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1回) 議事要旨

1 日時

令和7年7月31日(木)13:30~15:00

2 場所

国家サイバー統括室会議室

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

高橋 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

武尾 伸隆 経済産業省商務情報政策局サイバーセキュリティ課長

○構成員

神崎 忠彦 内閣官房内閣参事官 (内閣官房副長官補付)

田淵 敬一 内閣府科学技術・イノベーション推進事務局企画官(代理出席)
併任 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

森田 正敏 警察庁長官官房技術企画課長

増原 剛輝 デジタル庁統括官 (戦略・組織担当) 付参事官

齋藤 翼 外務省大臣官房情報通信課首席事務官(代理出席)

武田 伸二郎 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長

石丸 光宏 防衛省整備計画局サイバー整備課 AI・サイバーセキュリティ
政策調整官(代理出席)

4 議事要旨

○幹事会の趣旨説明等

会議に先立ち、杉本内閣官房内閣参事官が、参考資料1、参考資料2及び参考資料3について、本幹事会の構成員の官職の指定及び運営要領等の説明を行った。

○冒頭挨拶

西山議長から、先月に第1回連絡会議が開催され、本幹事会において具体的な検討を進めていくことになっており、PQCへの移行には、多岐にわたる課題の検

討が必要であるため、本幹事会でしっかり検討を進めていく旨挨拶がなされた。

○議事

(1) 検討すべき論点について

関係府省庁から説明があった主な内容は以下のとおり。

- 杉本内閣官房内閣参事官から、政府機関等における暗号の利用、PQC の概要、諸外国における PQC 移行の状況等について説明。
- 田淵内閣府科学技術・イノベーション推進事務局企画官から、量子計算機の開発・普及状況について説明。
- 梅城総務省サイバーセキュリティ統括官付企画官から、暗号の危殆化、PQC の安全性等の評価等について説明。
- 武尾経済産業省商務情報政策局サイバーセキュリティ課長から、PQC の安全性等の評価等について説明。
- 高橋内閣官房内閣参事官及び杉本内閣官房内閣参事官から、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説明。
- 中川デジタル庁統括官付参事官から、政府の情報システムの整備及び管理について説明。

次に、意見交換が行われ、出席者より、以下のような発言があった。

- 梅城総務省サイバーセキュリティ統括官付企画官
 - ・現代暗号の危殆化時期についての予測は困難である。諸外国の動向を踏まえ 2035 年に言及するならば、政策的な判断となるのではないかと。
 - ・政府システムは多数あり、移行の優先度を確認することがまず必要ではないかと。また、どんな暗号がどこで使われているか把握すること（クリプト・インベントリ）が重要。
 - ・PQC は成熟途上の技術であり、NIST の標準化プロセスの中で脆弱性が判明し取り下げられたものもあった。暗号部分を迅速に切り替えられる能力（クリプト・アジリティ）の構築も重要。
 - ・共通鍵暗号の移行やハイブリッド暗号などにも留意。
 - ・PQC の実装に関し、民間企業からも対応製品の動向を聞いてはどうか。
- 杉本内閣官房内閣参事官
 - ・PQC 移行に関しては、既存暗号と PQC が並存する期間があるとともに、PQC に脆弱性が見つかる可能性もあることには注意をしていきたい。
 - ・有識者等からのヒアリングとして、民間企業のほか、量子計算機等の専門家の話を聞くことも考えられる。
- 武尾経済産業省商務情報政策局サイバーセキュリティ課長
 - ・技術の不確実性はあるものの、一方で、諸外国もそういった中で、安全性を考えて、2035 年としていると考えれば、日本だけ遅れることのないよう

にしていくことには違和感はない。

- ・他方、EUのように、リスク等に応じてスケジュール感が違うところがあり、Harvest Now, Decrypt Later (HNDL) 攻撃のようなリスクがあるものについては、前倒しをしなければならないかもしれない。
- ・民間企業から現状や課題意識を聞くことは意味があると思う。

○中川デジタル庁統括官付参事官

- ・PQC 移行を実際にどのように進めていくかについては、パイロット事業のようなものを含め、PQC 移行に対応した機器が必要になってくる。

(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予定していることが報告された。

○今後の予定

- ・次回は、有識者等からのヒアリングを検討することとされた。