平成12年3月10日

日本電信電話株式会社
三菱電機株式会社

ＮＴＴと三菱電機が共同で次世代暗号アルゴリズム「Camellia」を開発
－高度な安全性と世界最高レベルの効率性を両立させた共通鍵ブロック暗号－

日本電信電話株式会社（以下、ＮＴＴ　本社：東京都千代田区大手町　宮津　純一郎社長）と三菱電機株式会社（以下、三菱電機　本社：東京都千代田区丸の内　谷口　一郎社長）は、次世代の共通鍵暗号(*1)アルゴリズム「Camellia」(開発コード名)を共同で開発しました。

高度化する情報流通社会における企業情報や個人情報の機密性を保証する暗号化方式として、安全性と様々なプラットフォームでの効率性・実用性を両立させた次世代共通鍵暗号アルゴリズムの開発が、現在必須の状況にあります。

Camelliaと名づけられたこの新しい暗号アルゴリズムは、１２８ビットブロック長(*2)の共通鍵暗号で、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と、三菱電機が世界に誇る小型／高速ハードウェア処理に適した暗号設計のノウハウ、並びに両社が持つ世界最高水準の暗号安全性評価技術を結集して設計開発されました。

Camelliaは、今後２０年以上の利用に対しても十分な安全性を有することはもちろんのこと、ソフトウェアだけでなく専用ハードウェアによる実装においても十分な小型化と高速化が実現できるように設計されました。このため、様々なプラットフォームでの効率性・実用性において世界最高レベルの性能を有しています。

<開発の背景>

インターネットの普及に伴い、プライバシー保護が重要な課題となっており、これにともない暗号技術の必要性も増しております。特に、エレクトロニックコマース等の商用分野において、従来よりも安全性が高く様々なプラットフォームでの効率性・実用性を両立させた暗号技術が求められています。米国ではＤＥＳ(*3)に代わる新しい連邦政府標準暗号ＡＥＳ(*4)の制定が

進められており、また欧州でも標準暗号開発の動きが始まるなど、次世代共通鍵暗号の世界標準化の動きが活発になってきました。さらに日本においても２００３年に開始が予定されている「電子政府」構想において、次世代共通鍵暗号の利用は必須と考えられます。

　そこで、この分野で世界トップレベルの研究者を擁している両社はお互いの得意とする暗号技術を持ち寄り、安全でしかもソフトウェア実装にもハードウェア実装にも適した共通鍵暗号アルゴリズムCamelliaを共同で開発しました。Camelliaは、ＡＥＳと同様に、１２８ビットのブロック長を採用しており、鍵長(*5)も１２８、１９２、２５６ビットの３種類をサポートしています。また実用性の面では、インターネットや様々な応用分野で広く使われる３２ビットプロセッサ上でのソフトウェア実装とともに、専用ハードウェアを使った暗号機器への組込みや、ICカードに組み込まれた８ビットプロセッサへの適用も考慮されており、極めて柔軟な実装が行なえるように設計されています。

　Camelliaの性能をＡＥＳ最終候補暗号(*6)と比べると、ソフトウェア実装では同等もしくはそれ以上の高速処理が可能です。さらにハードウェアでも同等もしくはそれ以上の高速実装が可能であることのみならず、世界最小クラスの小型化が実現できることが大きな特長です。

＜技術のポイント＞

（１）次世代共通鍵ブロック暗号(*7)の標準インターフェイスを採用

　現在利用されているほとんどの共通鍵ブロック暗号は６４ビットを処理単位として暗号化を実現しています。しかし、今後これとともに、より安全性を高めた１２８ビットを処理単位とするブロック暗号が求められており、米国の新しい連邦政府標準暗号ＡＥＳも１２８ビットブロック暗号となっています。
　今回開発した暗号は、この次世代１２８ビットブロックインターフェイスを採用するとともに、鍵サイズも１２８ビットから２５６ビットまで幅広く対応できるよう設計されています。

（２）高度な安全性を実現

　最近、暗号の解読法研究は急速に進歩しており、例えば「差分解読法」や「線形解読法」(*8)といったきわめて強力な解読法に対する安全性の数値的評価は、新しい暗号を設計するうえで欠かせません。
　Camelliaは、両社がもつ暗号強度評価技術を結集して、その安全性を評価したもので、これらの解読法でも解読が事実上不可能であること

が確認されています。さらに「関連鍵攻撃」「丸め差分解読」や「スライド攻撃」といった最新の暗号解読技術に対しても、その安全性が十分であるよう設計されています。

（３）マルチプラットフォーム暗号を実現

情報セキュリティの適用分野の広がりとともに、さまざまな利用環境で実装可能な暗号方式が求められています。Camelliaは、マルチプラットフォーム暗号をめざし、ソフトウェアでもハードウェアでも十分な小型化と高速性が実現できるよう様々な工夫がされています。

例えば、Camelliaは置換表と論理演算という、プラットフォームによらず高速な基本要素だけから全体が構成されております（図１、２）。このことから、ＩＣカード等で用いられる８ビットＣＰＵからＰＣで広く用いられている３２ビットＣＰＵ、さらには６４ビットＣＰＵまで、実装プラットフォームに制約されることなく高速なソフトウェア実装が可能です。Pentium III（800MHz）ＰＣでは３００Mbits/sec以上の処理速度（アセンブリ言語）を有しており、ＤＥＳの２倍以上の処理速度です。

さらに、置換表はハードウェアで小型化が容易になるように設計されています。また鍵スケジュール部においては、データ暗号化部と共用可能な構造を採用し、また拡大鍵保持のためのメモリ量を削減しています（図３）。この結果、Camelliaは暗号化回路を１０Ｋgate程度で実現することができます。これは１２８ビットブロック暗号のハードウェアとしては世界最小クラスです。

＜今後の展開＞

両社は、Camelliaを[ＩＳＯ／ＪＴＣ１／ＳＣ２７(*9)]で現在進められている暗号標準化活動に対して提案し、世界標準暗号アルゴリズムを目指します。

＜用語解説＞

***1 共通鍵暗号**

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。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に多く使われている。

***2 ブロック長**

暗号化を行うデータのまとまりの長さ。ＤＥＳ暗号のブロック長は６４ビ

ットであるが、ＮＩＳＴ（米国商務省標準技術局）では安全性を高めるために次期標準暗号はブロック長を１２８ビットと規定している。

***3 ＤＥＳ**

データ暗号化規格（Data Encryption Standard）。１９７７年に米国商務省標準局（ＮＢＳ、現ＮＩＳＴ）が定めた共通鍵暗号の規格。現在も銀行間のデータの暗号化に用いられている。

***4 ＡＥＳ**

ＤＥＳ暗号に代わる共通鍵暗号として、ＮＩＳＴが２００１年頃の制定を目指している次世代の米国連邦政府標準暗号。

***5 鍵長**

利用できる鍵パターンの数を定めるもので、例えばＤＥＳでは、鍵長が実質５６ビットなので２の５６乗個の異なる鍵が利用できる。鍵長を長くすることによって、全数探索解読法に対する安全性を高めることができる。

***6 ＡＥＳ最終候補暗号**

現在、ＡＥＳの最終候補暗号として、ＭＡＲＳ（米）、ＲＣ６（米）、Rijndael（ベルギー）、Serpent（英、イスラエル、ノルウェー）、Twofish（米）の５つが残っている。

***7 ブロック暗号**

共通鍵暗号の一方式。共通鍵暗号はブロック暗号とストリーム暗号の２種類に分類される。ブロック暗号はデータを一定のまとまった長さごとに暗号化する方式。これに対し、ストリーム暗号はデータを１ビットずつ暗号化する方式。

***8 差分解読法、線形解読法**

ブロック暗号に対する強力な暗号解読法。平文と暗号文の組み合わせを使って暗号を解読する方法。全数探索法に比べ、より少ない計算量で暗号を解読できることがある。

***9 ＩＳＯ／ＪＴＣ１／ＳＣ２７**

ＩＳＯは国際標準化機関であり、その中のＪＴＣ１／ＳＣ２７は、暗号を含めた情報セキュリティの標準化を進める専門委員会。

別紙

・図１：Camelliaの暗号化プロセス(略図)

図２：Camelliaのラウンド関数と補助変換(略図)
図３：Camelliaのハードウェア構成(略図)

【本件お問い合わせ先】

ＮＴＴ情報流通基盤総合研究所
企画部 広報担当　倉嶋、佐野
Tel.0422-59-3650 Fax.0422-37-7461
e-mail：koho@mail.rdc.ntt.co.jp

三菱電機株式会社
広報部　増島
Tel.03-3218-2332 Fax.03-3218-2431
e-mail：Toshio.Masujima@hq.melco.co.jp