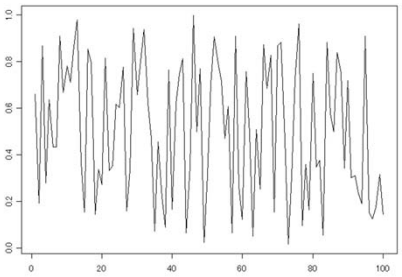
物理乱数と安全・安心社会

田村　義保　　データ科学研究系　教授

2010年1月、3月、7月に新しい物理乱数発生ボードを3種類導入した。

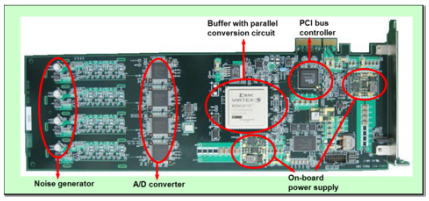
・統計科学スーパーコンピュータシステムに導入したボード

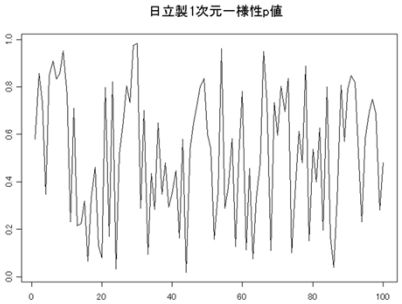
- **乱数源にツェナーダイオードを使用**
  - ・ツェナーダイオードの雪崩降伏現象により発生するノイズを利用する事で コストを軽減
- **乱数源とデジタル回路を分離**
  - ・乱数源（アナログ）をデジタル（FPGA）とは別のユニットにし、電源回路も分ける事で、デジタルノイズの影響を軽減
  - ・シールドケースで外来ノイズの影響を軽減
  - ・乱数源をユニット化しているため、乱数源のみ別途開発して交換が可能
- **400MB/sの速度で乱数を発生**
  - ・乱数源を4ch(+4ch)実装、100MspsでAD変換する事で、400MB/sを実現
  - ・大容量高速FPGAを使用
- **PCIeX＋2GByteのバッファメモリ**
  - ・PCIeX×4レーンのインタフェースと、1GByte×2のバッファメモリにより 乱数データを高速で転送
- **FPGAにて柔軟な回路を構成**
  - ・01補正処理の有無、マトリックス回路の設定等をレジスタで設定が可能



・物理乱数発生システムに導入したボード

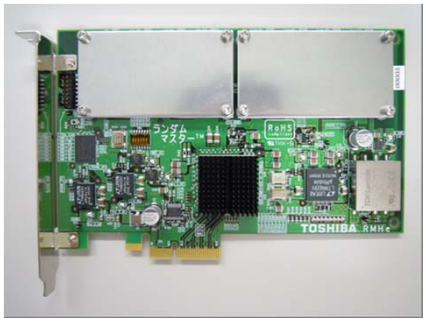
- **乱数発生ノイズ源**
  - ・白色ノイズ（熱雑音）
- **デジタル化法**
  - ・ADコンバータ
- **発生速度**
  - ・200MB/sを実現
- **インタフェース**
  - ・PCIeX×4レーン（Gen2）
- **一様化方法**
  - ・積算反転方式

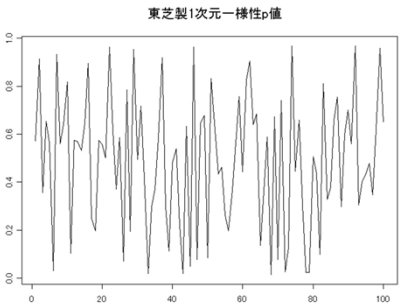




・物理乱数サーバーシステムに導入したボード

- **乱数発生ノイズ源**
  - ・ダイオードのノイズ
- **デジタル化法**
  - ・ADコンバータ
- **発生速度**
  - ・640MB/sを実現
- **インタフェース**
  - ・PCIeX（Gen1）
- **一様化方法**
  - ・ADCの下位2ビットを利用。排他的論理和による補正





物理乱数を用いた安全・安心社会の実現：乱数は暗号、シミュレーション、ID番号発行のため等に用いられます。数式を用いて作成される擬似乱数があります。擬似乱数は真の乱数ではありませんので、シミュレーションで間違った結果を出すこともあります。また、発生方式がばれると、ID番号を捏造することも可能になります。安心・安全な社会実現のためには物理乱数を用いる必要があります。ここで紹介している物理乱数の開発には統数研も関係しています。3番目のボードが現時点の世界最高性能のボードです。

物理乱数と放射線：初代の物理乱数発生装置は放射線式でした。「放射能」、「放射線」という言葉は、もう聞きたくないと思われている方も多いように思います。図は、6月上旬の東京都の5地点の空間放射線量です。単位はμSV/hです。地点により、日により違っていることが、分かります。東京都の過去の平常値は0.028から0.079μSv/hと発表されています。文京区は超えていて危ないと思われるかもしれません。示したデータで一番大きな0.17μSv/hを一年分に直すには24倍してから365倍すればよいということは容易に理解できると思います。約1.5mSv/Yearとなります。日本の過去の年間平均0.43mSvよりは、大きな値ですが、過去の最高値1.26mSv程度です。年間平均で5mSvを超えるような地点も世界にはあります。東京の数値は安心してもよい数値だと思います。原発関係の大量のデータを整理し、詳細な分析を行いつつあります。詳細は11月9日のセミナーで発表します。