ChaosWare Inc.

プレスリリース

平成 22 年 3 月 12 日 19 時(UTC+9:00 時)

乱数性評価ソフト「RanSure」のクラスター計算・グリッド計算化による高速化に成功。
―高速化された「RanSure」によるクラウド型乱数性評価の受託・認証サービスを開始―

株式会社カオスウェア(代表取締役社長　梅野健)は、自社開発し、2005 年より販売開始されている乱数性評価ソフト「RanSure」の分散処理化(OS:Linux)に成功し，実時間(5CPU で30分)で 1Gbit の乱数性評価を行える様になりました。それにより、大規模乱数性評価を行える様になり、その結果については、本日の統計数理研究所「物理乱数・擬似乱数の　発生法・検定法とその周辺」(http://mid.ism.ac.jp/stats/msg01051.html)での発表，及び3月８日の筑波大学で行われた”日本応用数理学会応用カオス研究部会”(http://www.chaosware.com/appliedchaos/)のオーガナイズドセッションにより発表されました。 標準暗号とされている eStream 暗号、KASUMI 暗号、AES，仕様の公開されている暗号、購入可能であった物理乱数等を評価し、本「RanSure」の100回以上の大規模回数評価の乱数性が3つの階層(レベル)に明瞭にクラス分け可能であることが判明し、ある種の標準暗号(RC4(SSL)， MT， SOSEMANUK(eStream)，KASUMI 暗号(3G 携帯電話で利用。W-CDMA の携帯端末から基地局までの電波の暗号化で利用))については、100回中5割未満の合格率であり、最高レベルの乱数性を持たないことが判明されました。 (詳細資料:http://www.chaosware.com/pdf/20100312_ransure_press.pdf)。

これらの結果は、情報通信の基盤となる暗号の評価に関わるもので重要であり、更なる大規模乱数性評価(クラウド型乱数性評価)を進めるとともに、当社としては、新しく「RanSure」のソフトウェアパッケージの販売だけでなく、「RanSure」の 1Gbit 単位の評価の受託・受託乱数データの「RanSure 乱数認証サービス」(乱数性評価受託と認証サービス合計で1セット10万円(4営業日以内で100回の1Gbit 検定、消費税別)を開始します。

今後の展開:

今後、標準暗号、ライブラリーが公開されている擬似乱数系、仕様が公開されている暗号系・擬似乱数系の「RanSure」による評価結果をツイッター(TM) (http://www.twitter.jp/)でリアルタイムに公表(100回の「RanSure」評価当りに一度の公開。累計の評価結果もいたします。ツイッターアカウントは @ransure_ です。又、RanSure の評価の委託方法は、暗号便私書箱の RanSure のページ(https://www.angobin.jp/pb/com/chaosware/ransure/)から安全に 1Gbit 以上の大容量ランダムビット列が受託元である当社に送信できます。

連絡先:

株式会社カオスウェア　梅野健
〒184-8795　東京都小金井市貫井北 4-2-1
TEL:042-359-6299　　FAX:042-359-6339
E-mail:info@chaosware.com
http://www.chaosware.com