NEWS RELEASE

NTT

日本電信電話株式会社

2005年7月20日

日本初！128ビットブロック暗号アルゴリズム「Camellia」がインターネットにおける次世代標準暗号規格に採用

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」）と三菱電機株式会社（本社：東京都千代田区、執行役社長：野間口 有、以下「三菱電機」）が2000年に共同開発した128ビットブロック暗号※1アルゴリズム「Camellia（カメリア）」が、このたび国産暗号アルゴリズムとしては初めて、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※2、S/MIME※3、XML※4における標準規格（IETF Standard Track RFC※5）の暗号方式として採用されました。また、IPsec※6においても標準規格としての採用に向けたIETF※7での審議が終了し、今秋中の採用が内定しました。

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、すでにISO/IEC国際標準暗号※8をはじめ、欧州連合推奨暗号※9や電子政府推奨暗号※10などの国際的な標準化規格・推奨規格に採用されています。今回のIETFでの採用により、インターネットの世界においても標準実装すべき次世代のインターネット標準暗号として認められたことになります。

背景と標準化の意義

Camelliaは、世界的にも米国政府標準暗号AES※11と同等の安全性と処理性能を有する唯一の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。その結果、2003年には欧州連合推奨暗号と電子政府推奨暗号に、また最近ではISO/IEC国際標準暗号にも選定されてきました。

その一方、例えば、オンラインショッピングやネットバンキングなどのWebサービスを利用する場合、一般的にはホームページの閲覧で利用するWebブラウザに標準搭載されているSSL/TLSが使われています。これは、インターネットを経由した電子申請システムなどの政府系システムにおけるWebサービスでも同様です。

このSSL/TLSで利用できる暗号は、あくまでSSL/TLS用インターネット標準暗号に規定されたものの中からしか選択できないので、いくら電子政府推奨暗

号などにCamelliaが選定されていても、SSL/TLS用インターネット標準暗号にCamelliaが規定されていなければ、電子政府システムなどにおけるWebサービスといえどもCamelliaは利用できないのが現実です。
　つまり、アルゴリズムとしての技術的な優秀さやデジュレ標準などに採用されるだけでは、インターネットを利用したサービスや実際の製品で広く利用される環境として不十分でした。

　ところで、インターネットでの現在の主要な暗号通信プロトコルであるSSL/TLSやS/MIMEなどでは、プロトコル制定当時に利用可能だったTriple DES, IDEA, RC2, RC4など1995年以前に開発された暗号をインターネット標準暗号として採用しており、現在でもTriple DESとRC4が標準的に利用されています。
　IETFでは、近年の解読技術の進展に伴う安全性低下が懸念される従来の標準暗号とは別に、国際的に安全と認められた暗号アルゴリズムのインターネット標準暗号への追加検討を行ってきました。とりわけ、現在主流の64ビットブロック暗号Triple DESや脆弱性が指摘されているRC4よりも安全性が高く、今後の移行先として国際的に推奨されている128ビットブロック暗号を対象に審議が行われてきました。
　今回、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様々な標準化規格・推奨規格に採用されていることが評価され、国産暗号アルゴリズムとしては初めて、SSL/TLSでのインターネット標準暗号規格として採用されることがIETFにより承認されました。また、そのほかの主要な暗号通信プロトコルであるIPsec、S/MIME、XMLにおいても採用もしくは採用が内定しています。
　これにより、Camelliaは、欧州連合推奨暗号と電子政府推奨暗号などでの選定のほか、本年5月のISO/IEC国際標準暗号への採用と合わせて、インターネットの世界においても標準実装すべき次世代のインターネット標準暗号として認められたことになります。今後は、もっとも身近な通信手段であるインターネットを利用した電子政府システムやネットバンキング、オンラインショッピングなどのさまざまなシステムにおいても、国産暗号アルゴリズムが初めてインターネット標準暗号として利用されることが期待されます。
　なお、IETFでは、Camelliaのほか、AES（米国政府標準暗号）とSEED※12（韓国政府標準暗号）のみを次世代のインターネット標準暗号として採用もしくは採用内定としています。これは、次世代標準としてISO/IEC国際標準暗号に採用された128ビットブロック暗号と一致しております。

今後の展開について

　今回、世界（ISO/IEC国際標準暗号）、欧州（欧州連合推奨暗号）、日本（電子政府推奨暗号）の3つの主要な暗号評価／標準化プロジェクトでの採用に加え、国産暗号アルゴリズムとしては初めてインターネット標準暗号規格に

Camelliaが採用されたことにより、日本の暗号技術がさらに世界規模で幅広く利用されることが期待されます。

NTTでは、Camelliaをより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、今後も研究開発を推進していきます。

また、世界のデファクトスタンダードを目指すCamelliaの早期普及の観点より、Camellia搭載製品のラインアップの充実、ならびにCamelliaに関心を持っていただいた企業、法人様などによる基本特許無償化を通じたCamellia搭載製品の展開を働きかけていきます。

＜参考＞

CamelliaのRFC番号

- RFC 3657 [Standard Track - Proposed Standard]:
  Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)
- RFC 3713 [Non-standard Track - Informational]:
  A Description of the Camellia Encryption Algorithm
- RFC 4051 [Standard Track - Proposed Standard]:
  Additional XML Security Uniform Resource Identifiers (URIs)
- RFC 4132 [Standard Track - Proposed Standard]:
  Addition of Camellia Cipher Suites to Transport Layer Security (TLS)
- RFC Ed Queue [Standard Track - Proposed Standard]:
  The Camellia Cipher Algorithm and Its Use With IPsec

Camelliaの特長

Camelliaは、世界最高レベルの安全性を有するとともに、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もつ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。とりわけ、実装性の点では、AESとは異なり、暗号化処理と復号処理が同じ構造で実現されることから、メモリ搭載量が少ないICカードや小型ハードウェアにおいて優位な性能を発揮します。

実際に、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が行われており、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、AESとは異なる暗号構造※13であるうえ、セキュリティマージン※14が大きめに取っているため、安全性の観点から様々な標準化規格・推奨規格でAESとCamelliaの両方が選定されています。

また、NTTと三菱電機では、Camelliaの普及・促進により低コストで安全な情報化社会の実現に向けて主導的役割を果たすため、公開仕様をもとにみずから Camellia を搭載した製品を開発、事業化していただける企業、法人様を主な対象に、相互主義の下、非独占的にCamellia基本特許の無償化を2001年から実施しています。

Camelliaホームページ：　http://info.isl.ntt.co.jp/crypt/camellia/index.html
Camelliaニュースリリース：
http://www.ntt.co.jp/news/news00/0003/000310.html
http://www.mitsubishielectric.co.jp/news/2000/0310.htm

＜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、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）と、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。「https:」ではじまる Web コンテンツの通信では、SSLでの暗号通信を意味している。

TLS は、SSL の最新バージョンSSL3.0の次期バージョンに相当するが、ネットスケープ社ではSSL4.0ではなくTLS1.0とし、SSL3.0に若干の改良を加えて名称変更を行い、IETFで標準化された。

※3 S/MIME (Multipurpose Internet Mail Extensions)

RSAデータセキュリティ社が提案し、IETFによって標準化された電子メールの暗号化方式。RSA公開鍵暗号方式を用いて証明書の確認やセッション鍵の

暗号化などを自動的に行うとともに、メッセージをそのセッション鍵による共通鍵暗号で暗号化して送受信する。

※4 XML (eXtensible Markup Language)

文書やデータの意味や構造を記述するためのマークアップ言語の1つで、「タグ」と呼ばれる特定の文字列でもとの文章に構造を埋め込んでいく言語の規格。コンピュータ同士でのデータの送受信に使用できるほか、Webブラウザで直接閲覧することも想定されている。現在のWebページ作成言語であるhtmlの将来的な代替規格と考えられている。

※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 IPsec (IP security protocol)

IPパケットの暗号化と認証を行なうことで、TCP/IP環境であるインターネット上での汎用的な暗号通信を行なうためのセキュリティ技術。現在インターネットで使われているIPv4ではオプションとして使用することができるが、次世代のIPv6では標準で実装される。

※7 IETF (Internet Engineering Task Force)

インターネットの標準規格を定める国際的に公開された団体で、WWW関連以外の一般的な幅広いインターネット標準を扱っている。IETFが策定したプロトコル仕様はTCP/IPプロトコル仕様から、上位のアプリケーション層まで多岐にわたっている。ISOなどのような国際標準団体ではないが、IETFで決定された仕様は、インターネットの事実上の国際標準となっている。

※8 ISO/IEC国際標準暗号

International Organization for Standardization（国際標準化機構）／International Electrotechnical Commission（国際電気標準会議）が初めて選定した国際標準暗号技術。

従来は、認証方式と署名方式を標準化の対象とし、暗号方式については登録制度（ISO/IEC9979）のみを運用してきた。しかし、ISO/IEC9979に替わって、2000年より暗号方式も標準化対象とすることとし、第三者評価（NESSIE、CRYPTREC等）などによって検討された結果、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。

※9 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 Signature, 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。

※10 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。

※11 AES (Advanced Encryption Standard)

2001年にNIST（米国商務省国立標準技術研究所）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したベルギー提案のRijndaelをベースに規格化された。

※12 SEED

1998年にKISA（韓国情報保護振興院）により制定された韓国政府標準の128ビットブロック暗号。CamelliaやAESと異なり、鍵長は128ビットに限定。

※13 暗号構造

ブロック暗号の構造としては、DES/Triple DES/MISTY1/Camellia/SEEDなどで利用されているFeistel型構造とAESで利用されているSPN型構造に大別される。前者は、データを二分割して片方のデータごとに撹拌していく構造であるのに対し、後者は全部のデータを一度に撹拌していく構造である。

Feistel型構造は、基本的に暗号化と復号が同一の演算処理で構成されることから、両方の処理を一つの実装で実行できる。これに対し、SPN型構造は、暗号化処理と復号処理を別々の実装とすることで、処理の並列度を向上させ、全体として高速性を実現できる。

※14 セキュリティマージン

ブロック暗号の将来的な安全性期待度を表す指標のひとつ。実際の仕様上の段数と現時点での解読可能な段数との比率として算出され、この値が大きいほ

ど、将来の暗号解読手法の進展に対する耐性が大きいと期待される。また、新たな解読手法が発見されるとこの値は徐々に低下し、最終的に1以下になるとその暗号は解読されたと言われる。ちなみに、現時点でのAESのセキュリティマージンは1.25-1.4であるのに対し、Camelliaは1.8-2.0である。

＜参考図＞

図1　ブロック暗号標準化の現状

図2　暗号構造の解説

問い合わせ先
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、井田
TEL：0422-59-3663
E-mail：koho@mail.rdc.ntt.co.jp

NTT ニュースリリース