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（第１回）議事要旨

１　日時

令和７年６月30日(月)17:30～18:00

２　場所

中央合同庁舎８号館６階623会議室

３　出席者

○議　長

阪田　　渉　内閣官房副長官補（内政担当）

○副議長

股野　元貞　内閣官房内閣審議官（国家安全保障局）

木村　公彦　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

楠　　正憲　デジタル庁統括官（デジタル社会共通機能担当）

山内　智生　総務省サイバーセキュリティ統括官

奥家　敏和　経済産業省大臣官房審議官（商務情報政策局担当）（代理出席）

○構成員

西山　英将　内閣官房内閣審議官（内閣官房副長官補付）

川上　大輔　内閣府科学技術・イノベーション推進事務局審議官（代理出席）

飯濱　誠　　警察庁長官官房技術総括審議官

冨安泰一郎　デジタル庁統括官（戦略・組織担当）

斉田　幸雄　外務省大臣官房サイバーセキュリティ・情報化参事官

塩見みづ枝　文部科学省研究振興局長

菊川　人吾　経済産業省イノベーション・環境局長

家護谷昌徳　防衛省大臣官房サイバーセキュリティ・情報化審議官

４　議事要旨

○連絡会議の趣旨説明等

会議に先立ち、西山内閣官房内閣審議官が本連絡会議の趣旨及び運営要領案の説明を行い、資料１－１のとおり本連絡会議の開催についての申合せ案が承認され、資料１－２のとおり運営要領に関して決定した。

○冒頭挨拶

阪田議長から、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危殆化が懸念されており、耐量子計算機暗号（PQC）への移行には、多岐にわたる課題に広範囲の検討が必要であり、政府機関等における耐量子計算機暗号（PQC）利用に関し、必要な施策を検討・推進するために、今後、諸外国の対応なども参考にしつつ、関係府省庁の緊密な連携による検討を進めていく旨挨拶がなされた。

○議事

（１）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

（２）検討すべき論点（案）について

（３）今後のスケジュール（案）について

・木村内閣審議官から、資料２、資料３及び資料４に基づき、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、検討すべき論点（案）、今後のスケジュール（案）について、説明がされた。

・出席者から、資料２、資料３及び資料４の内容について特段の異論はなかった。

（４）その他

出席者より、以下のような発言があった。

○股野内閣官房内閣審議官

・PQC 移行に向けた検討は喫緊の課題であり、移行が遅れた場合には安全保障上の支障も懸念されるため、関係省庁と連携しつつ、必要な検討を進めていく。

○木村内閣官房内閣審議官

・「政府機関等のサイバーセキュリティ対策のための統一基準」に基づき、サイバーセキュリティの観点から PQC への移行に対応するが、多岐にわたる課題があり、関係府省庁の知見が必要である。

・本年 5 月 29 日のサイバーセキュリティ戦略本部においても、「関係省庁による検討体制を立ち上げ、政府機関等における耐量子計算機暗号（PQC）への移行の方向性について、次期サイバーセキュリティ戦略に盛り込む」こととされており、関係府省庁と連携して検討する。

○楠デジタル庁統括官

・PQC への移行を円滑に進めるには、システム運営者との丁寧な調整を行い、多種多様なシステムの暗号利用の形態によって脅威が異なるこ

となどを踏まえた対応が重要である。利用形態や移行に要する期間などの特性に応じて、適切な目標や期限を設定することが必要なことから、とりまとめに向けてスピード感を持った検討に取り組む。

○山内総務省サイバーセキュリティ統括官

・国立研究開発法人情報通信研究機構（NICT）とも連携しながら、暗号の技術的評価に注力しており、現在、CRYPTREC において、PQC を「推奨『候補』暗号リスト」に掲載するための、技術的な安全性の評価に係る検討を進めている。PQC の安全性を確認するためには的確かつ十分な評価を実施する必要があり、この検討を踏まえつつ、関係府省庁連絡会議に対し、技術的観点から貢献していく。

○奥家経済産業省大臣官房審議官

・産業界においても暗号は広く使われており、特に重要インフラは社会経済への影響が大きく、民間部門も視野に入れるべき。暗号には数学に長けた高度人材が必要であるが人材の基盤が弱まっており、人材育成についてエコシステム全体で考えるべき。議論には学識経験者や産業界の実務者から専門的意見を聞く機会も持つべき。

○木村内閣官房内閣審議官

・民間部門への観点も重要であるが、まずは、政府機関等における移行の方向性を検討することで、民間部門における導入の呼び水となることも期待したいこと、高度人材の基盤が弱まっていることの認識は共有すること、学識経験者や産業界の実務者からの知見を得る機会等を幹事会などで設けることも考えられる。

○西山内閣官房内閣審議官

・米国 NIST 標準以外の暗号方式の導入の可能性を検討することについてどう考えるか。

○木村内閣官房内閣審議官

・海外において米国 NIST 標準以外の暗号方式の検討がなされていることは事実であり、我が国において異なる方式を検討する可能性はあり得る一方、NIST 標準の暗号方式が国際的にも有力な候補であり、その方式との連携は無視できないと考える。

○今後の予定

・今後は、幹事会において具体的な検討を進めることとされた。