NEWS RELEASE

NTT

日本電信電話株式会社

２００２年４月１６日

日本電信電話株式会社

ESIGNの安全性について

本日公表されたCRYPTREC（*1）2001・暗号技術検討会2001年度報告書で、弊社から提案したESIGN（*2）について、ある特定のパラメータの組合せで安全上の問題があると指摘されました。これはCRYPTRECに提案したESIGN仕様の具体的処理手順の記述誤りによるものでした。

そのため、弊社が出荷したESIGN製品の全てを調査したところ、指摘された問題が発生し得るパラメータ設定はされておらず、現在の製品をそのままご利用いただいても安全上の問題はないことを確認しました。

更に、上記のような特定のパラメータ設定を行った場合でも安全にご使用いただけるように対処を行った改訂版を、速やかにご提供すべく準備しております。この度は、お客様にご迷惑をおかけしましたことを深くお詫び申し上げます。

なお、ESIGNの基本アルゴリズムは、1985年に国際会議で提案して以来15年以上に渡って広く安全性が検証され、1998年にはISO/IEC 14888-3でも標準化されており、安全性の問題はありません。

今後は再発の防止策を講じるとともに、更なる製品の品質向上に努めていく所存です。

＜用語解説＞

***1 CRYPTREC**
電子政府で利用可能な暗号技術を、安全性および実装性など技術的な面から評価するプロジェクト

***2 ESIGN**
NTTが1985年にアルゴリズムを開発し、1991年に製品化した公開鍵暗号方式に基づくディジタル署名方式

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

NTT NEWS RELEASE