

2025 年 6 月 6 日

量子技術と日本法

創・佐藤法律事務所
弁護士 水嶋 優

近年、量子コンピューターをはじめとする「量子技術」が急速に注目を集めています。具体的には、従来の情報技術を超える高い演算能力や暗号技術の革新などが期待され、実用化に向けて国内外で様々な主体による開発が進んでいます。

一方で、既存の暗号が破られるリスクなど新たな課題も顕在化しつつあり、安全保障やサイバーセキュリティ、契約実務においても、量子技術への対応が問われる局面が増える想定されます。本記事では、量子技術の代表として量子コンピューターに焦点を当て、その概要と現時点での日本法上の主要な論点を整理します。

【筆者略歴】

2010 年に司法試験合格後、日本銀行にて勤務。システム部署においてシステムの調達やリスク管理を長く担当したほか、金融部署や国際関係部署などへの所属、海外 MBA(INSEAD)への留学経験を有する。創・佐藤法律事務所においては、Web3、フィンテック、その他スタートアップ法務や企業法務を取り扱っている。

量子技術に関しては、文部科学省の「光・量子飛躍フラッグシッププログラム」の助成を受けた人材育成プログラム(「Q-Quest」)に参加し、同プログラムのビジネスコンテストにおいて受賞経験がある。同プログラム終了後も量子ビジネスの立ち上げに向けた検討を進めており、ビジネスサイドから見た量子技術に関する知見も深めている。

I. 法律整理の纏め

1. 国家安全保障関連法制

■ 外為法

2024 年、2025 年の政省令改正で、量子コンピューター本体や関連品目が輸出・技術提供の許可対象に。現在進行形で規制が拡大しつつあり、メーカー等は規制対象について継続的な注意が必要。

■ 経済安全保障推進法

「量子情報科学」が「特定重要技術」に指定され、官民協議会や大型補助金を通じた研究開発支援の対象に。また、現時点で量子技術は「特許非公開制度」の対象外だが、将来指定の可能性も否定できない。

■ 重要経済安保情報保護活用法

2025 年 5 月施行。重要インフラ・重要物資サプライチェーン関連情報を保護・利活

用する仕組みを定める。これらに関連すれば、量子技術関連情報も「重要経済安保情報」として厳格管理の対象となりうる(ただし政府保有情報に限る)。

2. サイバーセキュリティ法制

- 現行法には量子技術や量子耐性暗号への直接言及はないものの、量子コンピューター普及による脅威が高まれば既存法に基づく対応が求められ得る。
- ガイドラインレベルでは動きが始まっており、2024 年 10 月には金融庁ガイドラインにおいて量子コンピューターへの留意が明記され、2025 年 5 月には大手銀行・地方銀行に量子耐性暗号への速やかな移行の要請が出されている。

3. 量子コンピューター利用に関する契約上の論点

- 量子計算固有の課題・特性について、古典コンピューターとは異なる責任範囲や免責条項(確率的結果、潜在エラー等)を契約で定めることが必要となる可能性。
- 実機の大規模・高額化を踏まえ、クラウド型量子コンピューティングによる利用が一般的な利用方法だが、品質保証(エラー率や稼働率等)については標準的な取扱いが未確立。各社は品質に関する様々な指標を公表している。

II. 量子コンピューターの概要

1. 基礎原理

量子コンピューターは、量子の「重ね合わせ」、「もつれ」、「量子トンネリング」といった特性を利用して計算を行います。これにより、特定の問題に関して従来型コンピューター(=「古典コンピューター」)よりも非常に高速な計算が期待されています。

【用語説明】

■ 重ね合わせ(Quantum Superposition)

古典コンピューターのビットは「0」か「1」の状態しか取れませんが、量子ビットは同時に「0」でもあり「1」でもある状態を作れます。例えばコインが回転している間は、まだ表とも裏とも決まっていないようなイメージです。この重ね合わせにより、量子コンピューターは1つの量子ビットで複数の計算パターンを並行処理でき、特定の課題で古典コンピューターより大幅に高速な演算を実現します。

■ もつれ(Quantum Entanglement)

複数の量子ビットが互いに状態を連携させたまま存在する現象です。たとえば2つの量子ビットがもつれた場合、一方を測定すると瞬時に、かつ距離に関係なく、もう一方の状態が確定します。この性質を利用して、ビット同士を結びつけて複雑な並列計算を行ったり安全性の高い量子暗号通信を実現できると期待されています。

■ トンネル効果(Quantum Tunneling)

古典物理で越えられないエネルギー障壁を、量子力学的な性質により「すり抜ける」現象

です。最適化問題では、谷間に挟まれた「山」を乗り越えるのではなくすり抜けることによって最適解へ到達しやすくなり、効率的な探索が可能になります。

量子コンピューターには大きく「量子ゲート方式」と「量子アニーリング方式」の 2 種類があります。

方式	基本原理・性質	主な用途	代表的な企業
量子ゲート方式	量子の「重ね合わせ」「もつれ」を利用し、複雑な問題を並行的に計算することで高速に処理	汎用的な量子アルゴリズムにより多用途（化学シミュレーションや機械学習など）に対応	Google(超電導)、Intel(半 導 体)、IonQ (イオントラップ)、PsiQuantum(光)、QuEra Computing (中性原子)
量子アニーリング方式	量子の「トンネル効果」を利用し、エネルギーの最も低い状態を探索	最適化問題(物流ルート最適化、ポートフォリオ最適化など)に特化	D-Wave Systems

量子ゲート方式は、汎用的な量子アルゴリズムを実行できる“汎用量子コンピューター”であり、超電導、半導体、イオントラップ、光、中性原子などさまざまな方式が研究されています。しかし、まだ主流となる技術は確立しておらず、実用化には誤り訂正などの課題があります。これに対して量子アニーリング方式は組み合わせ最適化問題に特化しており、D-Wave Systems が商用機を提供しています。一般に「量子コンピューター」という場合は量子ゲート方式を指すことが多いものの、用途や実装技術によって使い分けが生じています。

方式	量子ビットの仕組み	利点	課題	代表的な企業・研究機関・大学
超電導方式	超伝導回路にマイクロ波を流し、電流や磁束の2状態を量子ビット化	・ゲート操作※が高速 ・既存の半導体製造技術の応用が可能	・ノイズやエラーが起きやすい ・極低温(絶対零度近く)環境が必要	[海外] Google、IBM、Rigetti
				[日本] 富士通、NEC、理化学研究所、産業技術総合研究所
半導体方式	シリコンなどの半導体中の電子や	・CMOS 技術との互換性が高く、	・量子ビットの一貫性(コヒーレ	[海外] Intel、Equal1、D

	スピンの状態を利用	将来的に大規模集積化しやすい	ンス時間)が短く、制御が困難	iraq、UNSW シドニー大学
				[日本] 日立製作所、理化学研究所、産業技術総合研究所、blueqat
イオントラップ方式	真空中に浮かせたイオンをレーザーで操作し、内部状態を量子ビットにする	・コヒーレンス時間が長く、ゲートの精度が高い	・装置が大きくなりやすく、多くの量子ビットを並べるのが難しい	[海外] IonQ、Quantinuum、AQT、Oxford Ionics、Universal Quantum
				[日本] 理化学研究所、産業技術総合研究所、Qubitcore
光方式	光子の偏光や経路などの状態を量子ビットにする	・常温動作が可能 ・量子通信やネットワークとの親和性が高い	・大規模な集積やエラー訂正技術が発展途上 ・光子源・検出器が課題	[海外] PsiQuantum、Xanadu
				[日本] NTT、理化学研究所、東京大学、OptQC、
中性原子方式	レーザーで冷却・配列した中性原子の内部状態や配置を利用	・多数の量子ビットを比較的容易に並べられ、スケーラビリティが高い	・ゲート動作が遅め ・レーザー制御の精度が求められる	[海外] QuEra Computing、Pasqal、Infleqtion、Atom Computing
				[日本] 産業技術総合研究所、分子科学研究所、京都大学、Yaquumo

※ ゲート操作：量子ビットに一定の刺激(マイクロ波パルスやレーザーパルスなど)を与えて状態を変える基本動作で、古典コンピュータの論理ゲート(AND/OR/NOT など)に相当します。例えば、Xゲート(量子ビットの0と1を入れ替える)や、H(アダマ

ール)ゲート(量子ビットを重ね合わせ状態にする)といったゲートがあります。これらのゲート操作を高速かつ高精度に実行することが、量子ハード開発の鍵となります。

一方、量子アニーリング方式は「組み合わせ最適化」に特化しており、汎用演算はできませんが、実用化はゲート方式よりも進んでいます。カナダの D-Wave 社が商用機を提供するほか、古典コンピュータで疑似的に挙動を再現する「量子インスパイアード・アニーリング」(Fixstars Amplify AE、富士通 Digital Annealer など)も開発されています。

2. 量子コンピューターの現状

2025 年 1 月、NVIDIA の Jensen Huang CEO が「実用的な量子コンピューターの実現には 20 年程度かかる」と発言したことで米国の量子関連株が急落しました。これは主にゲート型量子コンピューターを指した見通しと考えられ、本記事作成時点(2025 年 5 月末)において、多くの専門家は実用化までにまだ相応の時間を要すると考えています。主な理由は、ゲート型で「重ね合わせ」や「もつれ」を維持する過程で発生するエラー(外部ノイズによるデコヒーレンス)が深刻であり、この解決には高度な「誤り訂正」技術が不可欠だからです。しかし、誤り訂正技術の確立にはまだ相応の期間が必要とされ、10~20 年という見方が出る背景となっています。

もっとも、量子ゲート方式の各種アプローチは世界中で研究開発が加速しており、日本でも大企業やスタートアップ、研究機関・大学が競って実機開発を進めています。また、量子アニーリング方式はすでに商用機が普及しており、オンラインで利用できる環境も整備済みです。このように、量子技術は“遠い未来の話”ではなく、現在進行形で社会実装が進んでいるテクノロジーと言えます。

3. 量子コンピューターの活用場面、既存技術に対するリスク

量子コンピューターの活用場面としては、例えば以下のような分野が見込まれています。

分野	利用場面の例
金融・経済	・ポートフォリオ最適化(膨大な組み合わせから最適配分を瞬時に算出) ・リスク評価や価格シミュレーションの高速化
物流・サプライチェーン	・車両ルートや倉庫配置の最適化 ・災害時やピーク需要時の最適な輸送・移動ルートの計画
エネルギー・スマートグリッド	・電力網の需給最適化 ・再エネ変動を考慮したリアルタイム制御
材料設計・創薬	・電池材料や医薬候補分子の性質を量子化学計算で高精度に予測

ヘルスケア・ゲノミクス	<ul style="list-style-type: none"> ・遺伝子配列解析の高速化 ・タンパク質構造の高精度予測
気象・気候シミュレーション	<ul style="list-style-type: none"> ・大気海洋モデルの高解像度計算 ・温室効果ガス削減策のシナリオ評価
機械学習・AI	<ul style="list-style-type: none"> ・小規模データでも高精度を狙う量子強化学習 ・生成 AI の学習高速化

上記のような分野において、古典コンピュータでは何年もかかる計算を短時間で処理できる「量子超越性」の実現が期待されています。しかし、量子超越性は必ずしもメリットだけでなく、既存技術へのリスクも伴います。代表例は暗号技術の脆弱化であり、量子によって従来の公開鍵暗号が解読される可能性が懸念されています。

暗号解読	<p>実用規模の量子コンピュータが登場すれば、RSA や楕円曲線暗号など現在広く使われている公開鍵暗号は短時間で解読され、インターネット通信や電子決済など社会のあらゆる場面で安全性が一気に揺らぐおそれがある。</p>
------	--

現在の暗号技術は、古典コンピュータでは解読が困難な数学的問題を前提にしていますが、量子コンピュータが実用化されると、「Shor のアルゴリズム」などを使って短時間で解読される可能性があります。これはビジネスや日常のあらゆる場面で使われる公開鍵暗号を危険にさらし、改ざん耐性を前提とするブロックチェーンにも影響を与えると考えられています。さらに、「Harvest Now, Decrypt Later 攻撃」と呼ばれる手口では、現時点でデータを傍受・保存し、将来量子コンピュータが実用化された段階でまとめて解読するリスクが指摘されています。

このため、量子コンピュータでも解読が難しい「量子耐性暗号(Post-Quantum Cryptography : PQC)」への移行が急務となっています。米国では国立標準技術研究所(NIST)が2024年8月に複数のPQCを標準化候補に選び、その後も検討を続けています。日本では暗号技術の評価やモニタリングを行う CRYPTREC(暗号技術評価委員会)が2025年3月末に「CRYPTREC 暗号技術ガイドライン(耐量子計算機暗号)2024 年度版」¹を公表し、各種 PQC の技術解説や評価、導入ガイダンスを示しています。暗号技術はあらゆるサービスの基盤であり、各事業者はこうした PQC の標準化動向を注視し、早めに準備を進める必要があります。

4. 量子技術に対する海外政府の動向

¹ <https://www.cryptrec.go.jp/report/cryptrec-gl-2007-2024.pdf>

海外では、主要国が量子技術に対して大規模な投資を行い、一部の国では法的インフラの整備にも注力しつつあります。日本もこれらの動向を注視しつつ、国際競争力の確保とサイバーセキュリティや安全保障といった課題との両立を図る必要があります。

国	動向
米国	2018年に「National Quantum Initiative Act(国家量子イニシアティブ法)」を成立させ、連邦政府が一体となって量子 R&D 推進と人材育成体制を構築。
EU	「Quantum Flagship」と呼ばれる 10 億ユーロ規模の大型プロジェクトを立ち上げ、量子コンピューターや量子通信の研究開発を主導。
中国	国家を挙げて量子通信や量子コンピューターの研究開発に多額の投資を行っており、特に軍事・安全保障分野での応用を重視。

III. 量子技術と日本法

日本では、本記事作成時点(2025 年 5 月末)では量子技術を対象とする専用法は存在しません。この点、他の先端技術分野の例をみると、ブロックチェーン(暗号資産等)については既に各種の規制が課されており、また AI では 2025 年 5 月に利活用とリスク抑制を目的とした「AI 関連技術の研究開発・活用推進法」が可決されています²³。量子技術についても、将来的に専用法が制定される可能性はありますが、現状は利用場面ごとに既存法令の適用可否を検討する必要があります。具体的には、①国家安全保障関連法が量子機器や技術の輸出管理や開発支援にどう関わるか、②サイバーセキュリティ法制が量子技術による既存暗号への影響をどのように扱うかを確認します。さらに、③量子サービスを提供・利用する際には、契約上の責任分担や免責、品質保証のあり方など、新たに検討すべき論点が生じます。これらについて、法的枠組みを概観します。

1. 量子技術と国家安全保障

(1) 量子技術による国家安全保障へのリスク

量子技術は既存暗号技術の無効化や傍受困難な通信などの点で安全保障に直結するため、米国や中国が国家規模で巨額投資を行っています。米国では経済競争力と国家安全保障の両方を維持・強化する目的から 2018 年に「National Quantum Initiative Act(国家量子イニシアティブ法)」を成立させ、大学・企業・研究機関の連携と大規模予算投入による量子 R&D 体制を構築しました。日本には量子専用の法律はありませんが、既存の安全保障関連法令(外為法、経済安全保障推進法、重要経済安保情報保護活用法)において先端量子分野が対象となり得ます。これら既存法令の枠組みで、量子計算や量子センサーの研究・開発

² <https://www.nikkei.com/article/DGXZQOUA270UW0X20C25A5000000/>

³ https://www.cao.go.jp/houan/pdf/217/217gaiyou_2.pdf

が安全保障面からどのように規制・支援されるか、検討します。

(2) 外為法

(i) 外為法の概要

外為法(「外国為替及び外国貿易法」)は、安全保障等の観点から、物品・技術の海外提供や外国からの投資を管理する法律です。具体的には、①輸出規制(海外流出防止)、②役務取引規制(無形技術の提供も含む)、③対内直接投資規制(外国資本による出資・買収時の事前届出)を定めています。

(ii) 量子技術に適用される外為法上の規制

量子技術はまさに物品・技術の海外流出リスクが懸念される分野の一つです。このため、2024 年 9 月の政省令改正により量子コンピューターが輸出管理の対象とされ、全地域への輸出に許可が必要とされています⁴。さらに、2025 年 5 月 28 日施行の改正で、実用規模の量子コンピューターに不可欠なキー技術・材料も同様に規制対象として追加されています⁵⁶。なお、これら輸出管理の対象となる量子コンピューター及び関連品目については、技術提供も同様に規制対象となります⁷。

規制対象(2025 年 5 月末時点)		仕向地
量子コンピューター		全地域
量子コンピューター 関連品目	極低温冷凍機 極低温アンプ 極低温ウェハープローバ 同位体分離シリコン／ゲルマニウム基板・原料	全地域

量子関連企業は、外為法による輸出・技術提供規制が現在進行形で拡大していることを踏まえ、自社の製品や技術が規制対象となるかどうかを常に確認できる体制を整える必要と考えられます。

⁴ 外為法第 48 条、輸出貿易管理令第 1 条・別表第 1 の 8、輸出貿易管理令別表第一及び外国為替令別表の規定に基づき貨物又は技術を定める省令第 7 条第 6 号

⁵ https://www.nikkei.com/nkd/industry/article/?DisplayType=1&n_m_code=036&ng=DGXZQOUA316FJ0R30C25A1000000

⁶ 外為法第 48 条、輸出貿易管理令第 1 条・別表第 1 の 7、輸出貿易管理令別表第一及び外国為替令別表の規定に基づき貨物又は技術を定める省令第 6 条 (https://www.meti.go.jp/policy/ampo/law_document/shourei/20250403_gaiyo.pdf、https://www.meti.go.jp/policy/ampo/law_document/20250328_ristshiryoku.pdf)

⁷ 外為法第 25 条、外国為替令第 17 条・別表の 7 及び 8、輸出貿易管理令別表第 1 の 7 及び 8、輸出貿易管理令別表第一及び外国為替令別表の規定に基づき貨物又は技術を定める省令第 6 条及び第 7 条第 6 号

(3) 経済安全保障推進法

(i) 経済安全保障推進法の概要

2022 年に成立した経済安全保障推進法(「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」)は、国内企業・研究機関の技術・物資を支え、経済面から国家安全保障を強化することを目的としています。具体的な仕組みとしては以下の 4 つを柱とし、直接規制ではなく⁸公的支援や情報共有を通じてリスクを低減します。

- ① 重要物資の安定的な供給の確保
- ② 基幹インフラ役務の安定的な提供の確保
- ③ 先端的な重要技術の開発支援
- ④ 特許出願の非公開制度

(ii) 量子技術との関係

第三の柱である先端技術支援では、「量子情報科学」が特定重要技術に指定され⁹、資金支援や官民連携を通じた伴走支援のための協議会設置、調査研究業務の委託などを通じた研究開発の促進・活用が図られます。

また、第四の柱である特許非公開制度では、安全保障上問題となる発明の公開保留や外国出願禁止等の措置が可能です。本記事作成時点(2025 年 5 月末)では、同制度の対象となる「特定技術分野」に量子コンピューターや量子暗号通信は指定されていません。しかし、法の趣旨からすれば今後指定される可能性も否定できず、開発者としては留意すべき制度と言えます。

(4) 重要経済安保情報保護活用法

(i) 重要経済安保情報保護活用法の概要

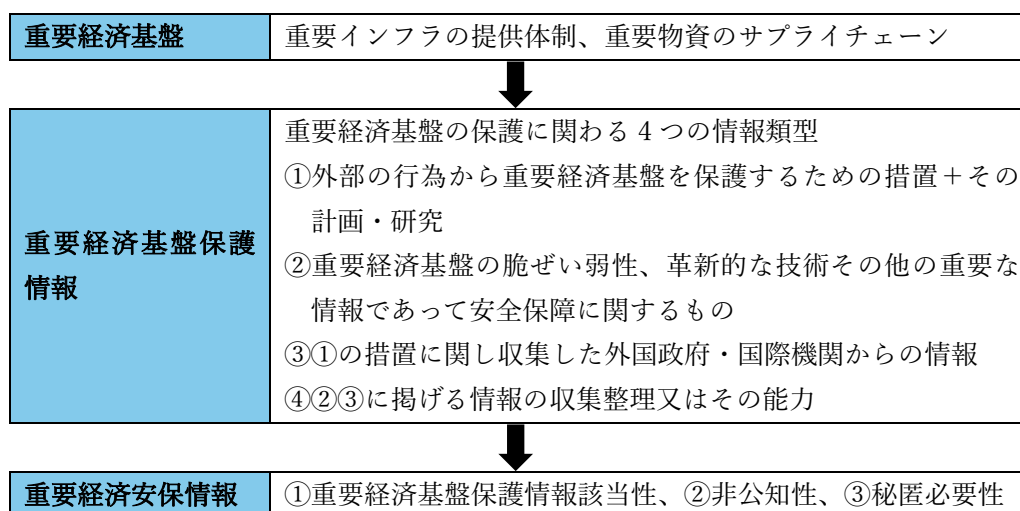
2025 年 5 月 16 日、「重要経済安保情報の保護及び活用に関する法律」が施行されました。従来、特定秘密保護法が防衛・外交・テロ・スパイ関連情報を対象にセキュリティ・クリアランス制度¹⁰を定めていましたが、本法はそれを経済安全保障の領域に拡張し、重要な経済基盤に関わる情報を保護・活用するための体制を整備することを目的としています。同法では、まず重要インフラの提供体制及び重要物資のサプライチェーンを「重要経済基

⁸ ただし②基幹インフラ役務の安定的な提供の確保については、電力・通信・物流など「特定重要設備」の導入・維持に際し、調達先や部品の事前審査が行われ、直接規制の対象となります。

⁹ https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/doc/kihonsishin3.pdf

¹⁰ 内閣府によれば、セキュリティ・クリアランス制度は「国家における情報保全措置の一環として、政府が保有する安全保障上重要な情報として指定された情報に対して、アクセスする必要がある者のうち、情報を漏らすおそれがないという信頼性を確認した者の中で取り扱うとする制度」と説明されています(https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/sankou_clearance.pdf)。

盤」として定めています(2 条 3 項)。そのうえで、重要経済基盤を保護するための措置、安全保障に関する重要経済基盤の脆弱性や革新的な技術等の情報など 4 つの類型を「重要経済基盤保護情報」と定義します(2 条 4 項)。そして、重要経済基盤保護情報に該当する情報のうち、非公知性及び秘匿必要性が満たされる情報について、政府が「重要経済安保情報」として指定する仕組みとなっています(3 条 1 項)。



同法は、指定された重要経済安保情報の「保護」と「活用」の両面を目的としています。具体的には、政府が持つ安全保障上重要な経済情報を適切に扱うために、重要経済安保情報に指定された情報について、情報提供が認められる事業者の要件や情報を取り扱う個人の適性評価方法などを定めています。なお、指定対象はあくまで政府保有情報に限られ、民間企業が独自に開発した技術情報が一方的に指定され、その取扱いに制約がかかるというものではありません。

(ii) 量子技術との関係

(i) で述べたように、重要経済安保情報保護活用法が対象とするのは重要経済基盤(重要インフラや重要物資サプライチェーン)の保護に関する 4 つの情報類型です。具体的には、インフラを外部脅威から守る対策や計画・研究、インフラの脆弱性や革新的技術など、安全保障に直結する情報が含まれます。なお、対象となるインフラや物資は、経済安全保障推進法や「重要インフラのサイバーセキュリティに係る行動計画」に定められたものを参照することとされており¹¹、電力・ガス・水道・通信・交通・物流・金融・化学・医療などのインフラ、半導体や先端電子部品などの重要物資が含まれます。

量子技術は、既存暗号を破るリスクをもたらす量子コンピューターや、安全性を高める量

¹¹ 重要経済安保情報保護活用法 18 条、「重要経済安保情報の指定及びその解除、適性評価の実施並びに適合事業者の認定に関し、統一的な運用を図るための基準」(4-5 ページ)。

子暗号通信など、上述の重要経済基盤の保護に関する情報に該当する可能性が高く、今後重要経済安保情報として指定される可能性は十二分に考えられます。もっとも、(i)で述べたことの繰り返しとなりますが、実際に重要経済安保情報に指定され得るのは政府保有情報だけであり、民間企業が自社開発した技術が一方的に指定されるわけではありません。

2. 暗号技術とサイバーセキュリティ法制

量子技術に関する日本法の論点としては、安全保障のほかに、サイバーセキュリティとの関係が考えられます。すなわち、II 3.で述べたように、量子コンピューターの発展により、従来の暗号技術が解読されるリスクが指摘されています。

(1) 法令レベル

日本ではサイバーセキュリティ基本法が国や事業者に対してセキュリティ確保の責務を課し、個人情報保護法が個人データの適切な管理を義務づけています。本記事作成時点(2025年5月末)では、これらの法令に量子技術や量子耐性暗号への具体的な言及はありません。ただし、量子コンピューターの普及で既存暗号が危殆化しセキュリティリスクが高まれば、条文上の明示がなくともこれらの法律に基づき必要な対策を講じることが求められる可能性はあります。

(2) ガイドラインレベル

これに対し、ガイドラインレベルでは既に量子技術への言及が始まっています。金融庁が金融機関向けに公表する「金融分野におけるサイバーセキュリティに関するガイドライン¹²⁾(2024年10月4日公表)では、脅威情報や脆弱性情報を収集・分析する際に「新技術(AI、量子コンピューター等)、地政学的動向、偽情報、業界動向などの組織を取り巻く状況に留意し情報収集を行うこと」が「対応が望ましい事項」として明記されました。

さらに、日本経済新聞(2025年5月14日付)¹³⁾によると、金融庁は大手銀行や地方銀行に対し、量子耐性暗号(PQC)へ移行するための準備を直ちに始めるよう要請しています。PQC対応にはシステム改修などで数年単位・多額のコストがかかるため、早急な対応を求めたものとみられます。

3. 量子コンピューター利用に関する契約上の論点

ユーザーが量子コンピューターを利用する場合、得られた量子計算結果に存在し得る誤りや揺れについて契約上どのように対応するべきか、という問題が浮上すると考えられます。こうした問題は、量子計算固有の課題・特性から生じ得るものです。

¹²⁾ <https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf>

¹³⁾ <https://www.nikkei.com/article/DGXZQOUB044OX0U5A400C2000000/>

(1) 量子計算固有の課題・特性(エラー、アルゴリズムレベルの確率性、演算結果検証の困難性)

前述したように、ゲート型量子コンピューターでは、演算中に発生するエラーが大きな課題となっています。加えて、量子アルゴリズムによっては繰り返し実行して統計的に最良解を抽出する性質があり、同じ入力から常に同じ出力が得られるとは限りません。量子アニーリング方式も、その原理の性質(確率的にエネルギーの低い解を探索する)やハードウェアのノイズ、熱雑音等により実行の度に解が異なる場合があります。また、量子超越性を伴う大規模計算は、古典コンピューターでの再現・検証が困難¹⁴なため、出力の正当性を完全には保証できません。

これらの理由から、量子計算の結果には誤りや揺れが残り、その後の予測やシミュレーションに影響を与えるリスクがあります。量子コンピューター利用サービスが増える中では、ハード(量子プロセッサ)、ソフト(アルゴリズム)、ユーザー回路・データの責任範囲を明確化し、結果が確率的であることや潜在的エラーを前提とした免責条項など、従来の IT 契約とは異なる条項の導入が必要となる可能性があります。

(2) クラウド型量子コンピューティングに関する契約上の留意点

量子ゲート方式・アニーリング方式いずれも実機は大規模・高額なため、当面はハードウェアベンダーが提供する機器をクラウド経由で利用するクラウド型量子コンピューティングが一般的な利用方法になると考えられます。

従来のクラウドでは SLA(Service Level Agreement)で一定の稼働率などが保証されますが、クラウド型量子コンピューティングの場合には、どのような品質保証(エラー率や稼働率等)を行うべきなのかが論点となり得ます。例として IBM Quantum Platform(量子ゲート型)、D-Wave Leap(量子アニーリング)、Amazon Braket(外部の複数の量子ゲート型・量子アニーリングを API で扱う)では、各社様々な指標(ゲート誤差率、コヒーレンス時間、ジョブ処理に要する時間など)を公表していますが、未だ標準的な考え方が確立していないと考えられます。

留保事項

- ・本書の内容は関係当局の確認を経たものではなく、法令上、合理的に考えられる議論を記載したものにすぎません。また、当職らの現状の考えに過ぎず、当職らの考えにも変更があります。

¹⁴ 検証方法として、対話型プロトコル(古典コンピューターを使う検証者が量子計算者に各種の質問をすることで、正しい量子計算が行われているかをある程度保証できる手法)やランダムサンプリングによる統計的検証(大規模な量子計算について測定結果の分布を古典コンピューターにより部分的にチェックし、一致度を確認する方法)などの手法があるが、大規模化への課題がある。

- ・本書はBlog用に纏めたものに過ぎません。具体的案件の法律アドバイスが必要な場合には各人の弁護士にご相談下さい。