PQC論点整理(1/3)

論点	検討状況	整理方向性（案）
【脅威リスク】 量子技術進展に伴う攻撃リスクについて	• 米国では大統領令などによりPQC移行を推進しており、グローバルな送金システムなどにおいて、PQC移行が接続前提条件となり、移行未完了のシステムが接続不可となるビジネスリスクの影響度が大きい	■ 高リスクとして、海外当局の規制により、グローバルな送金システムなどにPQC対応未完了システムが接続不可となるビジネスリスクについて、記載予定
【移行期限設定】 優先度高システムにおける2030年期限設定の妥当性	• NSA（National Security Agency）では、2033年までに、各ベンダーに対してPQC移行依頼 • 米政府では、2035 年までに連邦政府機関システムにPQC導入によりリスク解消する方針を発表 • 米国金融標準化団体ASC X9は、2027～2052 年にCRQCが実現見通し公表	■ ビジネスリスク観点において、優先度高システムは2030年代前半から半ばを目安にPQCのアルゴリズムを利用可能な状態にすることが妥当。もっとも、上記のタイミングについては、当局規制や技術状況をフォローしながら柔軟に対応することが必要 ■ PQCへの完全移行時期は、脆弱性や実装課題、顧客影響等も踏まえて、継続検討課題として各社が判断するものであることから本検討成果物における記載対象外 ■ 技術進展や規制動向に備え、暗号インベントリ作成は早期着手が必要
【暗号インベントリ作成に関する優先度検討】	• 各機関において、データ保存期間や漏洩リスク評価などリスクベースでの検討実施の上、優先度を策定 • 中長期的な視点では、暗号管理ツールの活用やSBOMなどのソフトウェア資産管理の取り組みに含めて推進する進め方も有り	■ リスクベースで検討した移行優先度の高いシステムから作成するのが現実的 ■ 中長期的にはSBOMなどのソフトウェア資産管理の取組に含めて推進
【移行対象に関する優先度検討】	• 暗号インベントリ作成と同様に、リスクベースでの移行優先度検討が必要 • 内部通信については、多層防御により一定レベルのセキュリティ強度が担保されており、ケースバイケースでの検討が必要	■ リスクベースでの検討により、各社ごとに移行対象システムの優先度選定が必要 ■ 内部システムは多層防御の観点に基づき、ケースバイケースで検討

PQC論点整理(2/3)

論点	検討状況	整理方向性（案）
【監督当局、業界団体等との連携】 政府機関や民間団体など業界全体としての発信について	**＜国の取り組み＞** • PQC対応は、金融分野のみならず、今後、重要インフラ全体に波及することも想定され、重要インフラ防護の観点から同政策を所掌するNISCの関与も必要 • 他方で、NISCが自ら全ての重要インフラの状況を把握することは困難であることから、個々の重要インフラの状況把握については、監督当局、業界団体が支援 **＜金融業界の取り組み＞** • 預金取扱金融機関やお客様に向けたPQC移行推進のためには、当局以外にも各ステークホルダー（ベンダーやシステムインテグレータを含む）への働きかけや発信が必要であるため、移行全体ロードマップ提示が必要 • 金融業界（預金取扱金融機関以外も含む）としての対応スタンスや移行ロードマップを取り纏め・策定する主体を、金融庁などの協力を得ながら決定する必要有	＜国の取り組み＞ ■ 報告書内に左記の趣旨の内容を記載 ＜金融業界の取り組み＞ ■ 金融庁や各団体と相談しつつ、業界全体向けのロードマップを作成する必要有
【コンティンジェンシープラン】	• 対応期限までに優先度が高いPQC移行が完了しない場合を不測の事態と捉えて、量子コンピュータを用いた暗号危殆化リスクを低減させるための代替の対策を検討しておくことを推奨 • 具体的なリスク低減策として、事前共有鍵による通信秘匿化、暗号通信の利用を必要最低限にする、重要な文書への署名については物理原本の厳重保管等	■ 報告書内に左記内容記載予定
【暗号アジリティ】 脆弱性への迅速な対応や段階的にPQC移行検討について	• PQCは既存暗号と比べて新しい技術であるため、将来的に効率の良い解読法や重大な脆弱性が発見される可能性があり、クリプト・アジリティ（暗号の俊敏性）の組み込みやハイブリッド方式の利用を検討 • PQC移行自体がゴールではなく、網羅的かつ継続的な暗号管理や迅速な暗号切り替え可能な仕組みの導入が必要	■ 報告書内に左記内容記載予定

PQC論点整理(3/3)

<table>
<tr><th>論点</th><th>検討状況</th><th>整理方向性（案）</th></tr>
<tr><td>【暗号インベントリ】
標準的なインベントリ構築手法について</td><td>暗号利用システム構築担当者（開発ベンダ含む）への問合せを想定するが、より正確かつ網羅的に調査するためツール利用による方法も要検討
(FS-ISACでは手作業やスキャンツール利用など複数の収集方法について提示)

＜インベントリ構築例＞
スコープ：自組織で利用される暗号機能をもつシステムで、以下対象を想定
● 自組織開発のシステム、自組織外から提供されたシステムおよび製品
収集する情報：
● 暗号利用場面：以下情報を想定
➢ ユーザとの通信
➢ インターネットVPNによるリモートアクセス
➢ 電子文書や電子メールへの署名
➢ サーバ証明書による認証
➢ データベースの暗号化
● 暗号利用用途：以下情報を想定
➢ 通信内容を保護するため
➢ お客さま情報を安全に保存するため
➢ 文書の改ざんを防ぐため
➢ サーバのなりすましを防ぐため
● 暗号実装箇所：以下情報を想定
(Ex.自組織開発アプリ、自組織外製品（ハードウェア/ソフトウェア/アプリ）
● 利用アルゴリズム：以下情報を想定
(Ex.RSA-OAEP、ECDH、RSA-PSS、ECDSA)
● 利用している鍵長
● 鍵管理方法 (Ex.自組織所有のHSMにて管理、クラウドサービスで管理)
● 利用担当者

収集方法：以下の複数手段を想定
● システム担当者、開発ベンダーや製品ベンダーへのヒアリング
● ネットワークスキャンツールやアプリケーションコード解析による発見</td><td>■ 報告書内に左記表で例示予定</td></tr>
</table>

【参考】論点に対する事前コメント抜粋(1/2)

論点	事前コメント
【移行期限設定】	PQC移行期限につきまして、「30年代前半から半ば」という考え方に加えて、システム更改のタイミングでの移行を整理方向性に含めることはできないでしょうか。 PQC移行時のシステム改修規模にもよりますが、システム更改と合わせて移行することで適用時のリスク低減を図ることが可能と考えております。
【PQC移行に関する優先度検討】	「リスクベースでの移行優先度検討が必要」との記載があるものの、金融機関同士の相互影響が大きい業界特性に鑑み、勘定系や自振システムなど、PQC移行を優先的に検討すべきシステムを例示いただきたい。
【監督当局、業界団体等との連携】	預金取扱金融機関やお客様に向けたPQC移行推進のためには、当局以外にも各ステークホルダーへの働きかけや発信が必要であるため、移行全体ロードマップ提示が必要 －－ 欧州においては、欧州委員会が、今年の4月に以下という文書を発行しています。 Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography ここでは、2年以内（2024年4月から2年以内）に以下のような理由から「耐量子計算機暗号協調実施ロードマップ」の策定を求めいます。 耐量子計算機暗号への効果的な移行のために、「耐量子計算機暗号号協調実施ロードマップ」は、ポスト量子暗号アルゴリズムの検討を含む、加盟国が取り組むべき行動のリストを提供し、それらの相互依存性や関与する利害関係者を考慮しながら、到達すべき異なるフェーズやマイルストーンの明確なタイムラインを提供するべきである。 －－ 相互依存性や関与する利害関係者によるCoordinated Implementation　は、やはり、金融業界に閉じた活動だけでは限界があり、「移行全体ロードマップ提示」は、今回の調査結果なども踏まえてNISC等に求めることも、重要かと思いました。 →本日ご議論いただきたい点

【参考】論点に対する事前コメント抜粋(2/2)

論点	コメント
【暗号アジリティ】 脆弱性への迅速な対応や段階的にPQC移行検討について	PQCの移行がすぐに可能になるとは思えず、例えば、現在、直近で計画されているシステムや、システム刷新にPQCが、直接的に適用できるとは考えにくいののですが、それであっても、今後、数十年利用されるシステムを想定した場合、PQCへの移行が可能なシステム構築が必要であり、そのためには、「暗号アジリティ」を確保した、システムの発注（そのためのRFP)が必要なのかなと思います。
【暗号インベントリ】 標準的なインベントリ構築手法について	収集する情報で「利用している鍵長」というのがありますが、「利用されている鍵長、および、鍵の利用期間」とすると、より有意な情報が、集まるかなと思いました。 鍵の利用期間は不明も多いかと思いますが、不明の場合、ある意味、移行のポリシーに欠ける可能性があるし、利用期間が明確な場合は、移行のタイミングの参考になるかなと思いました。
その他	ＰＱＣ移行時には、システム障害を発生させないことは重要な論点と考えております。システムテスト、システム移行など、システム実装時の留意事項を含めていただけないでしょうか。各行でシステム構成は異なりますが、共通的なポイント・観点があるものと考えております。