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（第２回）議事要旨

１　日時

令和７年９月８日(月)14:00～15:30

２　場所

中央合同庁舎第４号館 1214 特別会議室

３　出席者

○議　長

西山　英将　　内閣官房内閣審議官（内閣官房副長官補付）

○副議長

髙橋　文武　　内閣官房内閣参事官（国家安全保障局）

杉本　貴之　　内閣官房内閣参事官（国家サイバー統括室）

○主　査

中川　拓哉　　デジタル庁統括官（デジタル社会共通機能担当）付参事官

梅城　崇師　　総務省サイバーセキュリティ統括官付企画官

橋本　勝国　　経済産業省商務情報政策局サイバーセキュリティ課企画官（代理出席）

○構成員

石谷　寧希　　内閣官房内閣参事官（内閣官房副長官補付）

白木　宏明　　内閣府科学技術・イノベーション推進事務局上席政策調査員（代理出席）

飯田　晋一　　警察庁長官官房技術企画課情報セキュリティ対策室長（代理出席）

増原　剛輝　　デジタル庁統括官（戦略・組織担当）付参事官

森田　光枝　　外務省大臣官房情報システム総括課長

田渕　敬一　　文部科学省研究振興局基礎・基盤研究課量子研究推進室長

黒田　隆之助　経済産業省イノベーション・環境局イノベーション政策課調整官（代理出席）

荒　心平　　防衛省整備計画局サイバー整備課長

○有識者等　※敬称略

北川勝浩（大阪大学 特任教授 量子情報・量子生命研究センター長）、

日本電気株式会社、三菱電機株式会社

４　議事要旨

○冒頭挨拶

西山議長から、連絡会議で定めた「検討すべき論点」に関し、より知見を深め

るため、今回、有識者等よりヒアリングを行う旨挨拶がなされた。

○議事

（1）有識者等からのヒアリング及び意見交換

有識者等から以下のとおり説明があった。

○北川大阪大学特任教授量子情報・量子生命研究センター長から、量子計算機の開発状況等について説明。

○日本電気株式会社から、PQC に対応した製品の開発状況等について説明。
（企業秘密の情報であるため、説明及び意見交換の内容は非公開。）

○三菱電機株式会社から、PQC に対応した製品の開発状況等について説明。
（企業秘密の情報であるため、説明及び意見交換の内容は非公開。）

次に、意見交換が行われ、以下のような発言があった。

○西山議長

・米国や欧州といった諸外国が 2035 年に PQC 移行を目指していることについて、量子技術の研究者の目からすると合理的な目標設定か。

○北川大阪大学特任教授量子情報・量子生命研究センター長

・2030 年ごろまでに RSA-2048 が解けることはまずないだろうと考えているが、世界的に活発化している誤り耐性型量子計算機の研究開発が順調に進んだ場合、2045 年ごろまでに解けてしまう可能性もある。ただ、意見が分かれるところであり、あくまで可能性という話ではある。

・一方で、暗号に関していうと、長期にわたって秘密を守らないといけない情報であれば、Harvest Now, Decrypt Later という考えで、例えば 10 年～20 年後に暗号を解読可能な量子計算機が実現したときに解く前提で既に情報収集がされているかもしれないという考え方の下で対応が必要ではないか。

・2035 年の根拠は分からないが、聞いた話によると、暗号を移行するのに 20 年～30 年かかると言う人もいるため、解読が可能な量子計算機が実現するまでにシステムの移行を隅々まで終わらせるという意味では、2035 年というのはぎりぎりの期限との考えもあり得る。

○黒田経済産業省イノベーション・環境局イノベーション政策課調整官

・資料 14 頁に記載されているような、6,000 量子ビット規模で８ギガゲートの演算が実行可能な誤り耐性のある量子計算機で、誤り率が 10 のマイナス 10 乗程度であった場合、RSA-2048 を解くのにどの程度の時間を要するのか。

・解く時間を長く見積もれば誤り率がより高くとも解けるのか。

○北川大阪大学特任教授量子情報・量子生命研究センター長

・量子計算機の種類にもよるが、例えば、超電導や光量子の量子計算機であ

れば、数日で解くことができると考えられる。
・試行回数を増やすことによって誤り率が高くとも解ける可能性はある。
〇中川デジタル庁統括官付参事官
・超電導、イオントラップ、光量子等の量子計算機の方式のうち、誤り訂正と親和性が高い方式はあるか。
〇北川大阪大学特任教授量子情報・量子生命研究センター長
・誤り訂正と親和性が高い方式というのは、特に現状ではないと思われる。誤り訂正に関しては、５つの方式（超電導、イオントラップ、光量子、半導体、中性原子）がしのぎを削っており、どの方式が得意というのは今のところない状況である。
〇梅城総務省サイバーセキュリティ統括官付企画官
・演算回数が増えると計算時間がコヒーレンス時間を超えて量子状態が失われる。公開鍵暗号の解読には、量子ビット数と誤り率に加えて、コヒーレンス時間も関係してくるのではないか。
〇北川大阪大学特任教授量子情報・量子生命研究センター長
・コヒーレンス時間は量子計算機の方式によって全く異なるタイムスケールである。(誤り訂正を前提とする場合) コヒーレンス時間だけで性能を評価しているわけではなく、コヒーレンス時間と演算時間の比で決まるような形の誤り率を一般的に考えている。
・各ゲートの演算を行う際に生じる誤りも、演算している間にデコヒーレンスが起こってしまうことも、同じく誤り率として取り扱っている。
〇髙橋内閣官房内閣参事官
・RSA-2048 を解読可能な量子計算機が実現してから世の中に普及するまでに、どれくらいの時間がかかるのか。
〇北川大阪大学特任教授量子情報・量子生命研究センター長
・最初にそうした量子計算機が１台でも作られたときが、一番世の中にインパクトがあり、現代の暗号に関しては危険な状態と思われる。
・１台でも十分なものができたら、それを量産すること自体は難しくない。

（2）その他

杉本内閣官房内閣参事官から、デジタル庁と協力し、政府機関等に対して暗号移行に係る調査を現在実施していることが報告された。

〇今後の予定
・次回は、検討すべき論点のとりまとめの方向性を検討することとされた。