公開の状況等に関する情報

日本電信電話株式会社
平成 12 年 7 月 14 日

公開鍵暗号「PSEC 暗号」（PSEC-1, PSEC-2, PSEC-3 の３つのバージョンがある）の仕様等は以下のように公開されております。

1. PSEC-1 および PSEC-2 は以下のような形で公開されております。

（１） PSEC-1 および PSEC-2 は以下のような形で公開されております。岡本、藤崎、内山： 安全性の証明のついた公開鍵暗号：EPOC および PSEC、NTT R&D、日本電信電話株式会社、電気通信協会、Vol. 48, No.10, pp. 740--749 （1999 年 10 月）。

（２） 岡本、藤崎、内山、森田： 公開鍵暗号「EPOC」および「PSEC」、電子情報通信学会技術研究報告、 Vol.100, No.76, ISEC2000-9, 2000 年 5 月 25 日, 電子情報通信学会 (ISSN 0913-5685).

（３） http://info.isl.ntt.co.jp/psec/
NTT が開設している上記 PSEC ホームページより、概要説明、仕様、テストベクタ、サンプルコード等がダウンロード可能になっています。

２．PSEC-3 は、以下のような形で公開されて（する予定で）おります。

（１） Okamoto, T. and Pointcheval, D.: PSEC-3: Provably Secure Elliptic Curve Encryption Scheme (Version 3), submission to P1363a, http://grouper.ieee.org/groups/1363/P1363a/submissions.html (2000)

（２） 岡本他： EPOC-3 および PSEC-3, 電子情報通信学会技術研究報告、ISEC-2000、, 電子情報通信学会（2000 年９月発表予定）.

従って、暗号技術 公募要領「4.2 評価応募のために必要な情報の提出」の(2)～(6)のいずれの情報も、提供情報の非居住者への提供等に際して輸出管理上許可が不要であると考えます。