（資料２）

政府機関等の耐量子計算機暗号（PQC）利用に関する検討の背景等について

１．背景

○　量子計算機（量子コンピューター）技術の進展に伴い、従来型の計算機に対して安全性を有している一部の暗号アルゴリズムについて、将来、その安全性の低下（危殆化）が懸念されている。

○　このため、各国においても、量子計算機に耐性を持つ耐量子計算機暗号（PQC）への移行に向けて検討が進められているところ。

＜参考１＞ 量子計算機（量子コンピューター）について

量子力学の現象を利用して並列計算を実現し、従来型の電子計算機では効率的に解けなかった問題の一部を効率よく解けると期待される次世代の計算機。

＜参考２＞ 耐量子計算機暗号（PQC）について

量子計算機および従来型の電子計算機の双方に対して安全性が確保される暗号。量子計算機でも解読が困難な数学的問題を利用することで、量子計算機による攻撃に耐性を持つ。

２．諸外国の状況

・米国　：　可能な限り 2035 年までに、耐量子計算機暗号（PQC）に移行する方針。また、2025 年 12 月までに、広く入手可能な耐量子計算機暗号（PQC）をサポートする製品のリストを公表。

・欧州　：　可能な限り 2035 年 12 月末までに耐量子計算機暗号（PQC）への移行するロードマップを公表。

・英国　：　2035 年までの耐量子計算機暗号（PQC）への移行に向けたタイムラインを公表。

３．国内における状況

○　政府機関等における耐量子計算機暗号（PQC）については、2025 年３月の暗号技術検討会（CRYPTREC）を受けて、技術的な安全性等の評価に向けた検討が開始されている。

○　耐量子計算機暗号（PQC）への移行については、サイバーセキュリティ確保のほか、産業政策、安全保障、サービスの安定供給、国際連携・標準化の観点等があり、広範囲の検討が必要と考えられる。

＜参考３＞ 暗号技術検討会（CRYPTREC）について

「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」を検討する専門家の会合。デジタル庁・総務省・経産省が共同で事務局を運営。