MITSUBISHI
Changes for the Better

2013 年 3 月 26 日
日本電信電話株式会社
三菱電機株式会社

暗号アルゴリズム「Camellia」が新たな電子政府推奨暗号リストに採択決定

～128 ビットブロック暗号で国産暗号唯一の採択～

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: 鵜浦博夫、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: 山西健一郎、以下「三菱電機」）が 2000 年に共同開発した暗号アルゴリズム「Camellia（カメリア）」※1 が、インターネット上の通信などで最も普及が進んでいる 128 ビットブロック暗号※2 のカテゴリーにおいて、デファクト標準である米国政府の標準暗号 AES※3 と並び、数ある国産暗号の中から、唯一新たな電子政府推奨暗号リストに採択されました。

これは、「Camellia」が政府系情報システムの調達において、国産暗号の中で最も高い安全性と調達容易性を有していると評価されただけでなく、我が国の情報セキュリティ産業の競争力向上を先導する技術として期待されていることを意味します。

＜電子政府推奨暗号リスト採択の背景＞

「電子政府推奨暗号リスト」とは、暗号技術検討会（事務局: 総務省及び経済産業省）及び関連委員会（事務局: 情報処理推進機構及び情報通信研究機構）（以下、CRYPTREC※4）により 2003 年 2 月に制定されました。制定から 10 年目を迎えたこの度、内容の見直しによって「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」に改定され、安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するものを新たな電子政府推奨暗号リストとして採択することになりました。

＜「Camellia」の優位性＞

「Camellia」は、継続して評価されてきた安全性に加えて、過去 10 年以上にわたって行ってきた、各種標準化活動、「Camellia」基本特許無償化、及びオープンソース化により加速した利用・普及のための活動により、調達が容易な暗号としての実績も評価されてきました。これらの優位性から、今回の採択に至りました。

（1）高い安全性及び実装性能

暗号の安全性は、数多くの解読を試みる攻撃に長年耐えることにより評価が高まります。「Camellia」は開発以降 10 年以上にわたって国内外の暗号研究者らによってさまざまな解読手法を試みることによる安全性評価が続いており、新たに発表されたさまざまな解読法、例えば関連鍵攻撃や biclique を使った中間一致攻撃※5、rebound 攻撃※6 などについても解読可能かどうかの検証が行われましたがいずれも解読成功に至っていません。この点は、現実的な脅威には至っていないものの、理論的な問題点として指摘されている関連鍵攻撃での解読が成功した 192 および 256 ビット鍵長の AES との安全性面での違いとなっています。

（2）豊富な実績に基づく高い調達容易性

NTT と三菱電機は、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に 2001 年に「Camellia」基本特許の無償化を、2006 年にはオープンソース化を行いました。国内外で認められた国産暗号がオープンソース化されるのは日本で初めてのことであり、その結果として、OpenSSL、Firefox、Linux kernel、FreeBSD など国際的に有名なオープンソースプロジェクトにも数多く採用されるとともに、多くの国内外の市販製品で採用が進んでおります。

さらに、標準化活動にも力を入れており、世界最高レベルの安全性と実装性能に優れた暗号方式と

して既に ISO/IEC※7 国際標準暗号をはじめ、欧州連合推奨暗号※8 や、暗号通信プロトコル SSL/TLS などインターネット関連規格を含め数多くの国際標準規格・推奨規格に採用されています。特にインターネット関連での標準規格への採用は、国産暗号として初めてのことです。

＜今後の展望＞

NTT と三菱電機は、今後も「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及びそれらを活用したアプリケーションサービスの開発を推進し、引き続き公共/民間システムの安全性を支えるとともに、今後導入が想定される社会保障・税番号制度における情報管理など、安心・安全な高度情報化社会の構築に貢献していきます。

＜用語解説＞

※1 「Camellia（カメリア）」

2000 年に NTT と三菱電機が共同開発した 128 ビットブロック暗号。名称の由来である「Camellia（カメリア、つばき）」は日本原産の植物で、学名は「カメリア・ジャポニカ」。日本から生まれた暗号技術が、世界中でいろいろな形で発展していって欲しい、という開発者らの願いから名付けられた。

※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、また携帯端末の認証などに多く使われている。

※3 AES（Advanced Encryption Standard）

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

※4 CRYPTREC

CRYPTREC とは Cryptography Research and Evaluation Committees の略であり、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトのこと。総務省及び経済産業省が共同で運営する暗号技術検討会と、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で運営する暗号方式委員会、暗号実装委員会及び、暗号運用委員会で構成される。

※5 biclique を使った中間一致攻撃

2011 年に Bogdanov らにより発表。古くから知られている中間一致攻撃に、完全 2 部グラフ（biclique）を適用することにより、中間一致攻撃の適用範囲を拡大したもの。

※6 rebound 攻撃

2009 年に Mendel らにより発表。暗号学的ハッシュ関数の使い方に着目することにより、より効果的に差分解読法を適用可能としたもの。

※7 ISO/IEC

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

※8　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39暗号技術を含む総計44の暗号技術の中から17方式が選定された。日本の暗号としてはCamellia（128ビットブロック暗号）や他のカテゴリーを含め計3方式が選ばれた。

＜商標関連＞

【本件に関するお問い合わせ】
日本電信電話株式会社
サービスイノベーション総合研究所
企画部広報担当
TEL: 046-859-2032
E-mail: randd@lab.ntt.co.jp

三菱電機株式会社
広報部
TEL: 03-3218-2333