(資料１－１)

政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議の開催について

令和７年〇月〇日
関係府省庁申合せ案

１　量子計算機技術の進展に伴い、現在広く利用されている公開鍵暗号の安全性が著しく低下すると予想されており、耐量子計算機暗号（PQC）への移行は急を要する課題である。
　移行には、技術的課題のみならず、安全保障、産業政策、サービス安定供給、対応支援策、国際連携など多岐にわたる課題があるが、まずは、政府機関等における耐量子計算機暗号（PQC）利用に関し、関係府省庁の緊密な連携の下に必要な施策を検討・推進するため、政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議（以下「連絡会議」という。）を開催する。

２　連絡会議の構成は、次のとおりとする。ただし、議長は、必要があると認めるときは、関係者の出席を求めることができる。

議　長　内閣官房副長官補（内政担当）
副議長　内閣官房内閣審議官（国家安全保障局）
　　内閣官房内閣審議官（内閣サイバーセキュリティセンター）
主　査　デジタル庁統括官（デジタル社会共通機能担当）
　　総務省サイバーセキュリティ統括官
　　経済産業省商務情報政策局長
構成員　内閣官房内閣審議官（内閣官房副長官補付）
　　内閣府科学技術・イノベーション推進事務局統括官
　　警察庁長官官房技術総括審議官
　　デジタル庁統括官（戦略・組織担当）
　　外務省大臣官房サイバーセキュリティ・情報化参事官
　　文部科学省研究振興局長
　　経済産業省イノベーション・環境局長
　　防衛省大臣官房サイバーセキュリティ・情報化審議官

３　連絡会議の下に幹事会を開催する。幹事会の構成員は、関係行政機関の職員で議長の指定する官職にある者とする。

４　連絡会議及び幹事会の庶務は、関係行政機関の協力を得て、内閣官房において処理する。

５　前各項に定めるもののほか、連絡会議の運営に関する事項その他必要な事項は、議長が定める。

（資料１－２）

政府機関等における耐量子計算機暗号（PQC）利用に関する
関係府省庁連絡会議・連絡会議幹事会　運営要領（案）

政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議（以下「会議」という。）及び政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議幹事会（以下「幹事会」という。）の運営については、この運営要領の定めるところによるものとする。

１．会議及び幹事会は、非公開とする。

２．会議及び幹事会の議事要旨は、原則として公開する。ただし、議長が特に必要と認めるときは、その一部を非公開とすることができる。

３．会議及び幹事会で配布された資料は、原則として公開する。ただし、議長が特に必要と認めるときは、その一部を非公開とすることができる。

（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。

（資料３）

検討すべき論点（案）

１．量子計算機の開発・普及状況及びそれに伴い危殆化する公開鍵暗号等の特定とその時期について

２．諸外国の動向の把握について

３．耐量子計算機暗号（PQC）の安全性等の評価・確認とその時期について

４．耐量子計算機暗号（PQC）への移行期限及び危殆化した公開鍵暗号等の利用に係る停止の時期について

５．政府機関等の移行への対応に必要な支援策等について

６．政府機関等の移行に向けた工程表（ロードマップ）の策定について

７．その他

（資料４）

今後のスケジュール（案）

令和７年６月　　第１回関係府省庁連絡会議の開催

（議事内容）
- 連絡会議及び幹事会の設置
- 検討すべき論点の設定
- 今後のスケジュールの確認

令和７年７月
～１１月　連絡会議幹事会の開催（随時）

（議事内容）
- 工程表（ロードマップ）の骨子の検討

〈主な検討内容（例）〉
- 危殆化する公開鍵暗号の特定とその時期
- PQC の安全性等の評価・確認とその時期
- PQC への移行期限及び危殆化した公開鍵暗号の利用停止の時期
- 移行への対応に必要な支援策等

令和７年１１月頃　第２回関係府省庁連絡会議の開催

（議事内容（案））
- 工程表（ロードマップ）の骨子のとりまとめ

令和８年度中　　第３回関係府省庁連絡会議の開催

（議事内容（案））
- 工程表（ロードマップ）の策定について