NEWS RELEASE

NTT

日本電信電話株式会社

2007年11月13日

次世代暗号「Camellia」の
主要オープンソースソフトウェアへの採用が大きく進展

～ 大手ベンダ製品にも相次いで搭載 ～

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：三浦 惺、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、昨年OpenSSLに採用されたことに続いて、LinuxやFirefoxなどの国際的にも主要なオープンソースソフトウェアに相次いで採用されました。これにより、安心・安全な高度情報化社会を支える国際的な次世代の基盤技術として、名実ともに初めて国産暗号が本格的に利用できる環境が大きく整ってきたことになります。

また、大手企業によるCamellia搭載製品の開発、リリースも加速しており、日本セーフネット株式会社のQuickSec Toolkitをはじめとして、セキュリティ製品やサービスでの利用も急速に進展しています。

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

＜背景とCamellia普及の意義＞

NTTは、安心・安全な高度情報化社会の健全な発展を図るべく、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基本的な方針のもと、2006年4月13日にオープンソース化を実施し、Camelliaを自由に利用できる環境を提供してきました。また、オープンソースソフトウェアコミュニティに対してもCamelliaのソースコードを提供、提案する活動を行ってきました。

その結果、2006年9月にリリースされた暗号ツールキットOpenSSL 0.9.8c版にCamelliaが採用されたことを皮切りに、LinuxやFreeBSDなどのOSカーネルや、Webブラウザ Firefox（次期版）など、多くの国際的に主要なオープンソースソフトウェアに相次いで採用されました（表1参照）。これは、国産暗号として初めての快挙であり、次世代暗号として名実ともにCamelliaが国際的な信用も獲得した証明といえます。

特に、一般に流通しているWebブラウザであるFirefoxに新規暗号としてCamelliaが今回採用されたことは、十分に国際的な信用を得た暗号でない限り追加採用をしないMozillaが米国政府標準暗号AES※2を採用して以来、約5年ぶりの異例な出来事になります。Firefox次期版もしくは開発版（Gran Paradiso alpha7以降）で、Camelliaに対応したWebサーバ（下記のアドレス）にアクセスするとCamelliaでWeb暗号通信（SSL/TLS通信※3）を実際に行っていることをご確認いただけます（図参照）。

Camellia ホームページ[https用]
（https://info.isl.ntt.co.jp/crypt/camellia/index.html）
※接続後、右クリックをして「View Page Info」を選択してください。

図　国産暗号によるSSL/TLS暗号通信が初めて可能に

さらには、日本市場をはじめとしてCamelliaの利用が期待される状況になりつつあることを反映して、NTT/三菱電機グループ以外にも、QuickSec Toolkit（日本セーフネット株式会社）のほか、Netcocoon Analyzer（松下電工株式会社）、SH7781グループ（株式会社ルネサステクノロジ）、netHSM・nShield（エンサイファー株式会社）など、大手企業によるCamellia搭載製品の発売・開発が急速に進展しています。また、株式会社ミクシィなど大手企業の情報システムでのCamelliaの採用も進んでおります（詳細は、各社のニュースリリース・ホームページ、またはCamellia ホームページの製品情報・採用実績をご参照ください）。

このように、様々な環境でCamelliaが実際に利用できるようになったことで、暗号利用製品やサービスにおいてAESとCamelliaという2種類の次世代暗号アルゴリズムを選択できるようになり、一つの暗号技術だけに依存しない、より安全性の確保された高度情報化社会の実現に国産暗号が大きく貢献することが期待できるようになりました。

表1 オープンソースソフトウェアコミュニティが提供するCamellia搭載プロダクト

オープンソースソフトウェア	搭載バージョン	備考
OpenSSL toolkit	0.9.8c以降	暗号ツールキット
Crypto++ library	5.4以降	暗号ツールキット
NSS (Network Security Services)	3.12以降（予定）	暗号ツールキット
The Legion of the Bouncy Castle	1.30以降	Java 暗号ツールキット
libgcrypt (GnuPG)	2以降	GNU版 暗号ツールキット
Linux kernel	2.6.21以降	OSカーネル

Fedora	7以降	OSカーネル （Linuxディストリビューション）
FreeBSD	7.0以降（6.x準備中）	OSカーネル
Firefox	3.0 以降（予定）※注	Webブラウザ
IPsec-tools	0.7以降	IPsec支援アプリケーション

※注 Firefox 3.0は2007年冬頃リリースが予定されています。現在は、Firefox 3.0開発版（Gran Paradiso alpha7以降）でCamelliaをご利用いただけます。

＜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やICカードなどの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。

Camelliaはその仕様を当初から公開しており、すでに世界中の第一線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、報告書や論文、国際暗号学会等で公表されており、技術的にCamelliaが世界最高レベルの暗号方式であることの裏付けとなっています。

このことから、実際に、AES同等の安全性と処理性能を有する世界唯一のAES代替暗号アルゴリズムとして、また事実上の日本を代表する暗号アルゴリズムとして、国際的にも多くの標準規格・推奨規格に採用されています（表2参照）。

表2　Camelliaが採用されている標準規格・推奨規格

標準化機関等	標準化概要
ISO/IEC	ISO/IEC国際標準暗号 (ISO/IEC18033-3)
NESSIE	欧州連合推奨暗号
CRYPTREC	電子政府推奨暗号
IETF	SSL/TLS標準暗号 (RFC4132)
	IPsec標準暗号 (RFC4312)
	S/MIME標準暗号 (RFC3657)
	XML標準暗号 (RFC4051)

	OpenPGP暗号 (審議中)
	Description of Camellia (RFC3713)
RSA Laboratories	暗号トークン標準インタフェース (RSA PKCS#11)
ITU-T	次世代ネットワーク(NGN)用暗号 (審議中)
TV-Anytime Forum/ ETSI	次世代放送コンテンツ流通システム著作権管理・情報保護(DRM)用暗号

＜今後の展開＞

オープンソースソフトウェアコミュニティやソフトウェア開発者へのCamellia活用・導入に向けた活動を継続すると共に、Camelliaが搭載されたオープンソースソフトウェアや暗号製品を活用したアプリケーションサービスの研究開発を推進し、安心・安全な高度情報化社会の構築に向けた活動を幅広く展開していきます。

＜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　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。

※3　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Internet Explorer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。

・図　国産暗号によるSSL/TLS暗号通信が初めて可能に

【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）、山形
TEL：0422-59-3663
E-mail：islg-pr@lab.ntt.co.jp

NTT ニュースリリース

Copyright(c) 2007 日本電信電話株式会社