耐量子暗号（PQC）移行ロードマップ

2025 年 5 月

©2025 The MITRE Corporation.無断複写･転載を禁ずる。 一般公開を承認。 無制限配布 24-03931-7.

目次

背景 3

マイグレーション概要 3

カテゴリー1：準備 5

活動 1.1：PQC の関連性を識別する 5
活動 1.2：PQC 移行を管理するリーダーを任命する 6
活動 1.3：既存のインベントリーの識別と認識 6
活動 1.4：ステークホルダーの識別と戦略的メッセージの開発 7

活動 1.4 a：システムベンダーおよびオペレーターとの連携を開始する。 8

カテゴリー2：ベースラインの理解 9

活動 2.1：ディスカバリープランと予算を決める 9
活動 2.2：PQC 移行のためのインベントリーを構築する 9

活動 2.2 a：棚卸に使用するツールと方法を検討する 10
活動 2.2 b: 暗号資産に関する情報の収集と分類 10

活動 2.3：移行のための重要資産の優先順位付け 10

カテゴリー3：計画と実行 12

活動 3.1：移行計画と予算を設定する 12
活動 3.2：解決策を識別する 12

活動 3.2 a：ベンダーと移行ニーズを確認する 13
活動 3.2 b: ソリューションの構築 14

活動 3.3：短期的対策を確立する 14
活動 3.4：PQC ソリューションを獲得／開発する 15
活動 3.5：PQC ソリューションの導入 15

カテゴリー4：モニタリングと評価 16

活動 4.1：妥当性の確認 16

活動 4.1 a：業界標準との整合性確保 16

活動 4.2：PQC 移行の成功を追跡するための指標を作成する 17
活動 4.3：労働力ニーズのアセスメント 17
活動 4.4：継続的なモニタリングと更新 18

結論 19
参考文献 20

背景

先進的な量子コンピュータの開発競争におけるブレークスルーは、通信の安全確保、認証の確保、機密データの保護といった現在のシステムを脅かし、耐量子暗号（PQC）への移行を必要としている。現在の暗号セキュリティーを突破できる暗号関連量子コンピューター（CRQC）の開発には、あと 10 年から 20 年かかるかもしれないが、計画と実装を成功させるためには、今すぐ移行プロセスを開始する必要がある。PQC への移行を開始することで、敵対者が後で解読するために今データを収集するという脅威も緩和される。

この移行ロードマップは、組織がポスト量子への移行を計画し、実施するためのガイドとして書かれたもので、PQC への移行を進めるための 4 つの主要カテゴリー（(1)準備、(2)ベースラインの理解、(3)計画と実行、(4)）の概要を示している。

モニタリングと評価さらに、各カテゴリーとそれに関連する活動について、望ましい成果を挙げており、このロードマップに概説されているプロセスを通じて、組織がどの段階にあるべきかを知ることができる。

マイグレーション概要

組織全体における PQC への移行は、主に 4 つのカテゴリーに分けることができる。 これらのカテゴリーに付随して、PQC への移行を進展させ、維持するために組織が取るべき活動がある。カテゴリーと活動の実施方法は組織によって異なり、図 1 に見られるように、このロードマップの構成要素は、同時に実施することも、順序をずらして実施することもできる。

カテゴリー1：準備

組織は、PQC 移行の目的の概要を把握し、移行リーダーを任命し、必要な利害関係者を特定し、戦略的メッセージを通じて利害関係者を調整することによって、PQC への移行を準備する。

カテゴリー2：ベースラインの理解

組織は、データインベントリ、優先的に更新すべき資産、必要なリソースと利用可能な予算について、基本的な理解を深める。

カテゴリー3：計画と実行

あなたの組織は、システムベンダーや社内のシステム所有者と協力して、耐量子ソリューションが外部から取得され、または社内で開発され、効果的に実装されるようにする。

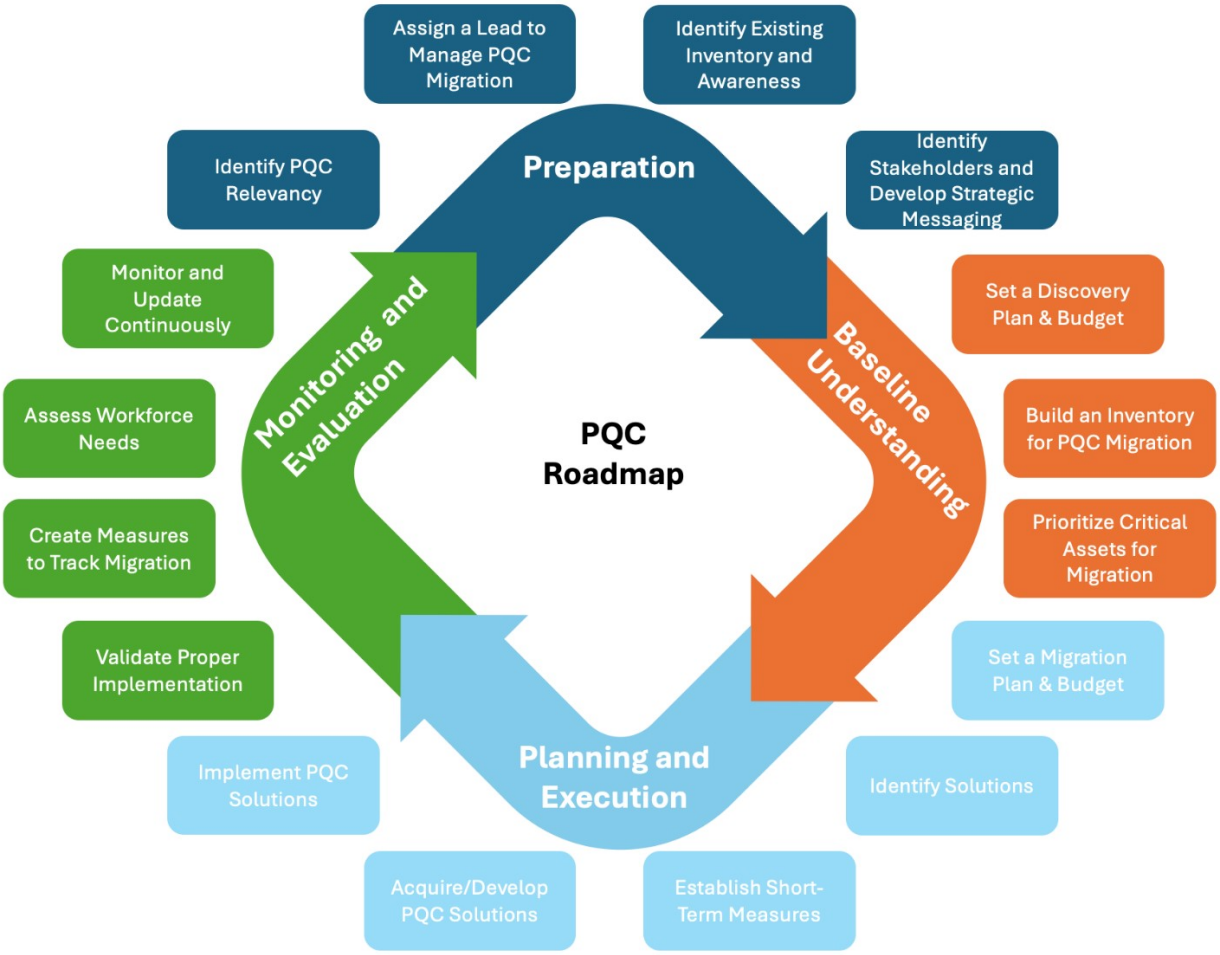
カテゴリー4：モニタリングと評価

貴組織は、移行プロセスを追跡するための手段を開発し、量子機能の進化に応じて暗号セキュリティを再評価するプロセスを策定する。

推奨ロードマップ

組織がこのロードマップをどのように適用するかは、その組織の重要なデータの保存期間と量、その資産に関する利用可能な情報の量、潜在的に重要なソフトウェアとハードウェアの更新のための予算、その他多くの影響要因に依存する。カテゴリーと活動の実施方法は組織によって異なり、同時、連続、または個別に実施される。

図 1.PQC ロードマップのカテゴリー。



カテゴリー1：準備

PQC 移行の準備カテゴリーでは、組織は、PQC 移行の目的の概要を把握し、移行のリーダーを任命し、必要な利害関係者を特定し、戦略的メッセージを通じて利害関係者を調整することによって、準備を整える。

カテゴリー1 の成果：

- 組織は、自社の脆弱性とその緊急度を熟知し、PQC 移行を開始する適切なスケジュールを決定する。
- 組織は、PQC 移行の進行を担当する移行リーダーを割り当てる。
- 組織は、既存のインベントリーと PQC 意識を識別する。
- 組織は、戦略的メッセージを活用しながら、主要な利害関係者を特定し、PQC 移行のニーズと整合させる。
- 組織は、PQC ソリューションのための最初のベンダーとの契約を開始する。

活動 1.1：PQC の関連性を識別する

PQC 移行に着手する前に、組織はこのプロセスを今すぐ開始すべきか、それとも時期を遅らせるべきかをアセスメントする必要がある。組織の PQC 移行の適切なタイムラインを決定するには、移行、情報の保存期間、脅威のタイムラインを見積もる必要がある。以下の図 2 に見られるように、機密情報の保存期間は PQC 導入の緊急性に影響を与える可能性がある。組織が「今すぐ収穫し、後で復号化する」という脅威に直面しているかどうかにかかわらず、CRQC の登場によって生じる完全性と認証の脅威から重要な情報を保護するための準備を整えておく必要がある。

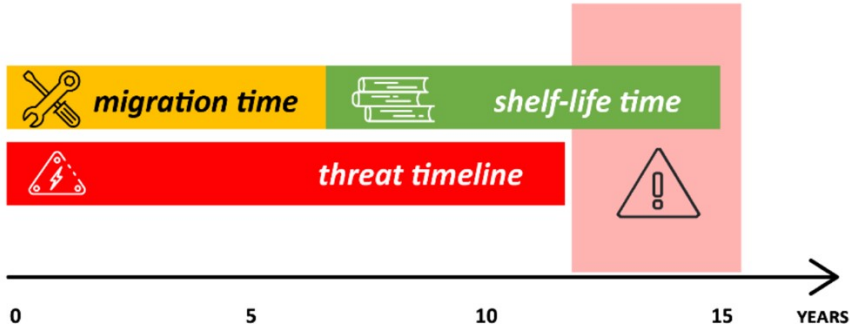


図 2.PQC 移行の緊急性を決定するためのモデル･タイムライン（量子準備作業部会）。

PQC 移行の行程において組織が必要とする一般的な関与のレベルを理解するためには、PQC 移行の目的を決定する必要がある。これにより、まず、データおよび資産の保護に関して、どの程度のリスクを取る意思があるかが明確になる。組織の移行目的を決定するために、以下のような特徴を考慮することができる：

- 組織の攻撃対象領域
- システムの種類と故障の可能性
- 取り扱うデータの重要性と機密性
- 移住の緊急性
- 交換または移行される資産の予想寿命
- 他組織との相互依存

あなたの組織は、緊急採用企業か通常採用企業のどちらかになるだろう。緊急導入企業は、機密性の高いデータや資産を扱い、セキュリティ侵害によって重要なインフラが危険にさらされたり、機密性の高い個人データや組織データが流出したりする可能性がある。レギュラー・アダプターは、緊急アダプターに該当しない組織である。通常の導入企業は、データの保存やシステムの運用を行う可能性があるが、Store-now-Decrypt-later スキームのリスクは低い。

活動 1.1 成果：

- 組織は PQC 移行の目的を明確にし、PQC 移行を開始する適切なスケジュールを決定する。
- 組織は、自社の脆弱性とその緊急度を熟知している。

活動 1.2：PQC 移行を管理するリーダーを任命する

組織が PQC 移行のスケジュールを開始することを決定したら、PQC 移行をモニタリングし進行させる個人またはチーム（「移行リーダー」）を任命すべきである。この役割の責任は、個々の組織に固有であるが、タイムフレームの設定、ベンダーへの連絡、その他の移行実施業務などが含まれる。結局のところ、PQC 移行には、様々な指導的役割や技術的役割との積極的な連携が必要であるため、移行リーダーは、組織内外の様々な分野を横断できるような立場にあるべきである。

活動 1.2 成果：

- 組織は、移行リーダーに期待される役割と成果を定義する。
- 組織は、PQC 移行の進行を担当する移行リーダーを割り当てる。

活動 1.3：既存のインベントリーの識別と認識

この活動では、移行リーダーは、組織の暗号化ニーズに関する基本的な理解 を収集するための計画を設定する。これには、すでに利用可能なインベントリを特定すること、現在どのような移行の取り組みが行われているかを判断すること、組織の移行態勢を全体的に把握することなどが含まれる。組織は、どのようなインベントリ、リスクアセスメント、暗号部品表（CBOM） をすでに保有しているかを確認する。組織は、異なる時点で特定の要件を満たすように設計された複数のインベントリやリスクアセスメントを持っている可能性がある。既存のインベントリやリスクアセスメントを調査する際には、データや資産の所在、所有者や運用者、作成理由、使用方法を

文書化する。組織が現在持っている（あるいは持っていない）情報を文書化することは、移行担当者が早い段階でニーズを明確にし、不必要なコストや労力を避けるのに役立つ。

活動 1.3 成果：

- 移行リーダーは、PQC 移行に関連する既存のインベントリ、リスクアセスメント、および認識を評価し、文書化した。

関連活動： 2.2, 2.3

活動 1.4：ステークホルダーの識別と戦略的メッセージの開発

このロードマップの活動を達成するために重要なことは、組織のリーダーと主要な利害関係者に PQC 移行の価値と目的を理解してもらうことである。このため、移行の主導者は、(1)利害関係者の識別と調整、(2)PQC 移行のプロセスと必要性のコミュニケーショ ンを行う、組織に特化したコミュニケーション計画を策定する必要がある。この活動には、組織の現在の移行の状況を把握するために、システムオペレーターやベンダーと最初に関わることも含まれる。戦略的メッセージを作成する際に考慮すべき質問には、以下のようなものがある：

- 組織を PQC に移行する価値／投資収益率（ROI）はどの程度か？
- PQC の移行を早急に開始する必要があるか？
- PQC 導入の影響をどのように測定できるのか？
- PQC の移行は、財政的、経営的に我々に何を要求するのか？

ステークホルダーとは、組織の PQC 移行に依存し、それを支援し、またはそれによって利益を得ることができる人々のことである。利害関係者の期待を理解することには、利害関係者が他の利害関係者にどのような影響を与えうるか、また与えるかを理解することも含まれる。 利害関係者の意見に耳を傾け、その意見を活用して継続的な改善と満足度の向上を推進することが、PQC 移行の進展に対する利害関係者のコミットメントを継続的に高める方法である。

戦略的メッセージの中で、組織は、PQC 移行の目的と範囲の概要を示すポジショニング・ステートメントを検討するとよい。また、ステークホルダーが PQC に移行することに懸念を抱いている可能性を予測し、ステークホルダーの理解を深め、組織の PQC の目標との整合性を高めるのに役立つ対応メッセージのドラフトを作成することも考えられる。さらに、組織内外の利害関係者に PQC 移行の価値を簡潔に伝えるためのエレベーターピッチをドラフトすることもできる。利害関係者の参画と戦略的メッセージングは、組織の PQC 移行の全体にわたって行われるため、利害関係者の活動に対する戦略的メッセージングの影響を追跡するための測定方法も確立しておきたい。

活動 1.4 成果：

- 組織は、主要な利害関係者を特定し、PQC 移行のカテゴリーと活動に整合させる。
- 組織は、利害関係者のエコシステム全体で、PQC 移行の価値と目的を明確に伝えることができる。

活動 1.4 a：システムベンダーおよびオペレーターとの連携を開始する。

組織の主要な利害関係者の関与には、移行ニーズの範囲を広げるために、ベンダーや社内のシステムオペレーターとの最初の会話が含まれる。 組織として事前に聞いておきたい質問には、次のようなものがある：

- ベンダーの PQC ソリューションはいつ利用可能になるのか？
- 社内開発システム向けの PQC ソリューションはいつ利用可能になるのか？
- PQC の更新にはハードウェアやソフトウェアの導入が必要か？
- 新たなソリューションのコストはどのくらいか？
- 導入努力によって予想されるビジネス・影響は何か？
- CBOM はソリューションに含まれるのか？
- 暗号化されたアジャイル・ソリューションの現状はどうなっているのか？

活動 1.4 (a) 成果：

- 組織がまだベンダーと定期的な取引を行っていない場合は、それを確立する。
- ベンダーと社内オペレーターは、PQC ソリューションが利用可能になるまでのスケジュール、および導入コストとその影響の見積もりを提供する。

カテゴリー2：ベースラインの理解

2 つ目のカテゴリーでは、移行担当者は、データインベントリ、優先的に更新すべき資産、ディスカバリーイニシアチブに必要なリソースと利用可能な予算について、基本的な理解を深める。

カテゴリー2 の成果：

- 組織は、追加の棚卸しや優先順位付けの必要性を判断する。
- 組織は、希望するレベルの PQC レジリエンスを達成するために必要なすべての暗号資産を識別し、文書化している。
- 組織は、機密性と寿命に基づいて、インベントリ・リストの資産に優先順位をつける。

活動 2.1：ディスカバリープランと予算を決める

この活動では、移行リーダーは、収集した初期情報（活動 1.3）を利用し て、組織がインベントリの作成と資産の優先順位付けを行うために、 追加の対策を進めるべきかどうかを判断する。既に入手可能な情報を活用し、移行リードは、追加的なインベントリ作成の取り組みが必要か（活動 2.2）、または組織が資産の優先順位付けに直接進むことができるか（活動 2.3）を決定する。移行リードは、インベントリ作成、資産の優先順位付け、およびその他の発見イニシアティブのために利用可能な予算を決定することもできる。

活動 2.1 成果：

- 移行の主導者は、PQC 移行のためにどのような目録作成と優先順位付けの作業が必要かを特定する。
- 移行の主導者は、発見のためのイニシアチブの予算を特定する。

関連する活動 1.3, 2.2, 2.3

活動 2.2：PQC 移行のためのインベントリーを構築する

一元化されたインベントリは、エンタープライズ・レベルの移行スケジュールを追跡し、すべてのセキュリティ・ギャップに対処するための包括的な計画を確保するために不可欠である。資産と暗号使用の明確なインベントリを構築することで、組織は積極的に課題を特定し、PQC 要件の計画における俊敏性を確保することができる。
PQC 移行を効果的に計画するために、移行リーダーはシステムオペレータと協力して以下を行う：

- インベントリ作成に使用するツールと方法を決定する
- 最も重要な輸入事業者の情報を文書化する
- 在庫を分類する

以下の小活動（活動 2.2 (a)および(b)）は、時系列的なものではないが、インベントリ作成のプロセス全体を通して考慮すべき事項である。

活動 2.2 成果：

- 組織は、資産および暗号使用の目録を文書化する。

関連項目：2.2 (a), 2.2 (b)

活動 2.2 a：棚卸に使用するツールと方法を検討する

あなたの組織は、ハードウェア、ソフトウェア・モジュール、ライブラリ、組み込みコードなど、エ ンタープライズ・インフラストラクチャのさまざまなコンポーネントにわたって暗号化アルゴリズ ムを識別するための自動化ツールの使用を検討するとよいだろう。これらのツールは、暗号的に保護された情報を保護し、アクセスを管理するために重要な暗号鍵の確立と管理に使用されるアルゴリズムも特定する必要がある。さらに、自動化ツールは、静止時、転送時、使用時のデータの完全性を確保し、データのソースとコンテンツの両方を保護するアルゴリズムを特定する必要がある。ツールや方法を選択する際には、組織の許容リスクレベルを考慮する。

活動 2.2 (a) 成果：

- 移行リードと技術チームは、組織のインベントリを収集するためにどの方法とツールが最適かを特定する。

活動 2.2 b: 暗号資産に関する情報の収集と分類

この活動では、組織の移行リーダーとシステムオペレータが、最も重要な資産に ついて、誰が運用し、どのようなデータを保護し、どのようなアーキテクチャ設計、設 計プロトコル、インターフェースを使用しているかなど、詳細な技術情報を文書化する。また、組織が把握していないことを文書化し、オフラインの鍵、自動化ツール がアクセスできないファイル構造の鍵、不明なフォーマットの鍵など、インベントリ 内の潜在的な盲点を認識することも極めて重要である。組織がインベントリ・リストを作成する際には、活動 3.2 (a)で誰に連絡すればよいかを確実にするため、製品を供給者別に整理する。

活動 2.2 (b) 成果：

- 組織は、価値のある情報に触れるすべての暗号資産を分類したリストを持っている。
- 組織は、その資産に関する盲点や知らない情報を特定した。
- 組織は、各資産に関する連絡先を知っており、自社で実施する必要がある更新と、サプライヤーが実施する必要がある更新を認識している。

関連する活動 3.2 (a)

活動 2.3：移行のための重要資産の優先順位付け

この活動では、移行の主導者が重要な資産に優先順位を付け、その移行スケジュールを決定する。この活動では、活動 2.2 で収集した資産と暗号使用のインベントリをレビューし、その機密性と寿命を評価する。この基

礎的な理解は、どのシステムに早急な注意が必要かを優先順位付けし、将来のセキュリティニーズに対する計画を立てるのに役立つ。移行の主導者は、この活動の成果を導くために、関連するベンダーやシス テム運用者との協議を継続する。

あなたの組織は、潜在的なセキュリティリスク、運用リスク、コンプライアンスリスクをさらに特定するために、重要システムの詳細なリスクアセスメントを実施することを選択することができる。アセスメントの重要な側面は、敵対者が大規模な量子コンピュータを保有し、一部の暗号アルゴリズムが無効となるシナリオにおけるリスクを評価することである。そのため、脅威を再評価し、セキュリティを維持するために移行すべきシステムの優先順位を決める必要がある。量子リスクアセスメントを実施することで、すべてのリスク、それらのリスクを緩和するための管理策、緩和のために講じる必要のある追加措置の包括的なリストを作成することができる。

組織がリスクアセスメントを実施するかどうかにかかわらず、活動 1.1 で特定した移行、賞味期限、脅威のタイムライン（図 2 参照）を参照し、活用したい。最終的な優先順位付けされた資産リストは、推定移行時間、資産移行の緊急性、および実行可能なリスク緩和戦略を考慮したものとなる。

活動 2.3 成果：

- 組織は在庫をアセスメントし、感度と耐用年数に基づいて優先順位をつけた資産リストを作成する。
- リスクアセスメントを選択した場合、組織は、すべてのリスク、それらのリスクを緩和するために実施されている管理策、および緩和のために講じる必要のある追加措置の包括的なリストを作成する。

関連する活動 1.1, 2.2

カテゴリー3：計画と実行

このロードマップのカテゴリー3 は、組織が移行プロセスの初期段階で検討すべきハイレベルな活動に焦点を当てている。組織は、どの耐量子ソリューションをベンダーから取得するか、あるいは内部で開発するかを決定する。中長期的なリスクは、アウトオブバンドメカニズムと PQC ソリューションの実装によって緩和される。このセクションは、組織の移行プロセスに関する情報が不足しているため、意図的にあまり規定的ではない。

カテゴリー3 の成果：

- 組織は、PQC への移行を管理するための計画を策定し、どのようなシステムを取得または開発しなければならないかを決定する。
- 組織は、インフラストラクチャー全体で PQC ソリューションを導入、買収、または開発している。
- 組織は、機密データのエクスポージャーを緩和するための短期的な対策を実施する。

活動 3.1：移行計画と予算を設定する

活動 2.3 で作成した優先順位付けされた資産リストを使用して、優先順位付けされた各資産について、リスクを緩和するのか、PQC への移行を開始するのか、あるいは量子リスクを受け入れて例外を管理するのか、適切な対応策を決定する。また、資産のリスクレベルを十分に理解するために、組織のベンダーと連携することも考えられる（活動 3.2 (a)）。さらに、PQC への移行を実行するために、組織としてどのような人員の変更を実施する必要があるかについても、把握しておきたい（活動 4.3）。

移行担当者は、組織の財務チームおよびシステムオペレーターと連携して、これらの資産を PQC に移行するコストを見積もる。この活動では、優先順位をつけた資産の移行の作業内訳構造（スケジュールされたタスクと各タスクの見積もりコストを含む）を理解したい。

活動 3.1 成果：

- 組織は、優先順位を付けた資産を PQC に移行するコストを見積もり、予算計画を策定する。

関連項目： 2.3, 3.2 (a), 4.3

活動 3.2：解決策を識別する

この活動では、移行リーダーは、組織の移行ニーズに特化したソリューションを特定する。移行リーダーは、活動 2.3 で作成した優先順位付けされた資産リストを使用して、社内のシステムオペレータや保守担当者と調整する。最初の調整作業において、移行リーダーは、どのようなシステムの更新を取得しなければならないか、どのようなシステムを内部で更新しなければならないかを特定し、文書化するよう試みるべきである。さらに、移行リーダーは、どのシステムがソフトウェアの更新によって PQC に移行でき、どのシステムがハードウェアのアップグレードを必要とするかを特定するよう努めるべきである。

さらに、組織に最適な移行製品を選択する前に、現行の PQC 標準に準拠しているかどうかを確認することが重要である。現在、FIPS 203、204、205 に概説されている暗号アルゴリズムに関する NIST の標準とガイドラインに、ベンダーやシステムが合致しているかどうかを確認する。組織はまた、NIST の暗号モジュール妥当性確認プログラム（Cryptographic Module Validation Program）は、テスト可能な暗号およびセキュリティ要件のセットを使用して暗号アルゴリズムを妥当性確認し、セキュリティ評価の指標を機関に提供するものである。 最後に、この活動を通じて、組織はそのコンプライアンスを文書化すべきである。文書化することで、将来的に参照しやすくなり、重複した取り組みを防ぐことができる。

任意：この期間中、移行リーダーはハイブリッド暗号および/またはアジャイル 暗号実装の実行可能性をアセスメントすべきである。ハイブリッド暗号の実装は、移行プロセスにおけるコストを軽減し、後方互換性 と前方互換性の確保を支援する。アジャイル暗号システム／手法に投資して実装することで、コストと時間の効率的な方法で新たなセキュリティ脅威に迅速に対応する組織の能力を高めることができる。今、アジャイルなソリューションを採用することで、将来の暗号更新コストを削減し、システムの長期保守をサポートし、ベンダーロックインや時代遅れの暗号に関連するリスクを緩和することができる。

活動 3.2 成果：

- 組織はシステム／ソリューションの実施計画を作成する。
- 組織は、リスクを低減し、コンプライアンス要件を満たすために、どの脆弱性システムをアップグレードしなければならないかを決定する。
- 組織は、利用可能なソリューションが現行の PQC 標準に準拠しているかどうかを判断する。
- 組織は、機敏な暗号実装／ソリューションの必要性と要望を決定する。
- 組織は、PQC ソリューションの実施方法と予測される組織への影響をアセスメントする。

関連活動: 2.3

活動 3.2 a：ベンダーと移行ニーズを確認する

優先順位付けされた資産リストを使用して、移行リーダーは、関連する組織の取得権限者と連携して、システムベンダーとの連携を継続し、耐量子ソリューションの利用可能性を判断すべきである。 移行リードは、活動 1.4 (a)の以下の質問を確認し、再評価すべきである：

- ベンダーの PQC ソリューションはいつ利用可能になるのか？
- PQC の更新にはハードウェアやソフトウェアの導入が必要になるのか？
- 新たなソリューションのコストはどのくらいか？
- 導入努力によって予想されるビジネス・影響は何か？
- CBOM はソリューションと一緒に提供されるのか？

活動 3.2 (a) 成果：

- 組織は、商業ベンダーからどのような PQC ソリューションが入手可能かを識別する。
- 組織は、新規に取得したシステムが PQC 標準に適合するよう、取得言語と契約を更新する。
- 組織は、PQC ソリューションの利用可能なスケジュールとソリューションのコストを決定する。
- 組織はベンダーと調整し、実施プロセスにおける組織の混乱の程度を決定する。

関連する活動 1.4 (a), 2.3

活動 3.2 b: ソリューションの構築

優先順位付けされた資産リストを使用して、移行リーダーは、カスタムシステムまたは商用アップデートがまだ利用可能でないシステムのシステムオペレータと調整し、開発プロセスを開始すべきである。マイグレーションリーダーは、次のことを考慮すべきである：

- 耐量子ソリューションの開発スケジュールは？
- PQC の更新にはハードウェアやソフトウェアの導入が必要か？
- 解決策を開発するためのコストはどのくらいか？
- 商業的な解決策はあるのか？

活動 3.2 (b) 成果：

- 組織は、ニッチまたはカスタムアプリケーションのソリューションを開発するために必要なスケジュール、コスト、リソースを決定する。
- 組織は、同等の性能を提供する市販のソリューションが利用可能かどうかを判断する。

関連活動: 2.3

活動 3.3：短期的対策を確立する

ソリューションが利用可能になるまでのスケジュールと優先順位のアセスメントを利用 して、移行リーダーは、機密性の高いシステムと情報を確実に保護するために、 どのような対策を講じるべきかを決定しなければならない。さらに、「今ハーベストし、後で復号化する」攻撃を受けるリスクのあるシステムやデータについては、移行リーダーはシステム運用者／保守者と調整し、リスクを緩和するためにどのような短期的ソリューションを実施できるかをアセスメントしなければならない。これらの対策には以下が含まれる：

- 新しい証明書の寿命を縮める
- 新しく認証される鍵の長さを長くする
- 過度に長期の証明書を失効させる計画

- TLS 1.3 をサポートするように近代化する
- 長期保管データの物理的セキュリティ手順とデータアットレストの防御を 再検討する - データを保護するシステム（VPN）に追加のセキュリティレイヤーを追加することを 検討する

これらのセキュリティ対策は、量子コンピューティングの脅威に関連するリスクの緩和には役立つかもしれないが、PQC への移行の代わりにはならない。

活動 3.3 成果：

- 組織は、量子の脅威に対するリスクを緩和するための短期的な対策の必要性を判断する。
- 組織は、データのエクスポージャーを低減するためのリスク緩和戦略を策定し、実施する。

関連する活動 3.2 (a), 3.2 (b)

活動 3.4：PQC ソリューションを獲得／開発する

移行リーダーは、認可取得権限者と連携して、耐量子ソリューションの取得と、ソリューションの内部開発のためのリソースの分配を開始する。 これらの取得と開発のプロセスは、活動 2.3 で決定された資産の優先順位に従って行われる。

活動 3.4 成果：

- 組織は獲得と開発のための資源を分配する。
- 組織はベンダーから PQC ソリューションを購入する。
- 組織は PQC ソリューションの社内開発を開始する。

関連活動: 2.3

活動 3.5：PQC ソリューションの導入

組織は、短期および長期の緩和策と解決策を導入する。移行リードは、組織の混乱の程度を判断し、混乱が拡大した場合の緊急時対応 計画を作成する。組織がシステムを段階的に展開している場合、移行リードは、前方互換性と後方互換性を確保するための調整を促進する。

活動 3.5 成果：

- 組織は、買収または開発した PQC ソリューションを実施する。
- 組織は、新しいシステムの状態を反映するために在庫を更新する。

カテゴリー4：モニタリングと評価

移行プロセスを追跡し、量子機能の進化に合わせて暗号セキュリ ティを再評価するプロセスを策定する。このカテゴリーにおいて、移行のリーダーは、移行作業で作成されたすべての文書が維持されていることを確認し、将来の技術移行の可能性を支援するための継続的な評価のプロセスを作成する。

カテゴリー4 の成果：

- 組織は、ソリューションの実装と標準への準拠を妥当性確認する。
- 組織は、PQC ソリューションを利用／実施するために従業員を準備している。
- 組織は移行の進捗状況を追跡し、望ましい成果を妥当性確認する。
- 組織は、技術的発展に対してセキュリティを継続的にモニタリングするプロセスを構築する。

活動 4.1：妥当性の確認

移行リーダーは、システム実装者と協力して、実装された PQC システムの有効性を評価する。この活動において、システム運用者は、実装されたソ リューションがシステムの暗号要件および運用要件（すなわち、前後互換性）を満たしていることを確 認する。 実装の検証に成功した後、移行リードは、インベントリが新しいシステムの状態を反映するよう 更新されていることを確認する。

任意である：組織の規模や構造にもよるが、マイグレーションリーダーと組織のリーダーは、組織のマイグレーションプロセスを奨励し、迅速化するために、強制的な仕組みを導入することを選択することができる。

活動 4.1 成果：

- マイグレーション・リーダーは、優先資産の確保における PQC の有効性を評価した。
- 相互運用性と運用要件が検証され、文書化される。
- 在庫は新しいシステムの状態を反映するように更新される。

活動 4.1 a：業界標準との整合性確保

組織が扱うデータの種類によっては、PQC 移行が既存の業界規制を考慮したものであることを確認する必要がある。例えば、医療分野の組織であれば、HIPAA 標準に照らして PQC 移行を評価するかもしれないし、EU 圏内で活動する組織であれば、NIS2 コンプライアンスを認証するかもしれない。加えて、これらの標準は、将来への備えや定期的なリスクアセスメントなど、PQC に関連する活動をすでに要求している可能性があり、PQC 移行の計画を開始する説得力のある理由を提供している。全体として、現在の標準をアセスメントすると同時に、将来的な標準の変更も予測することで、脅威の状況だけでなく、規制の進展にも先手を打つことが可能になる。

活動 4.1 (a) 成果：

- 組織は、既存の業界標準を PQC 移行計画に統合する。
- 組織は、自社の PQC 移行が業界標準にどのように準拠しているかを文書化する。

活動 4.2：PQC 移行の成功を追跡するための指標を作成する

組織の PQC 移行の影響を知る上で重要なのは、暗号的に更新された機密情報の量を 決定することである。この活動につい ては、移行リーダーは、活動 2.3 で特定した優先順位付けされた資産リストを使用し て、インベントリの暗号化状態を追跡することができる。

業績測定計画を立案する際には、"You get what you measure"（測定したものを得る）ということを忘れてはならない。パフォーマンスを効果的に示し、現実的に収集できる尺度を選ぶ。測定は、データ主導型、進捗重視型、意思決定重視型であり、少数の重要な問合せに限定すべきである。最後に、測定は、組織の PQC 移行のさまざまなカテゴリーに対応する。例えば、準備のカテゴリーでは、戦略的メッセージングが利害関係者の連携に与える影響を追跡するための指標を特定するとよいだろう。計画と実行については、PQC に移行したシステムの数を追跡したい。

PQC マイグレーションのセキュリティをどのように測定するのが最適かについては、まだ広範な研究が必要である。それまでの間、組織は NIST と NSA の標準を参照し、最新の測定方法が採用されるようにすべきである。

活動 4.2 成果：

- 組織は、PQC 移行の成功を追跡できる指標を特定する。
- 組織は、新しい PQC ソリューションによって保護される機密情報の量を決定することができる。

関連活動: 2.3

活動 4.3：労働力ニーズのアセスメント

マイグレーション・リーダーは、新たに獲得／開発された PQC ソリューションの実装と保守を行うために、組織の現在の労働力を最適化する方法をアセスメントする。これには、システム所有者／オペレータと調整し、現在のワークフロー内の ギャップを特定すること、必要なトレーニングを配布すること、及び／又は移行プロ セスを実行するために追加的な人材が必要かどうかを判断することが含まれる。組織の人員に必要な変更が加えられた場合、組織の PQC 移行のための予算（活動 3.1）及び継続的な実施（活動 3.5）の方法に影響を与える可能性がある。

活動 4.3 成果：

- 組織は、PQC セキュリティの新規導入に追加のセキュリティ研修が必要かどうかを判断する。
- 組織は、PQC へのシステム運用／移行を支援するために追加労働力が必要かどうかを判断する。

関連する活動 3.1, 3.5

活動 4.4：継続的なモニタリングと更新

移行リーダーは、組織のセキュリティの進展を継続的にモニタリング・測定し、インベント リリストを更新し、新しい標準への適合状況を追跡し、組織のリスク環境をアセスメント する。これまでの活動で述べたように、これらの変更と更新を文書化することは、組織のセ キュリティレジリエンスを維持するために不可欠である。

活動 4.4 成果：

- 組織は暗号アルゴリズムの在庫を更新し続けている。
- 組織は、組織目標に対する移行の進捗状況を継続的に測定する。
- 組織は、技術開発やリスクの状況をモニタリングするプロセスを構築することによって、備えを維持する。

関連する活動すべて

結論

多くの組織にとって、PQC への移行は将来の量子の脅威からデータを守るために極めて重要である。このロードマップは、この移行における 4 つの重要なカテゴリー（(1) 準備、(2) ベースラインの理解、(3) 計画と実行、(4) モニタリングと評価）を通じて、カスタマイズ可能なガイドを提供する。各カテゴリーは、PQC 移行の複雑さを効果的に管理するために必要なツールと戦略を組織に装備させるように設計されている。このロードマップで説明されているプロセスは、技術の進歩に適応し、強固なセキュリティ体制を維持するために、戦略的な計画、利害関係者の調整、継続的なモニタリングと文書化が重要であることを強調している。量子コンピューティングの状況が進化し続ける中、組織は適応力を維持し、PQC の安全な移行を維持するためのガイダンスの更新を追跡しなければならない。

参考文献

Attema T, Duarte J, Dunning V, Lequesne M, van der Schoot W, Stevens M (2023) The PQC Migration Handbook.(Applied Cryptography and Quantum Algorithms, Cryptology Group, and Netherlands National Communications Security Agency). https://publications.tno.nl/publication/34641918/oicFLj/attema-2023-pqc.pdf.

サイバーセキュリティ・インフラセキュリティ庁(2023) Quantum Readiness：ポスト量子暗号への移行 https://www.nccoe.nist.gov/sites/default/files/2023-08/quantumreadiness-fact-sheet.pdf

FS-ISAC (2023) PQC ワーキンググループ インフラストラクチャインベントリ テクニカルペーパー https://www.fsisac.com/hubfs/Knowledge/PQC/InfrastructureInventory.pdf

FS-ISAC (2023) PQC ワーキンググループ リスクモデル テクニカルペーパー https://www.fsisac.com/hubfs/Knowledge/PQC/RiskModel.pdf

Moody D, Perlner R, Regenscheid A, Robinson A, Cooper D (2024) Transition to Post-Quantum Cryptography Standards.(National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8547 ipd. https://doi.org/10.6028/NIST.IR.8547.ipd.

国立標準技術研究所(2024) モジュール-格子ベースの鍵カプセル化機構標準。(商務省、ワシントン D.C.）、連邦情報処理標準公開（FIPS）NIST FIPS 203。 https://doi.org/10.6028/NIST.FIPS.203。

国立標準技術研究所(2024) モジュール-格子ベース電子署名標準。(商務省、ワシントン D.C.）、連邦情報処理標準刊行物（FIPS）NIST FIPS 204。 https://doi.org/10.6028/NIST.FIPS.204。

国立標準技術研究所（2024）ステートレスハッシュベースデジタル署名標準。(商務省、ワシントン D.C.）、連邦情報処理標準刊行物（FIPS）NIST FIPS 205。 https://doi.org/10.6028/NIST.FIPS.205。

Canadian Forum for Digital Infrastructure Resilience (2024) Quantum Readiness Working Group of Canadian National Quantum-Readiness Best Practices and Guidelines（デジタルインフラ・レジリエンスのためのカナダフォーラム量子レディネス作業部会） https://ised-isde.canada.ca/site/spectrum-managementtelecommunications/sites/default/files/documents/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf