

事業目的

あなたが使っている“乱数” — それは本当に信頼できる『予測不能性』ですか？

暗号鍵・認証・署名の信頼は『予測不能な乱数 = エントロピー』に依存します。

一方で実システム上では、初回起動時のエントロピー不足、仮想環境の複製、エントロピー源の停止などにより、弱鍵、状態重複、待ち時間やタイムアウト、停止の問題が生じ得ます。

クオルガは、東京高専との共同研究で培った磁性体の迷図磁区を利用する磁気光学物理エントロピー源とソニーの先端半導体技術との融合により、評価・監視・監査可能なQRU(Quantified Randomness Unit)の開発を目指します。ソプリクラウド／データセンターの暗号基盤、鍵管理システム、規制デジタル資産におけるPQC移行を見据えたQRUの導入を目指し、日本の産業の発展に貢献してまいります。

事業内容

本事業では、2026年度中の評価用テスト提供、および2028年度の製品テスト販売を見据え以下の4つのテーマに取り組めます。

- ①磁性体(エントロピー素材)の製造プロセス条件出し
- ②乱数生成モジュールの小型化開発
- ③高速生成可能な乱数生成システムの開発(最終出力層で3Gbps以上・設計目標)
- ④ NIST SP800-22の全項目検定クリア

事業成果

- 技術：①磁性体の製造プロセス条件出し完了。②研究初期の大型原理検証システムサイズ約600mmに対し、約40mm(サイズ比1/10以下)の乱数生成コアモジュールへの小型化原理検証を完了。
- システム開発：③FPGAデプロイによる出力速度:3Gbps以上の処理速を達成、システムアーキテクチャ確立。エントロピー源から乱数生成・評価までを一体で実演できる可搬型デモシステムを開発。
- 品質：④NIST SP800-22の全項目検定クリア。
今後は、NIST SP 800-90Bに基づくESV証明書取得に向けたMVP製品開発やデータ整備、鍵管理システム・重要インフラなどのパートナー候補とのPoCを進めます。

事業者情報

クオルガ株式会社
(東京高専 発 ソニースピンアウト スタートアップ)



代表取締役
CEO

赤木 真



技術顧問
(東京高専准教授)

水戸 慎一郎



■所在地:

東京都千代田区大手町1丁目6番1号
大手町ビル6階 Inspired.Lab

■設立年：2025年2月6日

■HP：<https://qorga55.com/> “QRU”は、クオルガ株式会社の登録商標です

概要図等

