Legal Wire

pillsbury

Japan Practice

Vol. 195 / May 2025

量子コンピューティングの時代に備えて
― 暗号技術の将来のゆくえと、企業が検討すべき課題

アンドリュー・L・キャプラン、ミア・レンダー、スコット・モートン、サム・レノ

- 量子コンピューティングは、サイバーセキュリティに重大な変革を引き起こすことになりますが、企業の幹部や法務担当者はこれを看過することはできません。

- 現代のデジタル社会において、暗号技術はセキュリティの基盤であり、メッセージの送信、パスワードの入力、オンライン取引をするたびに、データの秘匿性を保つために暗号化が使用されています。暗号化とは、情報を特定の鍵によってのみ復号可能な不可読の形式に変換するプロセスを指します。最も広く使用されている暗号方式には、対称暗号と非対称暗号の 2 種類があり、それぞれ異なる目的に応じて用いられています。

- 量子コンピューティングが理論段階から近い将来に現実化する中で、各国政府は、データセキュリティに対する重大なリスクに備え、積極的な対応を始めています。政策立案者は、将来的に量子技術が現在の暗号方式を無効化し、機密性および整合性（integrity）を脅かす可能性があることを認識しています。これを見越して、EU および米国などでは、量子コンピュータに対抗できる暗号技術への移行を支援するために、法的枠組みの策定、技術基準の設定、政策ガイダンスの発表といった取り組みが進められています。

量子コンピューティングとは一体何であり、なぜこれほどまでに暗号技術に対して深刻な脅威となるのでしょうか。そして、企業は今、何をすべきなのでしょうか。

量子コンピューティングとは

量子コンピューティングを理解するには、まず従来のコンピュータがどのように情報を処理しているのかを知ることが有用です。「古典」コンピュータは、ビット（binary digit）と呼ばれるデジタル情報の最小単位を用いて情報を処理します。ビットは、0 または 1 として表され、電源スイッチのオンまたはオフのように作動します。実際には、コンピュータの世界において「1」はトランジスタ（非常に小さな回路）がオン、すなわち電流が流れている状態を意味し、「0」はオフ、すなわち電流が流れていない状態を意味します。電子メールの送信、プログラムの実行、動画の再生といったすべてのコンピュータの作業は、最終的にはこのようなビットの長い列を一つひとつ処理することで実現されています。

一方、量子コンピュータは全く異なる仕組みで動作します。ビットの代わりに、量子ビット（キュービット）を用います。量子ビットは、「量子重ね合わせ（superposition）」と呼ばれる量子力学に

由来する不思議な現象により、同時に複数の状態をとることができます。つまり量子ビットは、単に 0 か 1 か（オフまたはオン）ではなく、両方の状態を同時にとることが可能です。量子重ね合わせとは、たとえばコインが回転している最中の状態のようなもので、表か裏かは観測するまで決まりません。この性質により、量子コンピュータは、従来のコンピュータのように一度に一つの結果を処理するのではなく、複数の可能性を同時に評価することができます。

量子コンピューティングのもう一つの重要な原理が、「量子もつれ（entanglement）」であり、これも量子力学の不思議な現象の一つであり、量子ビット同士が量子もつれの関係になると、物理的に広大な距離によって隔てられていても特別な結び付きが生じます。もつれた量子ビットの一方を測定することで、離れていても対の量子ビットの状態を即座に知ることができます。これは、あなたと親友が同じコインを持っており、どんなに離れていても、あなたが自分のコインを投げて結果を見れば、相手のコインがどうなったかがわかるようなものです。この仕組みにより、計算手順が大幅に短縮され、古典コンピュータよりも高速に問題を解くことが可能になります。

量子ビットの重ね合わせともつれにより、量子コンピュータは、古典コンピュータであれば数千年を要するような問題にも取り組むことができます。これは、量子コンピュータが膨大な数量の回答案を同時に探索し、古典的なシステムでは実現不可能な計算を行い、量子力学の量子干渉 (quantum interference) の概念を利用して最適な解答に焦点を当てることができるからです。技術はまだ初期段階にありますが、IBM や Google などの企業が著しい進展をもたらしており、実用的な量子コンピューティングが現実に近づきつつあります。この技術の進展に関して特に懸念されているのが、暗号技術への影響です。これは、今日のデジタル社会におけるデータセキュリティの基盤となっているものです。

現代の暗号技術の仕組み

現代のデジタル社会において、暗号技術はセキュリティの基盤です。メッセージの送信、パスワードの入力、オンライン取引のたびに、データの秘匿性を保つために暗号化が使用されています。暗号化とは、情報を特定の鍵によってのみ復号可能な不可読の形式に変換するプロセスを指します。最も広く使用されている暗号方式には、対称暗号と非対称暗号の 2 種類があり、それぞれ異なる目的に応じて用いられています。

対称暗号方式：効果的だが脆弱性あり

対称暗号方式は、データの暗号化と復号化に同一の秘密鍵を使用する方式です。この方法は非常に効率的であり、保存されたファイルの保護からインターネット接続の安全性確保に至るまで、幅広く使用されています。AES（Advanced Encryption Standard）などの代表的なアルゴリズムは、世界中の政府機関や企業によって広く信頼され、採用されています。ただし、対称暗号方式における主な課題は、秘密鍵を安全に当事者間で共有することです。万が一、ハッカー等に鍵を傍受された場合、保護されたすべての情報が容易に復号化されてしまいます。

非対称暗号方式：オンラインセキュリティの基盤

秘密鍵を共有する問題を解決するために開発されたのが、非対称暗号方式（公開鍵暗号方式）です。この方式では、単一の鍵ではなく、数学的に関連づけられた 2 つの鍵を使用します。1 つは誰でも使用可能な公開鍵で、データの暗号化に使用されます。もう 1 つは受信者のみが保持する秘密鍵で、暗号化されたデータの解読に使用されます。この仕組みは、HTTPS、電子メールの暗号化、電子署名など、インターネット通信を保護する多くのセキュリティプロトコルの基盤となっています。最も広く使用されている非対称鍵暗号アルゴリズムには、RSA（Rivest-Shamir-Adleman）暗号、楕円曲線暗号（Elliptic Curve Cryptography、ECC）、

およびディフィー・ヘルマン鍵交換（Diffie-Hellman key exchange）方式などがあります。これら 3 つの暗号方式は、オンラインセキュリティの基盤を成し、インターネット上で秘密鍵を共有せずに安全に通信することを可能にしています。

例えば、RSA 暗号は、大きな素数の因数分解が極めて困難であるという数学的な特性に依拠しています。非常に大きな 2 つの素数を掛け合わせることで得られる積は、算出自体は容易です。この積は公開され、暗号化に使用されますが、復号化に必要な情報である元となる素数は秘密にされます。この積のみを保有する者が、その積から元の素数を逆算することは、素数が大きければ非常に困難です。現在の計算能力では大きな素数の因数分解に数百万年を要するため、現時点では RSA は安全であると考えられています。

これらすべての暗号方式は、特定の数学的問題がコンピュータにとって現実的な時間内に解くことが事実上不可能であり、解読には数百万年から数十億年を要するという前提のもとに設計されています。これは、古典コンピュータには当てはまる前提であり、古典的コンピュータは「オン、オフ、オン、オフ」といったように直列的に計算を行う仕組みです。一方、量子コンピュータは、膨大な種類の計算を（直列的のみではなく）同時に実行することが可能であり、そのため、標準的な暗号方式に対する根本的な脅威となり得ます。研究者らは、実用的な大規模量子コンピュータが実現された際に、これらの暗号方式を破ることが可能となる量子アルゴリズムをすでに開発しています。1994 年に開発された米国数学者のピーター・ショアのアルゴリズムは、量子計算を用いて大きな数を効率的に素因数分解することができ、RSA 暗号を無力化する可能性があります。

現時点では、量子コンピュータはこれらのサイバー攻撃を大規模に実行するにはまだ十分な性能を有していませんが、量子ハードウェアの進展により、その実現は多くの人々が予想するよりも早く訪れる可能性があります。こうした中で懸念が高まっているのが、いわゆる「今保存し、後で解読する（store-now, decrypt-later）」という脅威です。これは、敵対者が現在の時点で暗号化されたデータを傍受および保存し、将来的に量子技術が利用可能になった段階でそれを解読しようとするシナリオを想定したものです。特に、長期間にわたる機密保持が求められる情報、例えば、センシティブな個人データ、企業の営業秘密、政府の機密情報などにとって重大な懸念事項となります。

量子技術による脅威への規制対応

量子コンピューティングが理論段階から現実的な技術へと進展する中で、各国政府は、データセキュリティに対する重大なリスクに備え、積極的な対応を開始しています。政策立案者は、量子技術が将来的に現行の暗号方式を無力化し、機密性および整合性を脅かす可能性があることを認識しています。これを見越して、EU や米国をはじめとする複数の法域では、量子コンピューティングに耐え得る暗号技術への移行を支援するために、法的枠組みの策定、技術基準の設定、政策ガイダンスの発表といった対応が進められています。

EU におけるポスト量子暗号に関する規制および政策の枠組み

EU は、暗号セキュリティを政策上の優先事項として位置付けており、ポスト量子暗号（Post-Quantum Cryptography、PQC）、すなわち耐量子コンピュータ暗号の開発および導入を促進するために必要な措置について検討を進めています。

現行の法的枠組み

EU では、現行の脅威および技術の進展を反映した強固なセキュリティ対策を講じることを求める複数の法令がすでに存在しています。例えば、一般データ保護規則（GDPR）は、個人デ

ータを保護するために、企業などが適切な技術的かつ組織的セキュリティ対策を講じることを義務づけています。「適切」とされる対策の内容は、最新技術の水準（すなわち、現在利用可能な最も先進的かつ効果的なセキュリティ手段）、実装コスト、対象となる個人データの性質、個人データがどれほどセンシティブな内容か、喪失した場合のリスクといった要因に基づき判断されます。

GDPR は量子技術について明示的には言及していないものの、技術的には中立で原則を重視するアプローチを採用しているため、量子コンピューティングが進展し従来の暗号方式が脅威にさらされる場合には、特にセンシティブであったり、高リスクの個人データを処理する組織において、PQC の導入がコンプライアンス維持のために求められる可能性があります。英国データ保護監督機関（The Information Commissioner's Office、ICO）は、2024 年に発表した「量子技術に関する文書（Quantum Technologies paper）」の中でこのアプローチを採用し、「組織は、個人情報に対する新たな進行中のサイバー脅威に対応するという既存の法的義務の一環として、量子リスクの特定と対応を検討すべきである」と述べています。

同様の最新技術の水準に基づくセキュリティ義務は、サイバーレジリエンスに焦点を当てた EU 法にも導入されています。例えば、重要産業に適用される NIS2 指令や、IoT 機器などを対象とするサイバーレジリエンス法が該当します。

EU の政策提言

EU は、拘束力のある法律に加えて、PQC への移行を促進するための戦略的な政策提言も示しています。特に、2024 年 4 月に欧州委員会は、EU 全体で PQC への移行を進めるため、加盟国間で調整された実施に向けたロードマップの策定を促す勧告を公表しました。この政策文書は、加盟国に対し、欧州のデジタル基盤が量子コンピューティングに耐性のある暗号に、円滑かつ同期的に移行できるよう、統一的な戦略の策定を求めています。

2024 年後半には、EU 加盟国間のサイバーセキュリティ政策を調整する NIS 協力グループの下に、PQC に関する専用の作業部会が設置されました。この部会はフランス、ドイツ、オランダが共同で会長を務め、各国の戦略を調和させることを目的としています。同年 12 月には、18 の EU 加盟国のサイバー機関が共同声明を発表し、「官公庁、重要インフラ事業者、IT プロバイダー、産業界全体」に対し、PQC への移行を最優先事項とするよう呼びかけました。この声明では、センシティブなデータを取り扱うシステムについては、暗号解析が可能になるような量子コンピュータ（cryptanalytically relevant quantum computers、CRQC）に対して事前に備える必要があると強調されており、量子技術の開発スケジュールに不確実性があることを理由に対応を遅らせるべきではないと述べられています。特に、「今保存し、後で解読する」リスクについては、可能な限り早期に、遅くとも 2030 年末までに対応すべきであるとされており、同じ期間内に公開鍵基盤システムの詳細な移行計画の策定も求められています。

さらに、欧州ネットワーク情報セキュリティ庁（European Union Agency for Cybersecurity、ENISA）は、EU の政策方針に基づき、既存のセキュリティプロトコルにポスト量子アルゴリズムを統合するための技術レポートを公表しています。これらの報告書では、暗号の柔軟で迅速な対応性を EU ネットワークの耐性を強化するための基本原則として重視しています。ENISA はまた、NIS2 指令が義務づけるサイバーセキュリティリスク管理措置に関する実装指針の草案を公表し、パブリックコメント（public consultation）を求めています。この草案では、量子耐性を有する暗号アルゴリズムの採用を含め、暗号機構の将来適合性を確保する必要性が特に強調されています。

今後に向けて、EU の政策枠組みでは進捗状況の継続的な評価が求められており、欧州委員会および ENISA は PQC への移行状況を監視し、量子技術による脅威の深刻化に対し移

行が十分に進まない場合には、勧告の更新や新たな規制の提案を行う可能性があります。EU 政策の全体的なメッセージは明確です。それは、今すぐに計画を立て、移行を開始すべきであるということです。EU は、政策提言の発表や専門家グループの設置を通じて、各加盟国政府および産業界に対し、量子コンピュータが本格化するのを待つのではなく、将来の混乱を回避するためにも、今から協調して暗号システムの更新に着手すべきであると強く示唆しています。

米国における PQC に関する規制および政策の枠組み

米国においても、量子コンピューティング時代に備えて、暗号標準に関するいくつかの基準、政策、規制および法律が制定されています。

1. 2022 年に発表された「国家安全保障覚書 10（National Security Memorandum 10）」では、米国の量子コンピューティングの将来について検討が行われ、量子コンピューティングに伴う暗号上のリスクを軽減する方策が提案しました。

2. 2022 年に制定された「量子コンピューティング・サイバーセキュリティ準備法（Quantum Computing Cybersecurity Preparedness Act）」は、連邦政府機関に対し、PQC への対応計画を策定することを義務づけています。同法は、政府機関に対し、法律の施行から 6 か月以内に量子コンピューティングによる攻撃に対して脆弱なシステムの目録を作成し、優先度を設定することを求めています。また、同法は、国立標準技術研究所（National Institute of Standards and Technology、NIST）が PQC 標準を公表した日から 1 年以内に、行政管理予算局（Office of Management and Budget 、OMB）が各機関の移行計画に関する指針を提示することを求めています。

3. NIST は、2024 年 8 月に 3 つの PQC 標準（FIPS 203、FIPS 204、FIPS 205）を正式に策定し、即時利用可能な状態としています。

4. 国家安全保障局（NSA）は、2022 年に「商用国家安全保障アルゴリズムスイート 2.0（Commercial National Security Algorithm Suite 2.0）」を公表し、国家安全保障システムにおける将来的な量子耐性アルゴリズムに関する要件を示しました。

5. 国土安全保障省（Department of Homeland Security、DHS）は、NIST と連携し、組織が量子コンピューティング技術の進展に伴うリスクを軽減し、データおよびシステムの保護を支援するためのロードマップを公表しました。

6. サイバーセキュリティ・インフラセキュリティ庁（Cybersecurity and Infrastructure Security Agency、CISA）は、2024 年 7 月に「PQC イニシアチブ（Post-Quantum Cryptography Initiative）」を設立し、量子コンピューティングがもたらす脅威への対応と、重要インフラおよび政府ネットワーク所有者の PQC への移行支援を目的とした取組を開始しています。

これらの取組は、量子コンピューティングが現在の暗号方式にもたらす潜在的な脅威に対して米国が備えること、政府機関および民間部門の双方において PQC への円滑な移行を支援することを目的としています。これらの政策および規制から組織が得るべき教訓は、量子技術による脅威の緩和は差し迫った現実であり、法務・技術・事業の各分野からの早期の対応が求められているということです。

量子技術による脅威に備えて：法務・技術・事業分野からの戦略的アプローチ

量子コンピューティングの進展に伴い、企業は、現行の暗号技術に対する脅威に対応するための多面的な戦略を講じる必要があります。これには、法的義務への対応、技術的ソリューションの導入、そして長期的なデータセキュリティの確保を支える事業慣行の見直しが含まれます。

法的観点

企業は、量子耐性セキュリティを求める新たな規制や業界標準の動向に注意を払う必要があります。量子コンピューティング技術の実用化が進む中で、各国政府および業界の標準化団体は、情報セキュリティに対する量子技術のリスクに対応するための法制度および標準の整備を継続して進めていくことになり、企業としても、規制環境が進化する中で、コンプライアンスを確保することが重要となります。

また、企業は、現行のデータ保護法の下でのデュー・デリジェンスを遂行すべきです。該当する規制は、特定の暗号技術を指定してこれの順守を義務付けるのではなく、データを保護する責任をデータ管理者に課しています。量子技術に起因する新たなリスクを踏まえ、企業は、ガバナンスルール、運用ポリシー、サプライヤーとの契約を見直し、進化するセキュリティ要件に先手を打って対応していく必要があります。これには、第三者が新たな暗号標準に準拠することを確保するために、ベンダーやクライアントとの契約を改訂することを含みます。暗号技術の更新を義務づけ、ステークホルダー間で責任を明確にし、いかに分担するかという法的枠組みを整備することで、企業は量子耐性セキュリティへの移行に向けてより効果的な準備を行うことができます。

事業手続

法的対応にとどまらず、企業はリスク管理および業務運営においても量子対応の準備を進めるべきです。最初の適切なステップとしては、リスク評価および暗号資産の棚卸を実施することが挙げられます。これにより、すべてのセンシティブな情報および暗号化されたシステムを特定し、量子技術による解読が可能となった場合に最もリスクの高い資産を評価することができます。特に、「今保存し、後で解読する」という脅威を考慮する必要があります。こうしたリスク評価を通じて、PQC への早期移行が必要な対象についての優先順位を適切に設定することが可能となります。

もう一つの重要な優先事項は、従業員のトレーニングです。IT 担当者、開発者、セキュリティチームに対して、量子リスクおよび新しい暗号技術に関する知識を提供し、更新を適切に反映できるようにすることが求められます。テクノロジーに関わるパートナーとの連携も、技術進展に乗り遅れないために重要な鍵となります。企業は、クラウドサービスプロバイダー、サイバーセキュリティ業者、業界コンソーシアムなどと密接に連携し、量子耐性ソリューションの試験導入や情報共有を行うべきです。こうしたパートナーシップは、量子セキュリティに必要な専門知識やツールへのアクセスを可能にします。量子技術による脅威を戦略的に企業リスクとして位置づけることで、企業はリソースを適切に配分し、インシデント対応計画を更新し、将来的に暗号標準が無力化される可能性を見据えた事業継続計画を策定することができます。

結論

デジタルセキュリティに依存するいかなる分野も、量子技術による脅威から免れることはできませんが、特にクラウドベースやデータに大きく依存する業種は、その影響を大きく受ける可能性があります。クラウドサービスプロバイダーはすでに対応を開始しており、Amazon Web Services

は、インフラに PQC を段階的に導入する計画を発表しています。この計画では、一部の保護機能が初期設定として提供され、必要に応じてより強固な量子耐性設定に顧客が移行できるようになっています。これと同様に、Google も自社ネットワーク内の内部通信を保護するためにポスト量子アルゴリズムの利用を開始しており、新たな暗号方式への信頼を示すとともに、自らデータ依存型企業にとっての事例を示しています。また、暗号技術に大きく依存している金融業界も動きを見せています。欧州刑事警察機構（Europol）が主催する Quantum Safe Financial Forum において、銀行に対して PQC への移行を最優先事項とするよう促す提言をし、「今保存し、後で解読する」ことへの攻撃によって、機密情報が危険にさらされる可能性があると警告しました。

こうした実際の対応事例は、量子技術対策がもはや理論的な話にとどまらないことを明確に示しています。先進的な企業はすでに、量子耐性のある施策を自社のビジネスモデル、プラットフォーム、顧客向けサービスに組み込む動きを始めています。これらの先行事例から学び、これに続く組織は、量子技術による混乱の中にあっても、信頼と事業継続性を維持する上で有利な立場に立つことができるでしょう。

本稿の原文（英文）につきましては、Why Your Organization Should Be Thinking About Quantum Computing and the Future of Encryption をご参照ください。

本稿の内容に関する連絡先

Andrew L. Caplan
andrew.caplan@pillsburylaw.com

Mia Rendar
mia.rendar@pillsburylaw.com

Scott Morton
scott.morton@pillsburylaw.com

Sam Reno
sam.reno@pillsburylaw.com

奈良房永（日本語版監修）
fusae.nara@pillsburylaw.com

東京オフィス連絡先

白井 勝己
katsumi.shirai@pillsburylaw.com

サイモン・バレット
simon.barrett@pillsburylaw.com

松下 オリビア（日本語対応可）
olivia.matsushita@pillsburylaw.com

ニューヨークオフィス連絡先

秋山 真也
shinya.akiyama@pillsburylaw.com

Legal Wire 配信に関するお問い合わせ

田中里美
satomi.tanaka@pillsburylaw.com