耐量子暗号移行のための協調実装ロードマップ

Part1,Version:1.1, EUPQC ワークストリーム

11.06.2025

目次

1 エグゼクティブサマリー 3

2 序論と動機 5

3 範囲と定義 6

3.1 範囲 6
3.2 よく使われる専門用語の定義 6

4 年表 8

4.1 概要 8
4.2 タイムラインの詳細：マイルストーン、最初のステップと次のステップ 9

5 量子リスクの見積もり 12

6 PQC 移行へのステップ 14

6.1 序論 14
6.2 最初のステップ 14
6.3 次のステップ 16

7 EU にできること 19

参考文献 20

1 エグゼクティブサマリー

デジタル・インフラには強固なサイバーセキュリティが必要である。暗号システムは、データの機密性と認証器を保護するために不可欠である。量子コンピュータは、これらの保護目標を達成するために使用される暗号アルゴリズムの多くにとって脅威となる。現在、量子的安全性が確保されていないデータは、それが保存されるものであれ送信されるものであれ、また長期にわたって機密性を保持しなければならないものであれ、将来、量子コンピュータによって危険にさらされる可能性がある（「今すぐ保存、後で復号」攻撃）。さらに、認証器も量子コンピュータによって危険にさらされる。量子コンピュータがサイバーセキュリティにもたらす脅威は、タイムリーで包括的かつ協調的なポスト量子暗号（PQC）への移行によって対抗することができる。

その結果、欧州委員会は 2024 年 4 月 11 日に「耐量子暗号への移行のための協調的な実装ロードマップに関する勧告」を発表した[1]。この「実装ロードマップ」の策定にあたり、欧州委員会は NIS 協力グループ（NISCG）内に PQC に関するワークストリームを設置することを勧告した。

本文書は、PQC に関する NIS CG のワーク・ストリームの最初の成果物であり、加盟国を対象とした最初のハイレベル・ペーパーとなることを意図している。PQC への同期した移行のために加盟国が実施すべき一連の勧告は、移行を開始するために必要なファーストステップと、その後に続くべきネクストステップに分かれている。この文書の勧告には、国内、欧州、国際レベルにおいて、すべての利害関係者が暗号に対する量子の脅威を十分に理解し、知識と経験を交換できるようにするための方策が含まれている。また、量子的脅威をすべての関連事業体のリスクマネジメントの一部とし、成熟した暗号資産管理を確立することで、PQC への移行を促進し、暗号全般の俊敏性を改善することを推奨する。本文書で取り上げた PQC 移行のためのステップの多くは「後悔のない」動きであり、サイバーセキュリ ティ全般を改善し、サイバーセキュリティ規制、特に NIS2 指令[2]への準拠を支援するものである。

これらの提言に加え、本文書では、ドイツ連邦情報セキュリティ機関（BSI）による量子コンピュータの開発状況に関する現在のアセスメントを考慮し、最近の出版物「Securing Tomorrow, Today」に沿って、欧州連合における PQC への移行の推奨スケジュールを示す：これは、欧州 21 カ国のパートナーによる共同声明である。

特に、すべての加盟国が、2026 年末までにファーストステップに従った国内 PQC 移行戦略を開始し、EU レベルでの取り組みを調整することが推奨される。同時に、リスクの高いユースケースはできるだけ早く、遅くとも 2030 年末までに PQC に移行すべきである。さらに、量子安全アップグレードはデフォルトで有効にし、PQC 移行計画は、特に推奨される「次のステップ」の実施によって、より洗練されたものにすべきである。2035 年までに、、現実的に可能な限り多くのシステムで移行を完了させるべきである。この野心的なスケジュールは、暗号が解読されれば、EU とその加盟国の社会、経済、セキュリティ、繁栄に不可欠なデータの保護と機密コミュニケーションの確保に深刻な影響を及ぼすことから正当化される。耐量子暗号ソリューションに移行する際には、実行可能で適切な場合には、標準化されテストされたハイブリッドソリューションを使用することが推奨される。

過去数年にわたり、EU は、EU のサイバーセキュリティと集団的レジリエンスを強化するために、強力な戦略、政策、立法の枠組みを整備してきた。特に、NIS 2 指令[2]とデジタル・オペレーショナル・レジリエンス法（DORA）[4]は、対象事業体に対し、最先端の暗号技術の利用を含むサイバーセキュリティ・リスク管理措置の採用を義務付け、これらの要件を遵守しなかった場合、事業体のマネジメント団体が責任を問われる可能性があることを規定している。さらに、サイバーレジリエンス法（CRA）[5]は、2027 年 12 月 11 日以降、EU 上市されるデジタル要素を含むすべての製品について、サイバーセキュリティに関する水平的な要件を定めている。ソフトウェアとファームウェアのアップグレードの認証器と完全性を確保する必要性と、PQC 標準の進化に対

応するためにアップグレードされる機器の能力そのものは、製造事業者、特に加盟国にとって、CRA の実施とその将来の施行に備える上で重要である。さらに、学術界、産業界、公共団体を含むさまざまな利害関係者が参加する整合規格の策定も、本文書で言及されているタイムラインを考慮する必要がある。欧州委員会はまた、標準化のための欧州連合行動計画の中で発表される標準化活動を支援するための行動も計画している。

2 序論と動機

暗号技術は、私たちの日常生活に直接影響を与える広範なサービスの安全性を確保する上で極めて重要である。例えば、デジタル政府サービス、銀行システム、メッセージングアプリのようなコミュニケーションサービスなどである。暗号技術は、すべての重要なインフラの安全な運用を保証するために不可欠である。

現在展開されている暗号が破られた場合、デジタル・インフラへの影響は壊滅的なものになるだろう。量子コンピュータの開発は、暗号にそのような脅威をもたらす。このことは、1994 年にピーター・ショーが量子アルゴリズムを発表して以来、知られていることであり、この量子アルゴリズムを使えば、現在使われている暗号アルゴリズムの多くを破ることができる。したがって、これらのアルゴリズムが十分に強力な量子コンピューターで実装されれば、安全なデジタル基盤の基盤が損なわれることになる。

現在のところ、これがすでに可能であるという証拠はない。とはいえ、2015 年に米国国家安全保障局（NSA）は、量子コンピューターの開発が現在の量子脆弱性暗号に差し迫った脅威をもたらすという緊急警告を発した。欧州の機関も、[6]などで早くからこの脅威について公言している。量子コンピュータの開発の現状や将来的に利用可能になる可能性を適切に評価するため、当初 2017 年から 2020 年にかけて BSI に代わって「量子コンピュータの開発状況」という調査が実施され、直近では 2024 年に更新された[7]。この更新されたアセスメントによると、このような量子コンピュータは最長で 16 年後（すなわち 2040 年またはそれ以前）に実現可能となる可能性が高い。しかし、量子コンピュータのハードウェアだけでなく、エラー訂正と緩和における現在のヒューリスティックが完全に検証されれば、この期間は 10 年まで大幅に短縮される可能性がある。Global Risk Institute による最新の "Quantum Threat Timeline Report" [8]では、量子コンピュータが 24 時間以内に RSA-2048 を破れる可能性について、主要な専門家の意見に基づく推定が示されている。彼らは、今後 10 年以内にそれが起こる可能性は 19%～34%と見積もっている。

量子コンピュータが、現在使用されている量子脆弱性暗号をいつ破ることができるようになるかを正確に予測することはまだ不可能だが、そのような事態が発生した場合の影響を考えると、特定の組織はすでに今、緩和策に着手する必要がある。最も有望な解決策は、いわゆる耐量子暗号（PQC）である。PQC は現在使用されているシステムやコンピューターに実装することができるが、量子コンピューターに対して安全であることを目標に設計されている。しかし、量子脆弱性暗号から PQC への移行には多大な時間とリソースを必要とする。過去の移行から判断すると、このプロセスには 5 年以上かかるかもしれない。

現在、主に 2 つの脅威シナリオが懸念されている：

- 敵が暗号化されたデータを保存し、暗号に関連する量子コンピュータが出現した時点で復号化する「今すぐ保存、後で復号化」シナリオ。これは、データの機密性を長い期間防御する必要がある場合の脅威である（例えば、政府データ、機密性の高い個人データ、企業秘密や営業秘密など）。

- 公開鍵基盤（PKI）や寿命の長いデバイスのような複雑なシステムで発生する長い移行期間。最初のシナリオのように、システムが継続的な攻撃の影響を受けていない場合でも、量子安全暗号への移行が間に合わず、すべてのコミュニケーションの機密性と認証が損なわれる可能性があるというリスクがある。

したがって、PQC への移行には、十分な準備と体系的かつ粘り強い対応が必要である。各国政府は、PQC への移行を期限内に完了させるために今すぐ行動を起こす必要があり、このプロセスにおいて EU の支援を受けなければならない。

3 適用範囲と定義

3.1 適用範囲

本文書は、PQC に関する NIS CG ワークストリームの最初の成果物である。加盟国を対象とした PQC への移行に関する最初のハイレベルなコンセプトペーパーとなることを意図している。この文書は、NIS2 指令に準拠しなければならない事業体を含む政府機関やその他の事業体にとっても、若干の修正を加えることで有用なものとなるであろう。

暗号技術における量子の脅威を軽減するための情報やガイダンスが記載された出版物は、既にいくつか存在する。(リストは網羅的ではない)。

本文書は、欧州委員会の勧告に従った協調実施ロードマップの最初のリリースである。公共行政機関やその他の重要なインフラストラクチャー、特に NIS2 指令の適用範囲にあるものは、EU 全体で同期された移行を確実にするために、この文書と今後のリリースを参照すべきである。

この調整実施ロードマップの最初のリリースには、加盟国の PQC 移行に関する推奨スケジュールと、各加盟国の国内 PQC ロードマップに含めるべき措置のリストが含まれている。タイムラインは次のセクションで概説され、加盟国が国家プログラムを立ち上げる際の指針となるよう、対策はファーストステップとネクストステップに分けられている。調整実施ロードマップの後のバージョンおよび追加部分では、政府、産業界、学界との協議を経て、より詳細な（技術的な）詳細が示され、さらに推奨される措置が定義される予定である。

3.2 使用頻度の高い技術用語の定義

暗号アジリティ（または暗号アジリティ）

暗号プロトコルとシステムをモジュール方式で設計し、暗号コンポーネントを交換できるようにすること。この概念は、プロトコル実行中に暗号スイートをネゴシエートする要件と混同してはならない。

暗号インベントリ

暗号資産の構造化された概要。

暗号関連量子コンピュータ

現在の量子脆弱性暗号で使用されているサイズの因数分解問題や離散対数問題を解くのに十分な脆弱性を持つ量子コンピュータ。

ハイブリッド

同じメカニズムに対して、耐量子アルゴリズムと量子脆弱性アルゴリズムを組み合わせたもの。

耐量子暗号 (PQC)

従来の攻撃や量子攻撃に対して安全なように開発・設計された非対称暗号アルゴリズム。

公開鍵基盤 (PKI)

公開鍵証明書を発行、維持、失効するための枠組み。

量子攻撃

量子アルゴリズムを実行する暗号関連量子コンピュータを使用して、暗号アルゴリズムを攻撃すること。

量子安全

対称暗号アルゴリズムも対象となる。

量子脆弱性

量子安全でないもの。量子攻撃に対して脆弱性が予想される暗号アルゴリズム。

トラディショナル

文脈に応じて、量子脆弱性（暗号メカニズムに対して）または非量子脆弱性（ア タックなど）。

4 タイムライン

4.1 概要

欧州委員会の「ポスト量子暗号への移行のための協調実施ロードマップに関する勧告」[1]は、このようなロードマップを勧告の公表後 2 年以内（すなわち 2026 年 4 月まで）に公表することを示唆した。各国の PQC 移行計画の策定と更なる適応は、協調実施ロードマップに示された原則に従って行われるべきである。しかし、移行プロセスには長い年月がかかると予想されるため、できる限り早期に行動し、特にワークストリームの最終成果物を待たないことが賢明であると思われる。その結果、この文書は初期ガイダンスを提供し、EU 全域での PQC への迅速な移行を促進し、2026 年末までにすべての加盟国で最低レベルの準備態勢を確保することを目的としている。

一般的には、PQC 移行のためのリスクベースのアプローチが推奨される。しかし、最初のガイドラインとして、PQC に関する NIS CG のワークストリームは、最初の推奨スケジュールを作成した。一方では、このタイムラインは、移行にはある程度の時間が必要であることを考慮し、他方では、「量子コンピュータの開発状況」[7]という研究の最新のアップデートに基づいている。重要なことは、早急な対応が必要であることであり、使用されているすべての公開鍵暗号を一度に移行することは不可能であるため、明確な優先順位を設定する必要があることである。

現時点では、本文書には詳細な技術的推奨事項は含まれていない。しかし、耐量子暗号に移行する際には、標準化されテストされたハイブリッド暗号を使用することを推奨する。特に、RSA や離散対数をベースとした仕組みのような量子脆弱性公開鍵暗号が現在使用されて いる場合は、PQC を含む標準化されたハイブリッド暗号への置き換えを検討すべきである。高リスクのユースケースについては、2030 年末以降、量子脆弱性公開鍵機構を単独で使用してはなら ず、中リスクのユースケースについては、2035 年末以降、量子脆弱性公開鍵機構を単独で使用してはならな い。アプリケーションによっては、公開鍵暗号の代わりに共通鍵暗号を使用するなどの選択肢も検討に値することに留意すべきである。

ほとんどの用途では、推奨される期限を守ることで、量子の脅威から十分な防御が得られると同時に、テストが不十分なソリューションから新たな脆弱性が生じる可能性のある無秩序な移行を避けることができる。しかし、推奨される期限を守れない場合は、個々のリスクを評価する必要がある。これは、量子コンピューティングの発展を注意深く監視し、他の（その場限りの、場合によっては一時的な）対策を検討することを含むかもしれない。将来的には、量子の脅威の影響を最小化するために、より高度な脅威分析が必要になるかもしれない。

PQC への移行スケジュール

1. 2026 年 12 月 31 日まで：

- 少なくともファーストステップが全加盟国によって実施されていること。
- すべての加盟国により、初期 PQC 移行ロードマップが策定されている。
- 高リスクおよび中リスクのユースケースを対象とした PQC 移行計画と試験運用が開始されている。

2. 2030 年 12 月 31 日までに

- すべての加盟国によって「次のステップ」が実施されている。

- 高リスクのユースケースに対する PQC 移行が完了。
- 中リスクのユースケースに対する PQC 移行の計画とパイロット実施が完了。
- 量子安全ソフトウェアとファームウェアのアップグレードがデフォルトで有効になっている。

3. 2035 年 12 月 31 日まで：

- 中リスクのユースケースに対する PQC 移行が完了。
- 低リスクのユースケースに対する PQC 移行は、可能な限り完了している。

4.2 スケジュールの詳細：マイルストーン、最初のステップ、次のステップ

1.PQC に関する作業部会は、以下の一連の初期対策を特定した（「最初のステップ」を参照）：

- 移行を成功させるために必要である；
- 今すぐ開始できる；
- また、暗号の俊敏性を促進する。

特に、すべての加盟国は、本文書に記載されているステップを実施するため、2025 年に国の移行計画の開始または更新を開始すべきである。加盟国は、ファーストステップに記載された措置を 2026 年末までに確実に達成すべきであり、調和のとれた実装を確保するため、PQC に関するワークストリームに定期的な状況更新を提供することが奨励される。

展開の面では、加盟国は、パイロット版を実施し、リスクの高いユースケースの移行を開始することにより、移行を開始することが重要である。2026 年末までに達成すべき推奨されるステップとマイルストーンは、「マイルストーン 1」にまとめられているが、これらの措置の詳細については「ファーストステップ」を参照されたい。重要なことは、完了すべきステップのリストが網羅的であると見なすべきではなく、国レベルまたは PQC に関する作業の流れの中で追加措置が特定される可能性があるということである。また、ロードマップの追加部分に反映されるかもしれない。さらに、加盟国が「次のステップ」の実施を 2026 年末まで待たないことも極めて重要である。これらも可能な限り早く着手すべきだが、完了までにはさらに時間がかかるかもしれない。

マイルストーン 1：2026 年 12 月 31 日

- **最初のステップ**
  - 利害関係者を識別し、関与させる。
  - 成熟した暗号資産管理をサポートする。
  - 依存関係マップを作成する。
  - 量子リスク分析を行う。
  - サプライチェーンを含める。

- 国家的な意識向上とコミュニケーション・プログラムを作成する。
- 知識を共有し、PQC に関する NIS CG のワークストリームに参加する。
- タイムラインと実施計画を策定する。

- **主な成果**
  - 高リスクおよび中リスクのユースケースを対象とした PQC 移行の計画立案と試験運用が開始された。
  - すべての加盟国において、初期の PQC 移行ロードマップが策定された。

2.本文書は、3 つの量子リスクカテゴリーを定義することで、関連するユースケースを特定するためのガイダンスを提供する：「低」、「中」、「高」である。量子リスクの推定及びこれらのリスクカテゴリの背景については、量子リスクの推定を参照。データの機密性が公開鍵暗号方式で保護されている場合、10 年以上経過しても機密性が侵害されることで重大な損害が発生するようなユースケースを、本文書では高リスクと見なしている。これは特に、攻撃者が将来暗号を解読するために、現在でも暗号化された情報を捕捉して保存する強い動機を持っていることを意味する。7]の推定を考慮すると、少なくとも 10 年間は機密性を保つ必要があるデータは、遅くとも 2030 年末までには量子コンピュータ攻撃から保護されるべきである。この勧告は、共同ポジションペーパー'Securing tomorrow, today'[3]と一致しており、最も機密性の高いユースケースの機密性を確保するために直ちに対策を講じ、遅くとも 2030 年までに保護するよう強く勧告している。推奨される期限は、実際には必ずしも十分ではないかもしれず、国家的な実施計画は、最も重要な資産の保護を優先すべきであることに留意されたい。また、量子コンピューティングの予期せぬ進歩により、移行プロセスの加速が正当化される可能性があることにも留意する必要がある。

将来的には、暗号化された通信や静止データを量子攻撃から保護することが最優先されるが、移行計画では、ライフサイクルの長いシステムや複雑なシステム（PKI など）の PQC への移行には多くの時間がかかることを考慮しなければならない。したがって、これらのシステムの移行は、事前に十分な計画を立てる必要がある。従って、これらのシステムについては、できるだけ早く詳細な移行計画の策定を開始することが推奨される。これには、事業の継続性を確保するためのパイロットとテストの実施を含めるべきである。

マイルストーン 2　31.12.2030

- **次のステップ**
  - 暗号の俊敏性と量子的安全性を確保したアップグレードパスをサポートする。
  - 移行のためのリソースを割り当てる。
  - 認証スキームの適応。
  - ルールを進化させる。
  - エコシステム内の機会を探す。
  - ロードマップの作成と実施を通じて、横断的な活動を考慮する。

- 試験的なユースケースを実施し、テストセンターに貢献する。

- **主な成果**

  - リスクの高いユースケースの PQC 移行が完了。

  - 中リスクのユースケースに対する PQC 移行の計画とパイロットが完了した。

  - 量子安全ソフトウェアとファームウェアのアップグレードはデフォルトで有効になっている。

2030 年以降の移行計画に不可欠なのは、量子安全アップグレードパスである。そのため、2030 年以降に市場に投入される製品については、PQC へのアップグレードが可能であること、また、ソフトウェアやファームウェアのアップグレードの仕組みには、完全性と認証のためのポスト量子署名スキームを組み込むことが強く推奨される。

この推奨期限も、量子コンピュータの研究 [7]に基づいており、すべての関連システムを PQC に完全に移行するには、5 年から 10 年程度は容易にかかると推定している。マイルストーン 1 の完了を待つ余裕はない。

3. 加盟国は、2035 年末までに可能な限り多くのシステムの移行を目指し、中リスクのユースケースの移行完了を優先すべきである。この日付は、以下の考察に基づいている。最近公表された NIST IR 8547 の初期公開ドラフト[18]では、従来の公開鍵暗号メカニズ ムは 2035 年以降使用できなくなると述べられている。この日付は、米国の国家安全保障覚書 10 に示された目標、すなわち「2035 年までに量子リスクを可能な限り緩和する」という米国の目標に基づいている。同様に、最近発表された英国 NCSC のタイムライン[19]では、PQC 移行の目標時期を 2035 年としている。したがって、高リスクおよび中リスクのユースケースについて PQC 移行を完了させるというマイルストーンは、EU と国際的なエコシステムとの整合性をうまくとっている。

5 量子リスクの推定

本文書では、移行プロセスの優先順位付けに役立てるため、量子リスク分析を実施するよう助言している。将来的には、量子リスクは通常のリスクマネジメントに統合されるべきである。量子リスク分析には、"The PQC Migration Handbook" [17]のセクション 2.4 に記載されているモデルを使用します。このモデルは、ISO 標準 27001 や BSI 標準 200-3 "Risk Analysis based on IT-Grundschutz"[20]などの国内標準に定義されている一般的な IT リスクマネジメント手法と互換性があります。

推奨されるタイムラインでは、3 つの基本的な量子リスクレベル「高」、「中」、「低」を区別しています。これらのリスクレベルは、[17]の図 2.7 に定義されている量子リスクスコアに基づいて定義されている。このアプローチに従うと、ユースケース（アプリケーションやシステム）の量子リスクレベルは、以下の 3 つの要因に影響される：

- 使用する暗号技術の量子的弱点
- 使用する暗号の量子的な弱点、使用する暗号が破られた場合に予想される影響；
- PQC への移行に必要な時間と労力の見積もりを行う。この方法論は、「Mosca の定理」[移行を担当する組織の管理下にある]に存在する量を組み込んでいる。しかし、暗号学的に関連する量子コンピュータが利用可能になるまでの所要時間は、前節で概説した移行の日付に織り込まれている。 8]に記載されているが、そのような部分に焦点を当てている。

PQC マイグレーションハンドブックでは、これら 3 つの要素に点数を付け、総合的な量子リスクスコアにマッピングしている。本文書で使用する 3 つのリスクレベル「高」、「中」、「低」へのマッピングは以下の通りである。

図 2.7 に示す量子リスクスコア [17]	本文書における量子リスクレベル
1	低
2	中
3 - 4	高

PQC 移行ハンドブックでは、量子リスクスコアが 4 の場合、「急性リスク」という用語も使用しているが、本文書では 3 つのリスクレベルで十分であることに留意されたい。

以下では、機密性と認証器が伝統的な（量子脆弱性）公開鍵暗号で保護されているユースケースについて、非常に大まかな分類を示す。

- 機密性を保護する必要がある場合、量子リスクレベルは中または高である。
- 機密性を長期間（少なくとも 10 年以上）保護する必要があり、10 年以上経過した後でも攻撃が重大な影響を与える場合、量子リスクレベルは高い。
- 移行に要する労力が大きい（8 年以上かかる）場合、量子リスクレベルは中または高となる。
- 移行の労力が高く（8 年以上かかる）、攻撃のインパクトが大きい場合（例えば、ソフトウェアのアップデートの安全性確保など）、量子リスクレベルは高い。

2 つ目の例は、推奨されるタイムラインと合わせて、長期的な機密性を保護する必要がある場合、PQC 移行をできるだけ早く、遅くとも 2030 年末までに完了させる必要があることを示唆している。最後の例は、ソフトウェアやファームウェアのアップデートを量子安全署名で早急に保護する必要性を強調するものであり、これは推奨されるタイムラインにも反映されている。

6 PQC 移行に向けたステップ

6.1 序論

本節では、「スコープと定義」で述べたように、PQC ロードマップの作成に着手するための「後悔しない」 推奨ステップを説明し、加盟国は今すぐ行動を開始すべきであることを再度強調する。後悔しない」動きは、全体的なサイバーセキュリティ成熟度の改善と、NIS2 指令[2]のようなサイバーセキュリティ規制への準拠を支援する。複雑で大規模であることに加え、多くの不確定要素や急速な進展があるため、どの事業体や加盟国もこの移行を単独で行うことはできないし、行うべきでもない。

6.2 最初のステップ

- **利害関係者の識別と関与。**移行の範囲が広く複雑であるため、重要な（各国の）利害関係者を最初から関与させることが不可欠であり、彼らの戦略的助言を組織的に管理しなければならない。検討すべきステークホルダーには、各省庁、大規模政府機関、その他の重要事業体の CTO、CISO、CIO 機能、PQC の開発に関係する科学・研究機関の代表者などが含まれる。さらに関連する利害関係者としては、例えば、国家サイバーセキュリティ当局、サイバーセキュリティ法（CSA）[21]の文脈における国家サイバーセキュリティ認証局（NCCA）、国家調整センター（NCC）などが挙げられる。また、NIS2 や eIDAS などの監督団体を関与させ、重要インフラのすべてのプロバイダだけでなく、地方 自治体や地方自治体間の緊密な協力を可能にすることも重要である。戦略的事項に関する助言は、PQC への移行のための国内ロードマップの策定と、このロードマップの実施にとって重要である。利害関係者は、国内の PQC ロードマップを担当する団体または組織と緊密に協力すべきである。実例として、フランスでは、市場の準備状況を判断し、PQC 移行の障害を特定し、プロバイダ、ユーザー、コンサル ティング会社という 3 種類の利害関係者のニーズを知るための調査を実施した[22]。

- **成熟した暗号資産管理のサポート。**すべての事業体にとって最初の必須ステップであり、「後悔しない」行動であるのは、 資産管理の一環として、暗号処理を実行する資産および暗号処理が実行される資産の現在のインベントリを作成し、維持することである。このようなインベントリは、量子的脅威に関連するだけでなく、IT 全般統制の一環としてインシデントや脆弱性管理をサポートする。このようなインベントリは、オンプレミスとクラウドの両方で、それらが使用されているプロセスやサービスの信頼性と継続性をサポートする。加盟国は、有用な暗号インベントリが作成・維持されていることを促進・支援すべきである。暗号インベントリの保管に関する規制要件はすでにいくつか存在するが、PQC 移行に関連する情報を盛り込んで修正する必要があるかもしれない。 暗号インベントリの生成および維持は、ツール（ディスカバリツールおよび資産管理ツール）によって支援することができる。暗号インベントリには、CBOM（Cryptographic Bill of Materials、SBOM 標準の拡張）のような標準化された形式を使用することを推奨する。

- **依存関係マップの作成。**事業体は、アプリケーション、製品、プラットフォーム、業務の依存関係をマッピングし、内部依存関係とサードパーティ依存関係の両方に目を向けるべきである。この依存関係のマッピングは、最終的にはサプライチェーンの依存関係によって推進される。これは、移行の制約を特定し、効率的な計画を設計するのに役立つ。これは、サプライチェーンと完全な資産ライフサイクルとの整合性をサポートします。優先順位付けとプランニングに不可欠な情報は、このステップを経て初めてプロバイダに提供される。このような依存関係の分析に関するガイダンスとその例は、[12]に記載されている。マッピング活動により、EU レベルでの相互運用性のための調整を開始する観点から、国境を越えたサービスの提供を可能にするアプリケーションとプラットフォームの相互依存関係を特定することも可能になる。

- **量子リスク分析の実施。**加盟国は、公共行政機関やその他の重要インフラ（特に NIS 2 指令の適用事業体）に対し、暗号に対する量子の脅威をトップレベルのリスクマネジメントに含めるよう奨励すべきである。これにより、脅威とリスクは取締役会レベルで議論され、評価されることになる。加盟国がサイバーセキュリティの脅威やリスクに関する国内報告書（年次報告書など）を公表しており、それを組織が参照できる場合は、この報告書に暗号に対する量子の脅威に関する情報を含めることを強く推奨する。

- **サプライチェーンを含める。**すべての組織は、製品やサービスのサプライヤーとの対話を開始する必要がある。サプライヤは、PQC と暗号のアジリティ（「次のステップ」の該当項目も参照）を製品・サービスのロードマップ開発に統合する必要があり、国内および EU 全体で PQC ロードマップとの整合性を模索する必要がある。

- **全国的な意識向上とコミュニケーション・プログラムを作成する。**すべての関連組織や事業体は、公開鍵暗号に対する量子コンピュータの脅威と、今すぐ準備を始める緊急性を認識しなければならない。これを支援するために、意識向上とコミュニケーション・プログラムを策定する必要がある。この意識向上プログラムには、取締役会や経営陣、C レベル、IT や OT に関連する人材（開発者、システム管理者、IT やエンタープライズアーキテクトなど）など、この移行に役割を果たすすべての人材や利害関係者が含まれる可能性が高い。このようなプログラムでは、以下を考慮する必要がある：

  - **カスタマイズされた認識。**移行における利害関係者の役割はそれぞれ異なるため、脅威がそれぞれの責任や業務に与える影響も異なる。そのため、一律の啓発アプローチでは不十分である。一般的な序論をプロバイダに提供することは可能だが、すべての利害関係者が日常業務に沿ったメッセージを受け取れるよう、それぞれの専門用語を用いてコミュニケーションをとることが不可欠である。また、、すべての利害関係者に知らせるだけでなく、彼らの懸念やニーズについても話し合うことが推奨される。開発は日進月歩で進んでいるため、利害関係者に対する意識向上プログラムとキーメッセージを定期的に更新する必要がある。

  - **コミュニケーション手段。**必要な意識レベルに到達し、それを維持するためには、啓発活動だけでは不十分である。意識を高め、適切な危機感を醸成するために、さまざまなコミュニケーション手段を用いるべきである。様々な事業体からのガイドラインの発行や更新、主な利害関係者からの助言、PQC の国内・国際イベントなど、認知度の高いプラットフォームで関連情報を公表することが推奨される。認知度向上プログラムでは、ソーシャルメディアや専門誌を通じたコミュニケーション、影響力のあるカンファレンスやイベントにおける政治家やトップレベルの経営陣からの重要なメッセージも考慮に入れるべきである。

- **知識を共有し、PQC に関する NIS CG のワークストリームに参加する。**複雑で規模が大きく、多くの不確定要素や急速な発展があるため、どの事業体や加盟国も単独でこの移行を行うことはできないし、行うべきでもない。サイバー空間では、すべての国が国境を越えてつながっており、この移行においても互いに依存している。従って、加盟国は、組織、事業体、利害関係者が知識や経験を共有できる環境やコミュニティを作るべきである。また加盟国は、国境を越えたサービスが存在する場合には、他の加盟国との対話の機会を設けるべきである。これらのサービスには、関係加盟国によって合意される必要のある同期化された移行（計画）が必要である。さらに、各加盟国が PQC 分野の標準化活動をフォローし、PQC に関する NIS CG のワークストリームに積極的に参加することを強く推奨する。これは、EU 全体における PQC 移行の同期化に役立つだけでなく、各加盟国が量子安全に間に合うよう準備態勢を整えることにもつながる。

- **タイムラインと実施計画を策定する。**加盟国は、国別ロードマップの優先順位を定め、その優先順位に沿った実施計画を策定すべきである。これにより、推奨されるタイムラインの主要なマイルストーンを反映しつ

つ、各加盟国の個別の状況も考慮したタイムラインを策定することができる。このような計画には、3 つのハイレベルなステップを含めることが有効である：「準備」、「計画」、「行動」である。ただし、これらは PQC 移行の 3 つの連続した段階ではなく、個々のユースケースごとに異なるスケジュールに従うことに留意すべきである。

6.3 次のステップ

ファーストステップの作業が開始され、初期の導入計画が確立された後は、円滑な移行のため の活動を追求し、導入計画の微調整と更新を継続的に行うことが重 要である。このプロセスで考慮すべきさらなる行動を以下に挙げる。

ファーストステップの完了や 2026 年末を待たず、できるだけ早く以下のステップを検討することをお勧めする。例えば、トラストサービス・プロバイダのシステムへの統合、顧客の移行、適合性評価・監督の実施を可能にするために、PQC を含む認証された適格電子署名作成デバイスが利用可能でなければならない。

- **暗号の俊敏性と量子安全アップグレードパスをサポートする。**新製品を開発する際には、まず暗号アジリティのサポートを検討すべきである。そして、2027 年 12 月以降、CRA に従って体系的に実施する必要がある。この文脈での重要な例として、量子安全なアップグレードパスを提供することが挙げられる。つまり、輸入事業者が PQC に完全に移行していない場合でも、ソフトウェアやファームウェアのアップグレードルーチンは量子 安全な署名を使用する必要がある。これにより、量子の脅威が差し迫ったときに、製品を安全に PQC にアップグレードすることができる。これは、製品で使用される暗号メカニズムが更新可能であることを前提とするものであり、暗号の俊敏性の基本要件である。さらに、標準化された耐量子署名方式の展開が強く推奨される。PQC 移行ハンドブック[17]には、暗号アジリティに関する詳細な情報が記載されている。すべての利害関係者およびベンダーとの対話を継続すべきである。これによって、移行計画が繰り返し改善されることになる。暗号アジリティについては、すべての利害関係者と議論し、最初の段階が完了した時点、ま たは成熟した事業体についてはより早い段階で、国家調達プロセスにおいて検討すべきである。また、NIS2 適合性の評価に暗号アジリティを含めることを検討してもよい。

- **移行のためのリソースの割り当て。**PQC 移行には予算や人員といったリソースが確実に必要であるため、加盟国はあらゆるレベルで適切なリソースを見積もり、確実に割り当てるべきである。さらに、組織は、ライフサイクル管理において予算を確保するよう奨励されるべきである。

- **認証制度の適応。**国内及び欧州のサイバーセキュリティ認証制度（CSA に従って採択されたもの）を含む認証制度は、量子コンピュータがもたらす脅威を考慮すべきである。この領域における既存の作業には、共通規準（EUCC）に基づく EU サイバーセキュリティ認証スキームにおける IT 製品のセキュリティ認証に適用される European Cybersecurity Certification Group Agreed Cryptographic Mechanisms 文書[23]が含まれる。特に、この文書のバージョン 2 には、PQC のアルゴリズム勧告が含まれている。一般に、認証分野の関係者、特に欧州サイバーセキュリティ認証グループ（European Cybersecurity Certification Group）は、PQC 移行に協議し、関与する必要がある。並行して、CRA は、製品に PQC を統合するための対話を開始できるようにすべきである。PQC 対策を製品に課すことで、EU は量子の脅威に対応する産業供給を確保する。加盟国はまた、規制事業体にとっての量子の脅威の意味を理解するために、CRA 市場監視当局だけでなく、NIS2 や eIDAS 監督団体との接続も検討すべきである。

- **ルールを進化させる。**加盟国には、技術的な要件を盛り込んだ国内法／規制（または各国当局による暗号化勧告）が存在する可能性がある。初期の複雑な作業は、これらの規制や暗号ポリシーを特定し、PQC のための最新勧告を体系的に更新することである。このような規制や暗号ポリシーが存在しない場合、加盟国は、他国や NIS CG に相談するなどして、その作成を検討すべきである。大量導入には、製品の入手可能性と、機構による模範の両方が必要である。加盟国は、将来の国内調達プロセスにおいて PQC 要件の統合を開始することを検討すべきであり、現在の IT サプライヤーと接触し、PQC に関する成熟度を評価することが奨励される。通常、国家調達が一定レベルのアセスメント（認証など）を必要とする場合、新たな認証発行の潜在的なニーズを評価し、評価センターと協力してそれらを構築し、業界とともに PQC 製品が利用可能になるまでのスケジュールを確立する必要がある。

- **エコシステム内の機会を探す。**ファーストステップで概説したように、利害関係者を結びつけることが、円滑でグローバルな移行の鍵となる。特に

  - **民間セクターとの関係：**加盟国は、製品サプライヤーや、移行のためのコンサルティング・サービスを提供するサービス・プロバイダと移行計画について議論し、彼らが提供するサービスの移行を計画できるようにする必要がある（ハイブリッド・メカニズムや暗号の俊敏性の統合に関するアドバイスなど）。加盟国は、PQC に関する製品・サービスロードマップの策定について、加盟国ロードマップとの整合を図るため、これらの事業者との対話を開始すべきである。

  - **研修プログラム：**加盟国は、PQC に関する情報とともにそれらを強化するために、自国における PQC およびサイバーセキュリティ／暗号技術全般に関する既存の研修プログラムを特定すべきである。加盟国はまた、このプロセスにおいて研修を支援するための情報基盤を作成することも検討できる。研修は特定の対象者向けに調整されるべきであり、加盟国は互いの経験や教育の機会を共有すべきである。

  - **資金援助プログラム：**加盟国は、PQC マイグレーション関連の活動（資産目録、PQC 製品の強化、マイグレーション・サービスの構築、ユーザー導入の促進など）を国の資金プログラムに組み込むことを検討すべきである。加盟国はまた、ナショナル・コーディネーション・センター（NCC）および各国の欧州サイバーセキュリティ・コンピテンス・センター（ECCC）ガバナンス・ボード・メンバーとの対話を開始し、既存の欧州の資金提供機会についてさらに学び、将来の資金提供機会を定義するために有益な意見を共有すべきである。加盟国は、既存の資金提供プロジェクト（国内および欧州）とその状況についてフィードバックを求め、それが自国のロードマップにどのように役立つかを確認する。

- **ロードマップの作成と実施を通じて、横断的な活動を含める。**秩序ある移行には国際標準が不可欠であり、PQC の標準化作業は世界および欧州で進められている。加盟国当局がすでに標準化委員会に参加している場合は、PQC 標準化ワーキンググループへの参加と支援の可能性を評価すべきである。そうでない場合は、他の事業体（国内または NIS CG を通じて他の加盟国）と連携し、進行中の作業について詳しく知り、投資を決定することもできる。さらに、PQC と量子コンピューティングは依然として非常に活発な研究分野である。加盟国は引き続きこの研究を支援するとともに、これらのトピックに関する関連情報源を特定・追跡し、NIS CG と共有することで、加盟国全員が関連する質の高い情報を入手できるようにすべきである。加盟国はまた、共同研究プログラムや共同博士課程などを通じて、研究や教育訓練に協力することも奨励される。

- **試験的なユースケースを実施し、テストセンターに貢献する。**EU 全域における PQC の円滑な移行を支援するため、加盟国は、PQC ソリューションの相互運用性をテストするための国際協力を推進すべき

である。移行のために実施される手段をさらに推し進めるために、加盟国は、国内専門知識センターの設立を検討することができ、事業体は、デジタル欧州プログラムの下で資金提供される EU の試験インフラを利用することが奨励される。例えば、ETSI Plugtests や IETF PQC hackathon のように、実世界のシナリオを表す具体的なユースケースに取り組むことが奨励される。各国の専門家センターと EU の試験インフラは、実際の PQC 実装における脅威モデルと対策の実装を改良することを可能にする。この専門知識センターはまた、多くのソリューションの相互運用性を実際の条件下で評価し、実装前の概念実証を促進するための試験インフラを提供することもできる。

7 EU にできること

EU は、PQC への移行を促進するための包括的アプローチを実施している。加盟国、産業界、学識経験者との積極的な協議に加え、欧州委員会は、デジタル・ヨーロッパ・プログラムおよびホライゾン・ヨーロッパ・プログラムの下での活動を通じて、PQC に関する支援策を策定している。欧州委員会は国際政治レベルでの議論にも関与し、2024 年 4 月 11 日に「耐量子暗号への移行のための協調的実施ロードマップに関する勧告」を策定、採択した。EU は、欧州委員会および ENISA を通じて、PQC ロードマップと、PQC メカニズムおよびその評価に関する勧告を策定するために ECCG の下で行われている活動との橋渡しを行う。また、欧州委員会と ENISA は、PQC への移行を促進するベストプラクティス、手法、ツールに関する加盟国間の相互共有を支援することもできる。

参考文献

[1] 欧州委員会耐量子暗号への移行のための協調実施ロードマップに関する勧告（EU）2024/1101。2024.URL: https://eur-lex.europa.eu/eli/reco/2024/1101/oj.

[2] 欧州議会および理事会。規則（EU）No 910/2014 および指令（EU）2018/1972 を改正し、指令（EU）2016/1148 を廃止する、欧州連合全体で高 い共通レベルのサイバーセキュリティ対策に関する指令（EU）2022/2555（NIS 2 指令）。2022.URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

[3] 今日、明日を確保する：耐量子暗号への移行。2024.[Accessed 23.01.2025].URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/.

[4] 欧州議会と理事会.Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.2022.URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.

[5] 欧州議会および理事会.デジタル要素を含む製品に対するサイバーセキュリティの水平的要件と、規則（EU）No 168/2013 および（EU）2019/1020、指令（EU）2020/1828 の改正に関する指令（EU）2024/2847（サイバーレジリエンス法）。2024.URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[6] AIVD。量子コンピュータの情報化。2014.[Accessed 31.01.2025].URL: https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2014/11/20/

[7] BSI.研究：量子コンピュータの開発状況、バージョン 2.1。2024.[Accessed 30.01.2025].URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.html.

[8] グローバルリスク機構.Quantum Threat Timeline Report 2024.2024.[Accessed 31.01.2025].URL: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/.

[9] ANSSI.耐量子暗号移行に関する ANSSI の見解。2022.[Accessed 31.01.2025].URL: https://cyber.gouv.fr/sites/default/files/document/EN_Position.pdf.

[10] ANSSI.耐量子暗号移行に関する ANSSI の見解（2023 年フォローアップ）.2023.[Accessed 31.01.2025].URL: https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf.

[11] BSI.量子安全暗号 - 基礎、現在の開発、および推奨事項。2021.[Accessed 31.01.2025].URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html.

[12] ETSI.ETSI TR 104 016 V1.1.1 (2024-10), CYBER; a Repeatable Framework for Quantum-Safe Migrations.2024.2024 年。[2025.01.31 アクセス].URL: https://www.etsi.org/deliver/etsi_tr/104000_104099/104016/01.01.01_60/tr_104016v010101p.pdf.

[13] DGX WG on Cyber Security.耐量子暗号移行は今日から始まる.2024.[Accessed 30.01.2025].URL: https://www.tech.gov.sg/files/media/Reports/DGX_2024_Cyber_Working_Group_Report.pdf.

[14] NIST.Nist SP 1800-38A (初期ドラフト) - Migration to Post-Quantum Cryptography : 量子安全暗号の実装と採用を検討するための準備。2023.[Accessed 31.01.2025].URL: https://www.nccoe.nist.gov/sites/default/files/2023-04/pqc-migration-nist-sp-1800-38a-preliminary-draft.pdf.

[15] NIST.Nist SP 1800-38B（初期ドラフト）-ポスト量子暗号への移行：暗号発見。2023.[Accessed 31.01.2025].URL: https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf.

[16] NIST.Nist SP 1800-38C (初期ドラフト) - 耐量子暗号への移行：ドラフト標準のテスト。2023.[Accessed 31.01.2025].URL: https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf.

[17] TNO AIVD, CWI.PQC 移行ハンドブック、改訂増補第 2 版。2024.[Accessed 30.04.2025].URL: https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf.

[18] NIST.NIST IR 8547（初期公開ドラフト）、耐量子暗号標準への移行 - csrc.nist.gov.2024.URL: https://doi.org/10.6028/NIST.IR.8547.ipd.

[19] 英国 NCSC.ポスト量子暗号への移行スケジュール。[Accessed 21.03.2025].URL: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines.

[20] BSI.BSI-Standard 200-3: IT-Grundschutz に基づくリスク分析.2017.[Accessed 04.02.2025].URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html.

[21] 欧州議会および理事会.Regulation (EU) 2019/881 (Cybersecurity Act) on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (eu) No 526/2013.2019.URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

[22] ANSSI.L'ANSSI partage deux études de marché sur la cryptographie post-quantique menesuprès de l'écosystème.2024.[Accessed 30.04.2025].URL: https://cyber.gouv.fr/actualites/lanssi-partage-deux-etudes-de-marche-sur-la-cryptographie-post-quantique-menees-aupres.

[23] 暗号に関する ECCG サブグループ。合意された暗号メカニズム - バージョン 2.URL: https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.