2024.7.18
座長資料

「預金取扱金融機関の耐量子暗号への対応に関する検討会」の成果物について

1．成果物の作成方針

- 対象金融機関が PQC 対応の必要性や期限などを正しく理解し、自身のビジネスリスクの一環として適切なアクションをとるための情報を提供することを目的とする。
- そのため、技術論の深いところには踏み込まず、対象金融機関として考慮すべき点、留意すべき点を中心に記載する。

2．成果物の想定読者

- 対象金融機関の CIO、CISO など、PQC 対応にリーダシップを発揮して取り組む責任を有する者
- システムやサイバーセキュリティの統括部署の役席者など、実務的に PQC 対応を推進する役割を有する者
- 対象金融機関の経営層については、本成果物の直接的な読者とは想定しないが、本成果物をもとにした概要をもとに各金融機関内で説明することを想定

3．成果物の目次案（次ページ以降）

2024.7.18
座長資料

(仮題):預金取扱金融機関における耐量子計算機暗号(Post-Quantum Cryptography、PQC)への移行を検討する際の推奨事項、課題及び留意事項

- 会議での論点(案)を記載

【目次(案)】

1. 背景
2. はじめに
   - 要議論:量子コンピュータの脅威や移行の重要性もここで記載するか
   ① 金融分野の特性
3. 耐量子計算機暗号対応とは何か
   - 要議論:どこまで詳細に記載するか。QKD や FTQC・CRQC
   ① 量子コンピュータの発展と現在の暗号方式への影響
   ② 現在のセキュリティ対策への影響
      i. 既存暗号スキームへの影響
      ii. Harvest Now Decrypt Later (HNDL)のメカニズムと対策
   ③ 対策の標準的アプローチ
   ④ 対応期限のメルクマール
      - 論点:要否議論
4. 国内外の対応状況
   - 要議論:米国等海外の動向、国内でも ISAC 等どこまで記載するか
   ① 耐量子暗号対応の概要
   ② 標準化動向
      i. NIST
      ii. CRYPTREC
      iii. IETF
   ③ 政府・当局
      - 要議論:監督当局の取組みは別章か
   ④ 金融機関
   ⑤ 主要業界動向
      i. 通信、エネルギー、製造他
   ⑥ IT ベンダー
5. 金融分野における耐量子暗号対応の必要性
   - 要議論:現状と将来像として、金融分野に特化した記載が可能か
   ① 金融データの機密性と完全性
   ② 金融機関に対して起こり得る脅威シナリオ
   (既存サイバーセキュリティ対策の無効化)

③ 金融機関に対して起こり得る脅威シナリオ
（新たな脅威の手口の出現 – HNDL）

6. 耐量子暗号対応移行に向けた推奨事項

- **要議論：推奨事項をどのレベル（必須・推奨）、どの項目まで記載するか**

① 耐量子暗号対応の特徴（対応計画の前提事項）
② 耐量子暗号対応プリンシプル
③ 移行に向けた推奨事項
  i. 耐量子暗号対応の優先度・リスクの考え方整理
  ii. クリプト・インベントリの構築・更新（こちらは、より具体的に記述）
  iii. アーキテクチャの構築・更新
  iv. 耐量子暗号対応の期限の考え方整理
    - 論点：要否議論
  v. コンティンジェンシープランの整理
    - 論点：要否議論
④ IT ベンダーとの連携
⑤ 監督当局、業界団体等との連携

7. 耐量子暗号対応に向けた課題・留意事項

- **要議論：技術・態勢・法令等重視するのはどこか。幅広に態勢重視か。**

① 技術面
  i. システム互換性や運用上の課題
  ii. 長期的なセキュリティ戦略との整合
② 態勢面
  i. 経営陣の理解
  ii. 関係者の役割・責任の明確化
  iii. リソース（ヒト・カネ）の確保
③ 法令・規制面

8. 事例研究

① 国内外での PQC 導入事例
② 金融業界における先行研究と実装例（もしあれば）

9. まとめ

① 移行への全体的な見解
② 預金取扱金融機関に対しての注意喚起
  i. リスクとリスク低減戦略の理解
  ii. リスクの評価
  iii. リスク低減のための計画の策定

10. 参考文献

① 研究資料・技術文書

② 国際標準化機関の文書

４．PQC 対応における論点（案）

- 対応期限について
  - 優先度の高いシステムの対応は 2030 年という期限設定の妥当性
- リスク評価について
  - 「優先度」をどのように決定するか
    - ✧ リスク評価フレームワーク：WellsFargo、Mosca、CARAF のいずれを使うのがよいか
  - PQC が実装されるまでの間、HNDL に対するリスク低減策はあるのか
- クリプト・インベントリ作成について
  - クリプト・インベントリはどのようにして作成するのか（ツールがすべてをやってくれるわけではないということを明確にする）
- 移行について
  - PQC 移行の前提となることは何か（例：TLS1.3 への移行とか）
  - データサイズや計算量の増加にどのように対応すべきか
  - サプライチェーンのリスクをどのようにして評価するか
- ステークホルダーマネジメントについて
  - 経営にはいつ何を伝えるべきか
  - IT ベンダーにはどのように働きかけるべきか(契約に PQC 対応を盛り込むか)
  - お客さまへの通知はいつ、どのようなものを出すべきか
- 本成果物の活用について
  - 本成果物をもとに、業態にあわせて概要版を業界団体・中央機関が作成するということにできないか（個別各社の負担軽減にもつながる）

以上