NEWS RELEASE

NTT

日本電信電話株式会社

２００１年４月１７日

# ネット社会のセキュリティ確保に向け暗号技術の基本特許を無償化

日本電信電話株式会社（NTT）は、国内外の標準化機関等に対し、NTT情報流通プラットフォーム研究所が開発した世界最先端の共通鍵暗号方式（*1）「Camellia」（三菱電機株式会社との共同開発）、公開鍵暗号方式（*2）「EPOC」及び「PSEC」、並びに電子署名方式（*3）「ESIGN」に関する基本特許を、Camellia、EPOC、PSEC、ESIGNそれぞれの実装のために利用する場合に限り、無償で提供（実施許諾）する旨、表明していくことを決定しました。

インターネット上での電子商取引が活発化する中、企業情報や個人情報を保護する安全な通信環境を求める声が高まっています。日本政府も「電子政府」の基盤構築に向けて2000年１月に「ハッカー対策等の基盤整備に係わる行動計画」、同年4月に「情報セキュリティ政策実行プログラム」を打ち出すなど、本格的に情報セキュリティ政策の実行に乗り出しました。

安全な通信環境を確保し、高度情報流通社会を支える基盤となる技術が暗号技術と電子認証技術です。最近では、経済のグローバル化に伴い、暗号通信や電子認証における国際的な相互接続性も重要になってきております。そのため、ここ数年、国内外の政府、標準化機関等において暗号方式や電子認証方式の評価・標準化作業が急ピッチで進められています。NTTからも、共通鍵暗号分野でCamellia（三菱電機株式会社と共同提案）、公開鍵暗号分野でEPOC及びPSEC、電子署名分野でESIGNを国内外の標準化機関等に提案しております。

このたび、上記4つの暗号・電子署名方式について、その基本特許を無償で実施許諾することを決定したのは、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です。最先端のNTT暗号・認証方式を国内外の様々な製品やサービスに広く利用していただくための環境を無償で提供することによって、世の中での暗号・電子認証技術の活用が一層促進され、新しい情報流通サービスを低コストで安全に利用できるようになると考えております。

これからの具体的な活動としては、サンプルプログラムのフリーウェア化や標準化活動への貢献等を通じて、今後の暗号応用研究や暗号技術を利用した新しい情報流通サービスの開発などにNTT暗号・電子認証方式を広く活用していただける環境を提供してまいります。また、これらの暗号・電子認証方式を用いた電子認証システムや電子マネーシステムなどの暗号アプリケーションシステムの開発も積極的に進めてまいります。

なお、今回の無償化の対象は、各暗号・電子認証方式の基本特許の実施許諾に限定したものであり、関連するNTTの実装ノウハウ及びそれに関する特許（Camelliaに関する三菱電機株式会社の実装ノウハウ及びそれに関する特許も含む）などは、無償実施許諾の範囲に含まれませんのでご了承ください。加えて、Camelliaに関する基本特許は三菱電機株式会社との共有ですが、今回の無償化は同社の了解済みです。

**＜特許を無償実施許諾する各暗号の特徴＞**

○Camellia

128ビットブロック長（*4）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、三菱電機株式会社が世界に誇る小型・高速ハードウェア実装に適した暗号設計のノウハウ、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では、次期米国政府標準暗号AES（*5）の候補として最終選定されたRijndaelと比較して、より高い安全性を実現しています。さらに、低コスト型ICカード（8ビットCPU）からPC（32ビットCPU）、サーバ系（64ビットCPU）まで実装環境に応じた高速なソフトウェア実装、並びに世界最小かつ最高クラス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も兼ね備えた暗号方式です。

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

○EPOC

ハッシュ関数（*6）の出力がランダムであるという仮定と素因数分解問題（*7）が解読困難であるという仮定のもとで暗号の安全性を厳密に証明することができ、かつ高い実用性を有した公開鍵暗号方式です。これに対して、公開鍵暗号の代表であるRSA暗号で使われている関数は安全性が厳密に証明されていません。

EPOCホームページ：　http://info.isl.ntt.co.jp/epoc/index-j.html
EPOCニュースリリース：http://www.ntt.co.jp/news/news98/9804/980416.html

○PSEC （Provably Secure Elliptic Curve encryption）

ハッシュ関数の出力がランダムであるという仮定と楕円離散対数問題（*7）が解読困難であるという仮定のもとで暗号の安全性を厳密に証明することがで

きる公開鍵暗号方式です。RSA暗号などと比較して、短い鍵長でも十分な安全性を確保できるため、より高速な実装が可能です。さらに、NTTが開発した高速化技法と組み合わせることで、さらなる高速処理が可能になります。

PSECホームページ： http://info.isl.ntt.co.jp/psec/index-j.html

PSECニュースリリース：http://www.ntt.co.jp/news/news99/9905/990524b.html

○ESIGN （Efficient digital SIGNature scheme）

2001年4月施行の「電子署名及び認証業務に関する法律（通称：電子署名法）」に基づく運用指針により、認証業務に利用可能な電子署名方式として認定された電子署名方式です。従来の電子署名方式と比べて処理時間の大幅な短縮を実現した方式であり、専用コプロセッサを装備していないICカードなどへの搭載も可能です。

ESIGNホームページ：http://info.isl.ntt.co.jp/esign/index-j.html

**＜暗号標準化動向＞**

現在、国内外で進められている主な暗号評価・標準化の動きを紹介します。

○ISO （ISO/IEC JTC1 SC27）

国際標準化機関ISOのJTC1 SC27は情報セキュリティ技術の標準化を進める専門委員会です。従来は、認証方式のみを標準化の対象としていましたが（ESIGNは1998年に採用済み）、2000年4月より暗号方式も標準化の対象とすることになりました。NTTからはCamellia（三菱電機株式会社と共同提案）、EPOC、PSECを提案しています。

○IEEE （IEEE P1363）

エレクトロニクス関連で世界最大の学会である米国電気電子学会IEEEでは、1996年より公開鍵暗号・認証方式の標準化を行っており、その標準規格がP1363です。2001年にはP1363aが決定される予定で、NTTからはEPOC、ESIGNを提案し、P1363aに採用されることが内定しています。

○暗号技術評価委員会 （旧通産省委託・事務局：情報処理振興事業協会）

2000年4月に通産省（現経済省）が策定した「情報セキュリティ政策実行プログラム～電子政府のセキュアな基盤構築に向けての通商産業省の貢献～」に基づいて、電子政府に利用可能な暗号・認証方式の性能等を技術的・専門的見地から評価を行う委員会です。NTTからはFEAL、Camellia、EPOC、PSEC、ESIGNを提案しています。

○NESSIE （New European Schemes for Signatures, Integrity, and Encryption）

2000年から3年間の予定で始まった欧州連合における暗号・認証技術評価プロジェクトです。NTTからはCamellia（三菱電機株式会社と共同提案）、EPOC、PSEC、ESIGNを提案しています。

○IETF （Internet Engineering Task Force）
　インターネットの国際標準化団体IETFでは、TLS （Transport Layer Security）で利用可能な暗号方式の標準化を進めています。NTTからはCamellia（三菱電機株式会社と共同提案）を提案しています。

**＜用語解説＞**

***1 共通鍵暗号**
　データの暗号化と復号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や携帯端末の認証などに多く使われている。 NTTが開発した共通鍵暗号に、64ビットブロック暗号FEAL （Fast data Encipherment ALgorithm、1987年）、128ビットブロック暗号Camellia （三菱電機株式会社との共同開発、2000年）がある。

***2 公開鍵暗号**
　1976年にW. DiffieとM. E. Hellmanが提唱した新しい暗号方式。暗号化と復号で異なる鍵を用いる暗号方式であり、暗号化鍵を公開できるため、不特定多数の人々が情報をやりとりするネットワーク上での暗号通信に適する。共通鍵暗号で利用する秘密鍵を共有するための鍵配送方式として利用されることもある。NTTが開発した公開鍵暗号に、EPOC （1998年）、PSEC （1999年）がある。

***3 電子署名**
　公開鍵暗号において復号が復号鍵を有する本人にしかできないことを応用して個人の認証を行う方式。ディジタル署名ともいう。NTTが開発した電子署名方式に、ESIGN （1991年）、楕円Okamoto-Schnorr署名（1999年）がある。

***4 ブロック長**
　暗号化を行う入力データ処理長。かつての米国政府標準暗号であったDESのブロック長は64ビットだったが、NIST（米国商務省標準技術局）は、安全性を高めるために、次期米国政府標準暗号（AES）のブロック長を128ビットと規定した。

***5 AES (Advanced Encryption Standard)**
　次期米国政府標準暗号。世界中から公募された暗号の中から、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つが最終候補暗号として残り、2000年10月にRijndaelをAESの候補として最終選定した。現在、Rijndaelの情報処理連邦標準規格FIPS （Federal Information Processing Standards）への規格化を推進中である。

***6 ハッシュ関数**

任意の長さのメッセージを一定の長さのメッセージに圧縮する関数。

***7 素因数分解問題、（楕円）離散対数問題**

現在までに効率的な計算方法が見つかっていない数学分野における未解決問題。現時点では、問題のサイズ（暗号学的には鍵長と同義）が大きくなると、スーパーコンピュータを用いても解を求めることが難しいと考えられている。

【本件に関するお問合せ】
ＮＴＴ情報流通基盤総合研究所
企画部 広報担当 倉嶋、佐野、池田
TEL: 0422-59-3663
E-mail: koho@mail.rdc.ntt.co.jp

NTT NEWS RELEASE