量子強化型秘密鍵が「強固な暗号」を実現する

「hack now, decrypt later」のリスクが懸念されている。hack now＝今ネットワーク上にある大量の暗号化されたデータを収集し、decrypt later＝将来高性能な量子コンピュータが実用化されてからその暗号を解読する、という手法だ。

この攻撃手法は、現在すでに実行されていると考えられている。近い将来の量子コンピュータ社会が抱える新たなサイバーセキュリティのリスクに、今から備えておく必要がある。

強力な対抗策が存在する。量子コンピュータによるリスクへの対抗策もまた、量子コンピュータだ。量子力学を活用して「真に予測不可能な乱数」から生成した量子強化型秘密鍵が実現され、商用サービスとしての提供が開始されている。量子コンピュータが作り出す「強固な暗号」の最新技術と、社会インフラ化に向けた企業の取り組みをレポートする。

（渡辺 元・本誌編集長）

『月刊ニューメディア』2023年4月号掲載記事

「Quantum Origin」の技術

強固な「量子強化型秘密鍵」は完全に予測不可能な乱数から生成される

量子力学を活用することで、「真に予測不可能な乱数」から生成した量子強化型秘密鍵を実現できる。世界最大手の量子コンピュータ＆ソフトウェアプロバイダであるクオンティニュアム社（本社：英国・米国）は、すでに商用サービスとして量子技術を使ったサービスの提供を開始し、企業などでの導入が広がっている。同社の暗号鍵生成プラットフォーム「Quantum Origin」はどのように量子強化型秘密鍵を生成し、その品質を担保しているのかを解説する。

（取材・文：渡辺 元・本誌編集長）

クオンティニュアム株式会社 サイバーセキュリティ ソリューション アーキテクト 小林 聡氏

クオンティニュアム株式会社 Senior Enterprise Sales Executive 春田篤志氏

暗号鍵の脆弱性をもたらす擬似乱数

暗号通信に対する攻撃手法としては、❶暗号アルゴリズムを他のアルゴリズムによって破る、❷暗号鍵を管理しているハードウェアやソフトウェアから暗号鍵を盗み出す、❸暗号鍵の生成に使われた乱数の脆弱性を悪用する、といった方法がある。この中で見落とされがちなのが、❸への対策だ。

暗号鍵は乱数を基に生成されているが、この乱数がランダムではなく偏りがあると、暗号鍵を予測されてしまう。暗号鍵の安全性において、基になっている乱数のランダム性は非常に重要なファクターだ。「従来の暗号鍵用の乱数生成には、ハードウェアやソフトウェアの乱数生成器が使われていますが、そこでは決定論に基づいた乱数生成が行われています。乱数生成器のデバイスの偏りによって乱数の偏りが生じるため、そこから生成した暗号鍵の情報を解析することで、理論的には他の暗号鍵を予測することが可能です」（クオンティニュアム株式会社 サイバーセキュリティ ソリューション アーキテクト 小林 聡氏）。このような従来の乱数生成システムは真に予測不可能ではない乱数を生成するため、ハードウェアベースの真性乱数生成器（TRNG）を含め、厳密な分類では擬似乱数生成器（PRNG）に属するということができる。

これに対して、量子力学の特性を活用して予測不可能な乱数を生成する量子乱数生成（QRNG）の技術がある。よく使われているのは、レーザー光をビームスプリッターに通す方式で、理論上1/2の確率で光子が透過と反射に分かれることを利用して乱数を生成する。「しかし、ビームスプリッターの個体差によって乱数が偏ります。生成した乱数を事後的に検証すると、統計的な偏りから完全なランダムではないことがわかります」（小林氏）。安全な暗号鍵を生成するためには、使用する乱数が真に予測不可能な真性乱数であることを暗号鍵生成前に事前検証し、真に予測不可能な乱数のみを暗号鍵生成に使用するということが必要だ。

量子力学による真性乱数生成と検証

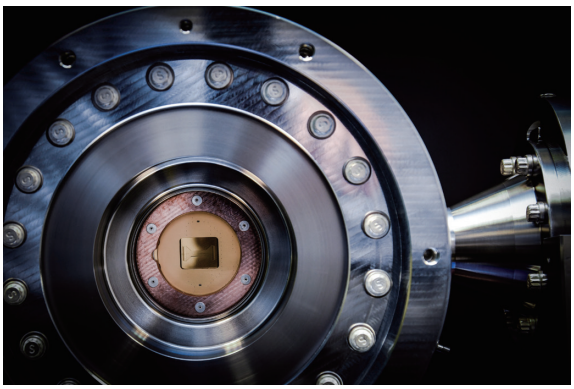
この真に予測不可能で、なおかつそれを事前に検証可能な乱数を生成するサービスがすでに提供されている。クオンティニュアムの暗号鍵生成プラットフォーム「Quantum Origin」だ。同社製のイオントラップ型量子コンピュータ「H-Series」を使用して真に予測不可能な量子強化型秘密鍵を生成するサービスで、SaaSとしてクラウドで提供されている。量子由来の乱数を生成するという点では前述の光子を使った乱数生成器と共通しているが、「乱数を生成する量子コンピュータの量子状態がランダムになっているか、具体的には量子もつれ（量子エンタングルメント）が起きているかを確認して、その上で乱数を生成します。予測不可能性を数学的に証明した乱数を基にすることによって、強固な暗号鍵を生成できるのです」（小林氏）。

乱数を生成する量子コンピュータの量子ビットが量子もつれの状態になっているかは、量子力学に基づくベルテス

トによって測定できる。ベルテストは複数の量子の量子状態を測定し、「ベルの不等式の破れ」を確認できれば量子もつれの状態になっていることを検証できる（**図**）。ベルの不等式の破れに関する研究は、2022年のノーベル物理学賞を受賞したテーマだ。「ベルテストで量子状態のもつれの度合い、すなわエントロピーを計算できます。エントロピーが高い、すなわち情報量が多い・乱雑な部分だけを抽出して“乱数の種（Quantum Seed）”に使用することで、真に予測不可能な乱数を生成することができるわけです」（クオンティニュアム株式会社 Senior Enterprise Sales Executive 春田篤志氏）。量子もつれ状態の２量子を観測した結果は、「00」と「11」の確率が必ず 1/2 で、真にランダムとなる。「乱数生成器のデバイスの特性に依存しない完全に予測不可能な乱数の生成が、量子力学の根本原理に保証されています。このようなプロセスを経て得られた真性乱数をベースに、暗号鍵を生成します」（小林氏）。

量子・古典のハイブリッドで品質向上

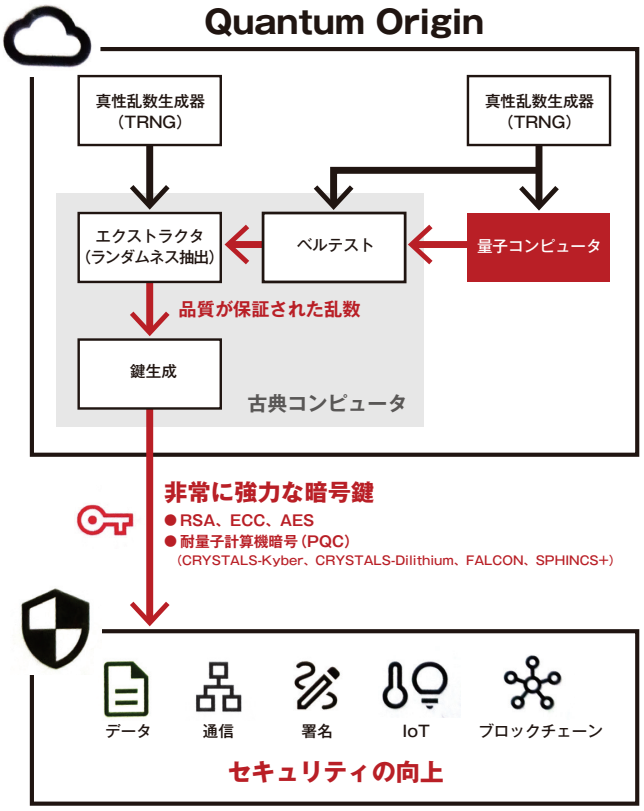
「Quantum Origin」の暗号鍵生成は、このような量子コンピュータ上での過程だけでは終わらないのも大きな特長だ。量子コンピュータでの過程をステップ１とすると、通常の従来型コンピュータ（古典コンピュータ）でのステップ２の過程を経ることによって、より高品質な暗号鍵を生成できる。前述のように量子コンピュータで生成した Quantum Seed と、古典コンピュータ上でのハードウェアが生成した乱数の双方を古典コンピュータ上のエクストラクタに入力し、関数によって再度乱数を生成する。そしてこの乱数から暗号鍵を生成するという仕組みになっている。「量子コンピュータによる量子由来の乱数生成と古典コンピュータによる乱数生成とのハイブリッドな仕組みによって、乱数の品質をさらに向上させています。このコンセプトは特許出願済みで、論文も発表しています。



クオンティニュアムのイオントラップ型量子コンピュータ「H-Series」

【図】 量子コンピュータによる乱数生成とランダム性の測定を組み合わせた量子強化型乱数生成

（出典：クオンティニュアムの資料）



『Quantum Origin』はブラックボックスではなく、そのロジックが公開されているのです」（小林氏）。「Quantum Origin」の数学的に検証可能な真性乱数列に基づく予測不可能な暗号鍵は、RSA や楕円曲線暗号（ECC）など既存の暗号アルゴリズムの秘密鍵だけでなく、耐量子計算機暗号（Post Quantum Cryptography / PQC）の秘密鍵を生成することも可能だ。

現在、「Quantum Origin」は企業での導入や、今後の導入を見据えた実証試験での使用が世界で拡大している。代表的なユースケースとしては、仏タレス社が暗号鍵を管理する HSM（Hardware Security Module）と「Quantum Origin」を統合させた。日本では、ソフトバンクグループのサイバートラストが自社の認証局と「Quantum Origin」と連携させた（34～36頁の記事に詳細を掲載）。富士通（英国）はSD-WANのセキュア化に活用するPoCを実施。そのほか、石油関連企業による拠点間通信の保護、ブロックチェーンや衛星通信のセキュア化などで、「Quantum Origin」が提供する量子強化型乱数とそれを基にした量子強化型秘密鍵が利用されている。

クオンティニュアムとサイバートラスト

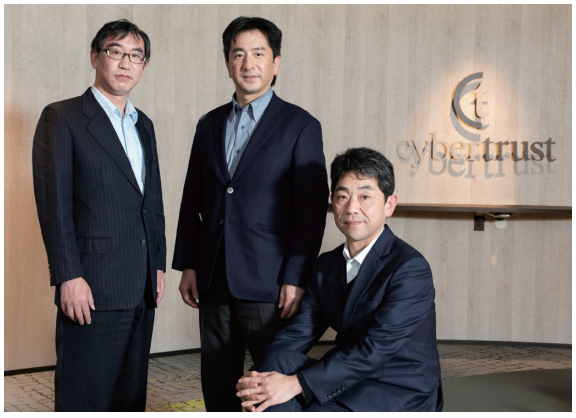
量子コンピュータ・IoT時代でも安全な量子強化型秘密鍵と電子証明書の提供で連携

サイバートラスト株式会社
R & D センター 執行役員
センター長 宿谷昌弘氏

クオンティニュアムとソフトバンクグループのサイバートラストは、サイバーセキュリティ分野での連携を2023年1月に発表した。クオンティニュアムが開発した量子強化型秘密鍵提供サービスと、サイバートラストの電子証明書提供サービスのシステム連携を実証。今後の量子コンピュータ時代、IoT時代の到来を見据えて、より安全な電子証明書提供サービスを実現できることを確認した。（取材・文：渡辺 元・本誌編集長、写真：広瀬まり）

現状の暗号鍵は「不完全な乱数」から生成

サイバートラストは認証・セキュリティ、Linux/OSS、IoTが事業の3本柱。認証・セキュリティ事業では、Webサイトの SSL/TLS 電子証明書の提供や、マイナンバーカードに格納されている公的個人認証の電子証明書を使った本人確認などのサービスを提供している。今回の協業によって、量子コンピュータが普及した社会の到来に向けて、より強固な暗号鍵とそれを活用した電子証明書を提供できるシステムを構築する。量子強化型秘密鍵と電子証明書を提供するサービスの連携は世界初。5G・6Gで端末が増大するIoT機器に対して、高速・大量により安全性の高い暗号鍵と電子証明書を配付するサービスの実現を目指す。



右から、サイバートラスト株式会社 R & D センター 執行役員 センター長 宿谷昌弘氏、クオンティニュアム株式会社 Senior Enterprise Sales Executive 春田篤志氏、同社 サイバーセキュリティ ソリューション アーキテクト 小林 聡氏

クオンティニュアムとサイバートラストが協業したのは既存の暗号技術は将来的に量子コンピュータによって破られる可能性が高いからだ。サイバートラスト株式会社 R & D センター 執行役員 センター長 宿谷昌弘氏は、「量子コンピュータにはたくさんのメリットがありますが、一方で既存の暗号が解読されるリスクも高まります。そこに向けた準備に今から取り組んでいくことが必要です」と述べる。例えば、現在広く利用されている RSA 暗号や楕円曲線暗号（ECC）は、量子コンピュータが進歩すれば破られると考えられている。クオンティニュアム株式会社 Senior Enterprise Sales Executive 春田篤志氏は、このリスクについてこう指摘する。「すでに現在、RSA-2048 を量子コンピュータで解こうという研究が世界で盛んに行われています。理論的には、『ショアのアルゴリズム』を使えば多項式時間で素因数分解が可能です。それを実現する性能を備えた量子コンピュータが開発されるのは、まだまだ時間がかかることになると思います。ただ、2022年末に中国の研究チームが発表した論文では、量子近似最適化アルゴリズムのコンセプトを活用することで、数百量子ビットの量子コンピュータでも素因数分解を効率的に行えると述べています。それに対して反論するレビューもあり、今すぐの脅威にはならないと考えられますが、将来的に量子コンピュータが RSA を破る可能性は高いという状況です」。

暗号鍵を生成する基になる乱数も量子コンピュータに解析されるリスクがある。暗号鍵の基になっている乱数にはソフトウェアベースの擬似乱数とハードウェアベースの真性乱数がある。前者の擬似乱数には周期性や偏りがあり、これらが暗号鍵の脆弱性につながる可能性がある。また、後者の真性乱数でも物理現象に由来するバイアスを完全には排除できない。「現在使われている擬似乱数も、過去何十年にもわたる研究の蓄積と利用実績があり、今すぐ脆弱性があるとは言われていません。しかし将来、量子コンピュータの飛躍的な計算力で解析すると、周期性や統計的な偏りの傾向などから暗号鍵を予測し、破られるリスクが出てくる可能性も考えられます」（宿谷氏）。

現在、「hack now, decrypt later」のリスクが指摘されている。今ネットワーク上を流れている大量の暗号化されたデータを収集し、将来高性能な量子コンピュータが実用化された後にその暗号を解読する、という手法が懸念されているのだ。「現在すぐには解読できなくても、送受信者間での

秘匿データを集めておく『hack now, decrypt later』の攻撃は、現在すでに起こっていると言われています」（春田氏）。

破れない量子強化型秘密鍵と電子証明書を提供

これらのリスクに対処する方法が主に３つある。❶鍵長を長くすること。❷量子コンピュータでも解析が困難なアルゴリズムを使った耐量子計算機暗号（PQC）へ移行すること。PQCについては、NIST（米国立標準技術研究所）が2022年７月に４種類のアルゴリズムを技術標準として選定し、移行を促している。そして、❸量子由来の乱数で暗号鍵を生成すること。偏りのない真性乱数の生成は非常に困難だが、量子コンピュータを使えば生成できる。クオンティニュアムの独自技術で作られた乱数は、RSAやECCなど既存の暗号にもPQCにも利用可能だ。

サイバートラストとクオンティニュアムの協業は、❷PQCと❸量子強化型秘密鍵で量子コンピュータによるリスクに対応していく。具体的な協業の内容は、クオンティニュアムが暗号鍵生成プラットフォーム「Quantum Origin」を使って、PQC・RSAおよびECCの量子強化型秘密鍵を生成し、サイバートラストの「新認証基盤」に安全な通信で提供。「新認証基盤」はサイバートラストがIoT時代に向けて開発した電子証明書提供サービスだが、「Quantum Origin」が生成したPQC・RSA・ECCの暗号鍵とそれに対応した電子証明書をパッケージ化して利用者に提供するというものだ（**図**）。

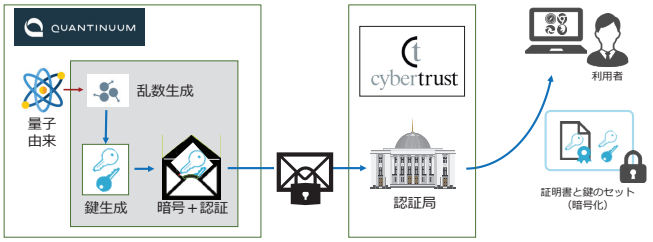
「Quantum Origin」による量子強化型秘密鍵の生成には、クオンティニュアムが開発した量子コンピュータが使われている。そして量子力学に基づく測定方法であるベルテストによって量子ビットの量子状態の相関を測定し、「ベルの不等式の破れ」を確認することで量子ビットが量子もつれの状態で乱数を生成したことを実証する。これによって、真に予測不可能であることを数学的に検証することができる乱数、ならびにそれを基にした暗号鍵生成を提供している。

「Quantum Origin」もサイバートラストの認証基盤も、すでに商用サービスとして実績がある。今回の協業では、両社の技術やサービスを連携させ、暗号鍵を量子強化型にした上で、電子証明書と組み合わせて、従来より高速・大量に提供できるシステムに強化する。「クオンティニュアムの技術を活用して生成した乱数は品質が高く、そこから生成された暗号鍵は予測困難なことが特長です。さらにその予測不可能性がロジカルに証明されていることから、システム固有のバイアスも排除され、何よりそれらを第三者も確認可能だということになります。信頼の拠り所となる秘密鍵が、何かよくわからないブラックボックスの中で作られて信じて使うしかない、ということではなく、透明性が確保されていると言え、非常に優位性があると感じています」（宿谷氏）。

サイバートラストの認証基盤は元々、電子証明書発行だけでなく暗号鍵生成の機能も持っているが、今回の協業では「Quantum Origin」が生成したPQCとRSA・ECCの暗号鍵の提供を安全な回線を通して受ける。そのため両社のシステム間の連携を実証試験で確認した。

【図】「Quantum Origin」とサイバートラストの新認証基盤の連携による量子強化型秘密鍵と電子証明書の提供

（出典：サイバートラストの資料）



IoT機器への高速・大量配付能力も確認

さらに実証試験では、これからのIoT時代に向けて暗号鍵と電子証明書を大量のIoT機器に高速配付できることも確認した。IoT機器に対する暗号鍵と電子証明書の配付では、インターネット上の無数のIoT機器や製造工場などでの大量の機器への対応が求められる。そのためサイバートラストの新認証基盤は、最小構成でも同社の従来比250倍の高速の電子証明書発行機能を実現し、並列化などにより数億台以上のIoT機器への大量提供の機能を新しく備えた。「安全性の担保やプライバシー保護のために、短期間だけ有効な電子証明書をどんどん更新していく考え方もあります。例えばコネクテッドカーに関連し、５分などの短時間の電子証明書を利用するといったイメージで、より高速・大量に電子証明書を発行する必要性が見込まれます。今回の実証では、『Quantum Origin』に多重にコネクションを張り並列して暗号鍵を要求するといったことも試していますが、コンスタントに暗号鍵が提供されました。現行のミニマムな環境でも１日に100万件というオーダーでの鍵生成にも難なく対応できるでしょう。IoT機器向けの高速・大量配付について十分な目途が立ちました」（宿谷氏）。両社が連携したシステムを使えば、自動車やスマートメーター、家電機器、スマートシティ用の環境センサーなどに高速・大量に暗号鍵と電子証明書を配付できるだけでなく、IoT機器側でもセキュアなメモリ領域に書き込むだけの構成も可能となる。

今後さらに高速・大量配付の向上が求められた場合にも対応できる。クオンティニュアム株式会社 サイバーセキュリティ ソリューション アーキテクト 小林 聡氏はシステムの拡張性に関して、「『Quantum Origin』は必要に応じて生成レートを向上させることが可能です。仮想マシンをベースにした構成になっているため、リニアにスケールできる能力を持っているのです」と説明する。今後も両社はシステムのスループットや性能の拡張に共同で取り組み、将来の6G時代のIoT機器向けサービスにも対応していく。

現在両社は、量子強化型秘密鍵と電子証明書の社会実装を拡大していくことに注力している。「今後のフェーズは、

ユースケースを増やし、お客様により幅広く使っていただくことです」（小林氏）。両社は製造業や医療、防衛など高度な安全性が求められる分野に対して今回の協業サービスの導入やPoCを提案しており、多数の企業などから導入に前向きな反応を得ている。導入やPoCの実施に向けたプロジェクトも複数進行中だ。量子強化型秘密鍵が安全な通信のデファクトとして活用される社会の実現に向け、両社は2023年から取り組みを強化していく。

世界最大級の量子コンピューティング企業 クオンティニュアムが顧客に選ばれる理由

ハードウェアからソフトウェアまで提供

クオンティニュアムは世界最大級の統合型量子コンピューティング企業。量子ソフトウェア事業を行う英Cambridge Quantumと、米Honeywellの量子コンピューティング部門で、量子ハードウェア事業を行う Honeywell Quantum Solutionsという、量子コンピューティング分野で世界を代表する2つの組織が2021年末に経営統合して設立された。本社は英国と米国で、その他ドイツと日本に拠点を構えグローバル展開をしている。

クオンティニュアム株式会社 経営企画 マネージャー 山中祐治氏

事業は、❶ハードウェア、❷ミドルウェア、❸ソフトウェア・アルゴリズム、❹共同研究の4レイヤーで幅広く展開。❶ハードウェアでは、イオントラップ型量子コンピュータ「H-Series」を開発・運用し、そのコンピューティングリソースを商用サービスとして提供している。H-Seriesの第一世代機であるH1-1は、量子ボリューム（IBMが導入した量子コンピュータの総合的な性能を示す指標）において業界最高レベルの8192※を実現している。なお、クオンティニュアムは2020年3月、今後5年間で量子ボリュームを毎年1桁ずつ向上させることをコミットしている。❷ミドルウェアでは、ゲート型量子コンピュータ向けソフトウェア開発キット（SDK）「TKET」をオープンソースとして研究者やデベロッパー向けに提供している。❸ソフトウェア・アルゴリズムでは、量子技術を活用した暗号鍵生成プラットフォーム「Quantum Origin」（詳細は32～33頁の記事）や、量子計算化学ソフトウェア「InQuanto」などを提供している。「InQuanto」は量子化学計算向けのさまざまな量子コンピューティングツールをひとつのアプリケーションとしてまとめたプラットフォーム。最新の量子アルゴリズムをさまざまなハードウェアやシミュレータ上で利用することができる。素材開発や創薬など、計算化学に携わる研究者を主な想定ユーザーとしている。

❹共同研究では、量子コンピューティングの応用に関するさまざまなプロジェクトを、クオンティニュアムのサイエンティストをはじめとするスタッフが顧客とチームを組んで実施する。❶～❸で述べたような技術力に加え、顧客のニーズや量子コンピューティングの習熟度などに応じた柔軟なプロジェクト設計が特長である。

クオンティニュアム グローバルCEO ラジーブ・ハズラ氏

クオンティニュアム グローバルCOO トニー・アトレイ氏

クオンティニュアム株式会社（日本法人）代表取締役 結解秀哉氏

科学者・技術者が顧客の課題を解決

クオンティニュアムの社員は現在全世界で約450名。量子コンピューティング専業の企業では世界最大級の社員数だ。しかも「その約8割をサイエンティストやエンジニアが占めているのが大きな特長になっています。量子コンピューティング分野はまだまだ進化途上。高度で複雑な技術的課題を解決し、顧客への価値提供に繋げていくためには、研究開発を推進するサイエンティストやエンジニアの役割が重要です」（クオンティニュアム株式会社 経営企画 マネージャー 山中祐治氏）。

また、同社がソフトとハードでこの分野を牽引する2つの組織が統合した企業であり、それぞれのサイエンティストやエンジニアが社内でコラボレーションできることも強みになっている。

日本法人もサイエンティストや理化学系出身者の比率が高い。「日本法人所属のサイエンティストが複数いることに加え、営業スタッフもPh.D.取得者が中心です。量子コンピューティングの専門家が顧客と日本語で円滑にコミュニケーションできます」（山中氏）。

クオンティニュアムとコラボレーションを行う企業が世界で拡大している。海外の顧客はスイスの製薬大手Rocheや独自動車大手BMWなど、大手企業が多い。

日本国内では、日本製鉄やJSRなどが共同研究を実施。研究テーマは組合せ最適化や計算化学などさまざまで、生産スケジュールの最適化、鉄の結晶のシミュレーション、半導体材料のモデル化などに取り組んでいる。サイバーセキュリティ分野での導入やPoCでも複数の企業とプロジェクトが進行中。2023年はクオンティニュアムとのコラボレーションを行う日本企業の事例が拡大しそうだ。（**取材・文：渡辺 元・本誌編集長**）

※ 記事掲載時の数値。その後、2023年2月23日に量子ボリューム32,768への更新を発表した。

量子乱数生成

統計的解析でも予測不可能な量子乱数が軍事、金融、エネルギー企業で導入へ

現在、世界で量子コンピュータの開発競争が繰り広げられている。従来のコンピュータの性能をはるかに上回る量子コンピュータのテクノロジーはさまざまな応用分野で期待されているが、その中でも他の応用分野に先行して本格的な商用サービスが始まったのが、量子コンピュータの代表的メーカーの一つである英米 Quantinuum（クオンティニュアム）社が提供している量子乱数だ。量子コンピュータが生成した量子乱数は外部からの予測が不可能であり、軍事、金融、エネルギー関連といった極めて堅牢な暗号鍵が必要な分野で利用検討が進められている。（取材・構成：渡辺 元・本誌編集長）

小林 聡
クオンティニュアム株式会社
サイバーセキュリティ ソリューション
アーキテクト

現代の暗号を支える乱数
量子乱数生成器も入手可能に

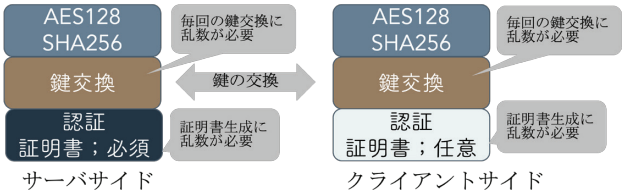
現代の暗号において乱数は非常に重要な役割を担っており、その品質が暗号強度を左右すると言っても過言ではない。例えば、TLS（古くは SSL）として知られる通信手段は、複数の暗号方式を使用するハイブリッドな方式だが、それらの暗号鍵はすべて乱数から生成されている（**図 1**）。一言で言えば、乱数の生成は文字通りランダムでなくてはならず、外部からの予測が極めて困難（不可能）であることが要求される。

乱数の生成手法は大きく分けて２種類ある。ソフトウェアベースのものと、ハードウェアベースのものである。前者は常に同一の処理しかできないため、厳密な意味での乱数を作り出すことができない。しかし、高度なアルゴリズムを駆使することにより、一般的な用途には耐えうる程度の乱数を生成することが可能となっている。このため、前者は擬似乱数生成器と呼ばれている。一方で、後者は従来から使用されているノイズなどの物理現象を利用して乱数生成を行うものであり、こちらは（擬似乱数と区別するため）真性乱数生成器と呼ばれている。加えて昨今では、量子由来の乱数を利用する量子乱数生成器も一般に入手できるようになってきている。

従来の乱数は統計的解析で予測可能
量子技術で予測が困難な乱数を生成

真性乱数生成器の場合、そのアルゴリズムが非公開とされることが一般的であり、製造者が悪意のあるコード（乱数に見えるが実際にはアルゴリズムを知る者が予測可能な数列を生成している）を実装し得ることが脅威となる。別の問題点として挙げられるのが乱数の検定に関わるものである。乱数が本当にランダムかの判断は事後でしか行うことができず、デバイスが不完全に故障した場合などには、偏りのある乱数が生成されながらもこれに気がつかないで使用してしまう脅威がある。また、攻撃側の手法として、該当のハードウェアを大量に購入し、個体差バイアスに起因する偏りを統計的手法で計測する、物理的な解析を伴うアルゴリズムの推測などが存在

【図 1】 TLS での暗号手法と乱数



『月刊ニューメディア』2023年１月号掲載記事

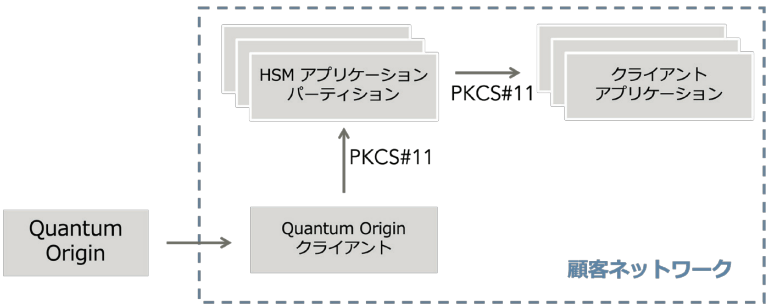
する。そのため、こうした脅威にも対抗しうる乱数の生成手段が必要とされている。

量子の特異な性質の一つに「重ね合わせ」というものがある。これはコインで言えば、表と裏とが同時に存在する状態である。実際には、この状態を観測することで、表か裏かが決定することとなる。この現象をベースにした乱数生成が可能であり、量子技術が一般用途で使用されている分野の一つとなっている。

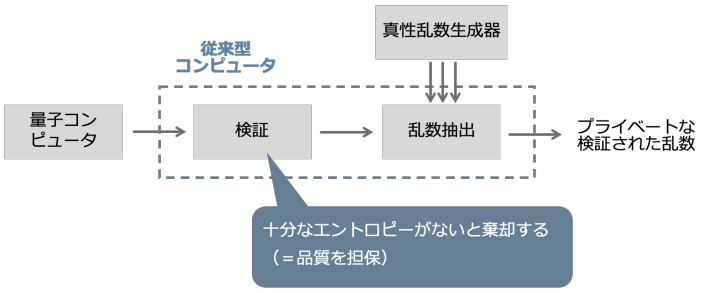
「量子もつれ」を利用することで「デバイス独立性」のある乱数生成へ

現段階ではコスト的な問題もあり、量子乱数は軍事、金融、エネルギー関連といった、セキュリティに対してのコストに寛容な業界での利用検討が進められている状況である。こうした分野では、既存の仕組みとしてHSM（Hardware Security Module）が導入されていることが一般的であるため、これら機器とのインテグレーションを行うことでユーザから見て透過的に利用できる点もメリットとなる（**図2**）。

【図2】 HSMと量子乱数生成サービス（Quantum Origin）とのインテグレーション例



【図3】 デバイスに極力依存せずに乱数を生成する手法



現状、複数のベンダーから量子乱数生成デバイスを購入することが可能である。しかし、そうしたデバイスは量子テクノロジーを使用してはいるものの、個体差バイアスを完全には排除できていないのが現状だ。これらの問題点は「デバイス依存性」と呼ばれ、より厳密な意味での乱数生成においてはこれを排除した「デバイス独立性」が求められている。多くの量子乱数生成デバイスは、乱数の品質という点では事後でしか確認できないということで、既存の真性乱数生成器と同等と考えることもできる。

一方で、量子乱数生成の別手法として「量子もつれ」を使用することも可能である。この利点は、「量子もつれ」は物理的な手法で計測することが可能である点だ。これを応用することで、従来では不可能であった生成中の乱数の品質確認が実現できる（**図3**）。逆に言えば、ここまで踏みこむことで初めて量子乱数生成を利用する明確な理由が生じるのではないかと考えている。暗号分野の研究者は現在、この「デバイス独立性」について活発な議論を行っている最中である。