2005年5月26日

（報道発表資料）

日本電信電話株式会社
三菱電機株式会社

世界の暗号アルゴリズムのデファクトスタンダードへ

128ビットブロック暗号アルゴリズム「Camellia」が ISO国際標準規格に採用

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アルゴリズム「Camellia（カメリア）」が、ISO/IEC※1（以下「ISO」）において、世界最高水準の安全性と実用性に優れた暗号方式として評価され、国際標準規格に採用されました。

背景と経緯

ISOでは、情報セキュリティ分野で署名アルゴリズムや認証メカニズムの標準化を行っていましたが、暗号アルゴリズムの標準化は行わず、暗号アルゴリズム登録制度(ISO/IEC9979)のみを運用してきました。

しかしながら、国際規格化に関する世界的な要望を受け、2000年にISOとして初めて暗号アルゴリズムの国際標準規格策定に着手し、約15カ国の提案に対して安全性や実用性（暗号処理性能やハードウェア/ソフトウェアの規模）を第三者評価（NESSIE、CRYPTREC等）などによって検討してきました。

その結果、今回「Camellia」を含めて、4カ国6種のブロック暗号アルゴリズムを標準規格(ISO/IEC18033)として採択しました。特に、次世代標準となる128ビットブロック暗号※2では、Camelliaのほかは、AES※3（米国政府標準暗号）とSEED（韓国政府標準暗号）のみが選ばれており、世界の暗号アルゴリズムのデファクトスタンダードへ向けての大きな成果となりました。

Camelliaの特徴

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、以下の(1)～(3)のような両社のノウハウ・技術を結集して設計開発されました。21世紀の暗号にふさわしい世界最高レベルの安全性を有するとともに、ソフトウェア・ICカード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、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暗号方式となっています。

（1）NTTが保有している高速ソフトウェア実装に適した暗号設計のノウハウ
（2）三菱電機が世界に誇る小型・高速ハードウェア実装に適した暗号設計のノウハウ
（3）両社が持つ世界最高水準の暗号安全性評価技術

なお、Camellia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を経て、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。具体的には、欧州連合推奨暗号※4、電子政府推奨暗号※5などですでに標準化採択済みです。さらに、現在、インターネット標準であるIETF※6標準暗号方式としての承認に向けた審議が進んでおります。

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

今後の展開について

NTTと三菱電機は、2000年に次世代ブロック暗号「Camellia」を共同で開発し、国内外の標準化活動に提案してきました。

今回のISOによる国際標準規格化により、「Camellia」は日本（電子政府）、欧州（NESSIE）、世界（ISO）の3つの主要な暗号評価/標準化プロジェクトすべてに採用されたことになり、これによって、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できます。

また、Camelliaの普及・促進により、低コストで安全な高度情報流通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、法人を主な対象に、相互主義の下、非独占的にCamelliaの基本特許の無償化を2001年から実施しています。

Camellia特許無償化：http://www.ntt.co.jp/news/news01/0104/010417.html

今後とも、Camelliaを広く利用していただけるよう、Camellia搭載の製品・サービスの開発を積極的に進めていきます。

ＮＴＴ／三菱電機の暗号技術開発の経緯

暗号アルゴリズム Camellia発表（ＮＴＴ、三菱電機）	2000年 3月
Camelliaの基本特許無償化を発表	2001年 4月
Camelliaが日本の電子政府調達暗号に認定	2003年 2月

CamelliaがNESSIEにおいて欧州連合推奨暗号に公式認定	2003年 2月
CamelliaがTV-Anytime ForumでのDRM暗号に採用	2003年 2月
CamelliaがISO国際標準規格に採用	2005年 5月（今回）

＜用語解説＞

※1　ISO/IEC

International Organization for Standardization（国際標準化機構）／International Electrotechnical Commission（国際電気標準会議）

※2　128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化に同じ秘密鍵を用いる暗号方式であり、高速な暗号処理ができるため、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。

※3　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。

※4　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。

※5　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。

※6　IETF （Internet Engineering Task Force）

インターネットの標準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。

問い合わせ先
日本電信電話株式会社
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

三菱電機株式会社
広報部
TEL：03-3218-2172
E-mail： prd.news@ml.hq.melco.co.jp

NTT ニュースリリース

Copyright(c) 2005 日本電信電話株式会社