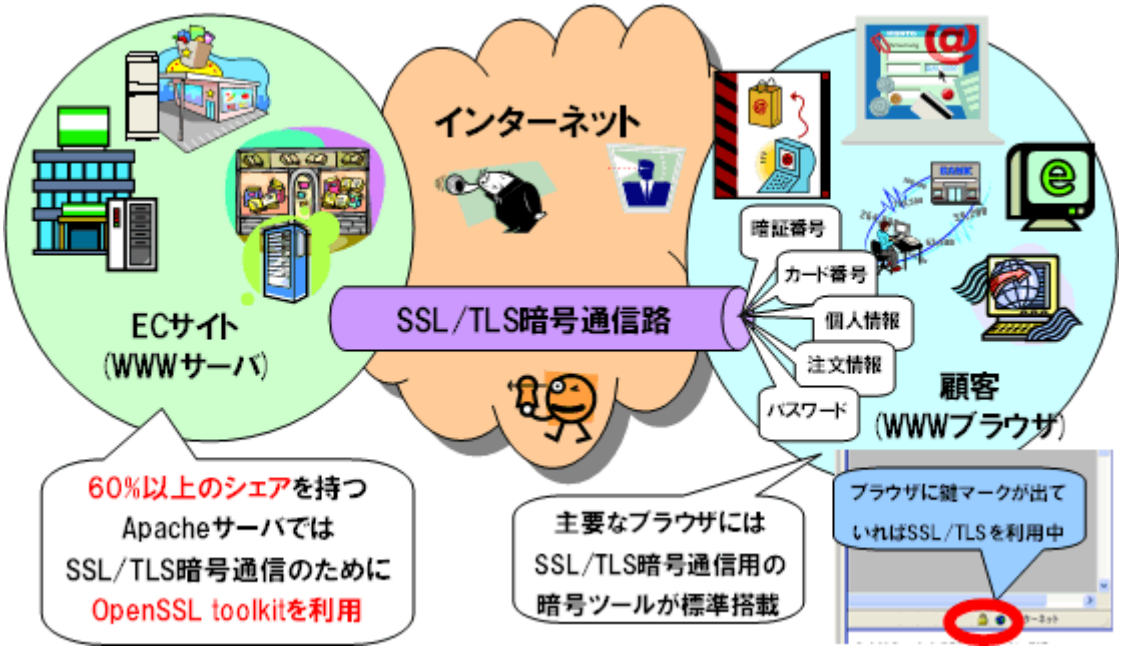
2000年から2003年にかけて評価・審議された暗号技術評価委員会CRYPTREC（CRYPTography Research & Evaluation Committees）において、電子政府システムでの利用に資するかどうかの観点から安全性に特に問題がないと判断された暗号技術。応募された暗号技術52個を含む総計66個の暗号技術のなかから31個が選定された。

※7　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。

<参考図>



【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（ちづか）、佐野、中村
TEL：0422-59-3663
E-mail：koho@mail.rdc.ntt.cp

NTT ニュースリリース