非機密

カナダ・サイバーセキュリティセンター

カナダ政府向けポスト量子暗号への移行ロードマップ (ITSM.40.001)

まえがき

本書は、カナダ・サイバー・セキュリティ・センター（Cyber Centre）の責任者の認可の下に発行された UNCLASSIFIED 出版物である。詳細情報または修正提案については、サイバーセンターまでご連絡ください：

- 電子メール：cryptography-cryptographie@cyber.gc.ca
- 電話 613-949-7048 または 1-833-CYBER-88 まで。

発効日

本書は 2025 年 6 月 23 日に発効する。

改訂履歴

改訂内容	改訂内容	日付
1	最初のリリース	2025 年 6 月 23 日

概要

情報技術（IT）システムを管理するすべての組織は、サイバー・セキュリティ・コンポーネントを量子安全に移行する必要がある。これにより、将来の量子コンピュータによる暗号の脅威から身を守ることができる。サイバーセンターは、この脅威を緩和するために標準化された耐量子暗号（PQC）の採用を推奨している。

本書は、カナダ政府（ガバナンス）が非機密 IT システム（[1] ）を PQC に移行するために推奨するロードマップの概要をまとめたもので、マイルストーン、成果物、各部門の計画と実行のためのガイダンスなどが含まれている。

連邦省庁のマイルストーンと成果物は以下の通り：

- 2026 年 4 月：部局の PQC 移行計画の初期段階を策定する。
- 2026 年 4 月以降：毎年 PQC 移行の進捗状況の報告
- 2031 年末：優先度の高いシステムの PQC 移行完了
- 2035 年末：残りのシステムの PQC 移行完了

[1]非機密 IT システムとは、機密情報を含まない、転送しない、または取り扱わない IT システムである。カナダ政府では、非機密システムは、UNCLASSIFIED、防御 A、および防御 B の情報を管理する。機密システムおよび防御 C 情報を扱うシステムについては、各省庁はサイバーセンターに連絡し、商用機器の移行に関する助言を得なければならない。

目次

1 序論 5

2 ステークホルダーと計画 6

3 実行段階 7

3.1 準備 7

3.1.1 役割と責任 7

3.1.2 資金計画 8

3.1.3 教育戦略 8

3.1.4 調達方針 8

3.1.5 識別のためのアプローチ計画 9

3.2 識別 9

3.3 移行 11

4 マイルストーンと成果物 13

5 ガバナンスと調整 14

5.1 関連するカナダ政府のガバナンス団体 14

5.2 進捗状況の報告 14

5.3 その他のリソースと支援 14

1 序論

サイバーセンターは、IT システムを管理する組織に対し、将来の量子コンピュータに脆弱な公開鍵暗号を置き換 えるため、PQC を使用するように移行することを推奨している。[2]GC 2011 の IT システムとカナダ国民のデータをこの脅威から保護するために、公開鍵暗号の全インスタ ンスを移行する必要がある。

米国の国立標準技術研究所（NIST）は、既存の脆弱性公開鍵暗号を置き換えることができる PQC アルゴリズムを標準化するために、暗号の専門家と世界的に協力してきた。PQC アルゴリズムに関するサイバー・センターの推奨は、UNCLASSIFIED、PROTECTED A、PROTECTED B 情報の暗号アルゴリズム（ITSP 40.111）で提供されている。ネットワーク・セキュリティ・プロトコルの標準が PQC アルゴリズムをサポートするようになると、サイバー・センターは「ネットワーク・プロトコルを安全に設定するためのガイダンス」（ITSP.40.062）出版物を更新する予定である。ガバナンスは、政府と産業界のニーズに迅速に対応するため、自社製品に PQC を組み込んでいる。

GCSI 内での PQC 移行には、多大なコミットメントが必要であり、数年を要する。サイバーセンターは、カナダ財務省事務局（Treasury Board of Canada Secretariat: TBS）およびカナダ共有サービス（Shared Services Canada: SSC）と協力して、GC のガイダンス、サポート、ポリシーに必要な更新を準備している。各省庁は、暗号の使用方法を明確に理解する必要がある。IT インフラ（ハードウェアとソフトウェアの両方）およびデータをエンタープライズ全体で分析する必要がある。既存の IT ライフサイクル予算を可能な限り活用するためには、PQC 移行を早期に開始することが重要である。

本書は、サイバーセンターが推奨する GC 内の非機密 IT システムを PQC に移行するためのロードマップである。本書は、この GC 全体のサイバーセキュリティ活動に関わる利害関係者、実行段階、マイルストーン、およびガバナンスの概要を示している。その意図は、GC 全体で PQC に移行するための各部門の計画活動の調整を支援する主要な活動とタイムラインを提供することである。本書は、連邦省庁の IT システムの責任者および管理者、ならびに PQC への移行の責任を負う意思決定者を対象としている。

[2]暗号に対する量子コンピュータの脅威の詳細については、『暗号に対する量子の脅威に備えるために組織を準備する』（ITSAP.00.017）https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threatcryptography-itsap00017 を参照。

2 利害関係者と計画

サイバーセンターは、カナダ GC における情報技術（IT）セキュリティの主要な技術認可機関である。[3]カナダの暗号機関であるコミュニケーション・セキュリティー・エスタブリッシュメント・カナダ（Communication Security Establishment Canada）の一部として、サイバーセンターは以下の役割を担っている：

- GC の各部門に対し、暗号に対する量子コンピューティングの脅威を認識させる。
- PQC の使用など、暗号に関する推奨事項のガイダンスを提供する。
- 強力なサイバーセキュリティ態勢に暗号技術を組み込むための推奨事項の提供

サイバーセンターは、PQC への移行を進める GC 各省庁を支援するため、引き続き適切な助言とガイダンスを提供する。

TBS は、政策リーダーシップ、戦略的方向性、監督を通じて、サイバーセキュリティを含むセキュリティ管理に対する政府全体のアプローチを確立し、監督する責任を負う。2024 年 5 月、TBS はカナダ政府のエンタープライズサイバーセキュリティ戦略を発表し、量子の脅威から GC の情報と資産を保護するため、GC のシステムを標準化された PQC を使用するように移行するための主要な行動を明らかにした。TBS は必要な政策文書を発行し、担当官に対し、部門ごとの PQC 移行計画を策定するとともに、既存の部門別報告プロセスに基づいて進捗状況を報告するよう求める。

SSC は、本 GC 内の多くの省庁に代わって IT インフラとサービスを管理している。GC システムの近代化において重要な役割を担っているため、SSC はすでに PQC への移行計画の策定に携わっており、サイバーセンターおよび TBS と直接協力し、実施の可能性について助言を行っている。

GC 内の連邦省庁は、それぞれのプログラム分野におけるサイバー・セキュリティ・リスクのマネジメントに責任を負う。各省庁は、SSC が管理する IT インフラでホストされるソフトウエア、および契約クラウドサービ スを含む SSC とは別に管理される IT インフラを維持する責任を負う。各省庁は、PQC を使用する責任を負うシステムの移行をカバーする、各省庁に合わせた PQC 移行計画を策定することが求められる。各省庁は、その計画を実行するとともに、進捗状況を追跡し、 に報告する責任を負う。本書は、各部局の PQC 移行計画を策定するために利用できる初期の検討事項を記載したものであるが、 TBS、SSC およびサイバーセンターは、さらなるガイダンスとサポートを提供する。

[3]カナダ財務委員会事務局の政府セキュリティに関する方針： https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578

3 実行フェーズ

このロードマップは、PQC 移行を実施するために推奨される 3 つの段階の概要を示している。これらのフェーズは重複する可能性が高い。

3.1 準備段階

準備段階では、各省庁は、PQC を使用する責任を負うシステムを移行するための部門別 PQC 移行計画を策定する責任を負う。この計画を策定するために、委員会を設置し、専任の移行担当者を特定することを推奨する。委員会は、組織全体の利害関係者で構成されるべきであり、経営陣の賛同と支持を確実にするために、上級管理職のメンバーを少なくとも一人は含めるべきである。IT システムの管理を担当する技術分野に加え、財務、プロジェクト管理、調達、資産管理などの非技術分野の利害関係者を含めることを推奨する。

部門別 PQC 移行計画は、その後のフェーズを実行する間、継続的に改訂され、拡大される必要がある。部門別 PQC 移行計画の初期版では、以下の責任者を定めるべきである：

- 計画の実行
- 財務計画
- 職員に量子の脅威と組織内のこの移行の進捗状況を知らせるための教育戦略
- 新規機器の調達方針
- 移行のためのインベントリ構築のための脆弱性システムの特定アプローチ

3.1.1 役割と責任

部門別 PQC 移行計画では、計画の実行における様々なタスクの責任者を特定する必要がある。最終的には、サイバーセキュリティの指定責任者（DOCS）が、サイバーセキュリティに対する量的リスクを緩和する責任を負う。
我々は、DOCS、または権限を委譲された幹部職員に、PQC 移行のエグゼクティブリードの役割を割り当て、提供することを推奨する：

- 監督
- 説明責任
- 各部門の PQC 移行計画実行のための執行支援

調整と部門横断的な関与は、PQC 移行のテクニカルリーダーが行ってもよい。テクニカルリーダーは、サービス提供、ネットワーク管理、IT 調達、その他移行に関連する分野を含む組織全体の調整を促進する責任を負う。部門別 PQC 移行計画を策定するために設置された委員会は、計画の実行管理のために再利用することができる。

3.1.2 財務計画

各省庁は、PQC を支援するために、多くの既存の IT システムの入れ替えや、新たなサービス契約の締結が必要になることを予期しておく必要がある。PQC 移行の実行は、新規雇用、外部委託、または他のプロジェクトや業務活動に影響を及ぼしうる役割の再編成を必要とする可能性のある人員配置への影響をもたらす。部門ごとの PQC 移行計画には、実行を完了するための資源配分を含むコスト見積りが必要である。計画の初期バージョンは、包括的なコスト見積もりにはならないが、識別と移行の段階が進むにつれて、財務見積もりは精緻化することができる。

この PQC 移行に関連するコストは、既存の IT 機器のライフサイクルやシステム近代化計画を活用することで削減できる可能性がある。そのためには、この計画の初期段階を迅速に実施し、こうしたコスト効率を活用できる場所を特定することが重要である。調達を急ぐことによる遅れは、コスト増につながる。

3.1.3 教育戦略

組織全体のスタッフが、量子の脅威と、その脅威が使用または担当するシステムに及ぼしうる影響について認識することが重要である。TBS GCxchange プラットフォームを活用し、様々な対象者向けのプレゼンテーションや出版物など、サイ バーセンターが作成した資料を含む成果物を部門や機関と共有する。サイバーセンターのラーニングハブは、暗号に対する量子の脅威について教育するためのコース教材を提供する。上級幹部は、PQC への移行が業務に与える影響を認識するよう説明を受けなければならない。

PQC への移行が進むにつれて、チームが直面する可能性のある新たな課題や障害も含め、上級役員に進展や進捗状況を常に報告することが重要である。

3.1.4 調達方針

新システムの耐用年数を最大化するために、各省庁は新規調達に PQC をサポートする要件があることを確認す べきである。サイバーセンターは、システムが確立されたサイバーセキュリティ標準を採用することを強く推奨する。標準に従うことで、独立したセキュリティレビューが保証され、ベンダーの囲い込みを避けるための相互運用性が促進される。一部のサイバーセキュリティ標準は、PQC をサポートするために現在も改訂中である。サイバー・センターは、標準における PQC のサポートが確定するのに合わせて、ネットワーク・プロトコルを安全に設定するためのガイダンス（ITSP.40.062）を更新している。製品カテゴリーによっては、PQC のサポートが現在利用できない場合もあることが予想される。

サイバーセンターは、暗号モジュールを含むシステムに関する契約条項を推奨している。これらは要望に応じて入手可能であり、今後より広く利用できるようになる予定である。一般的に、各省庁は調達に関する以下のベスト・プラクティスを考慮すべきである：

- 契約には、UNCLASSIFIED、PROTECTED A、および PROTECTED B 情報の暗号アルゴリズム（ITSP.40.111）におけるサイバー・センターの勧告に準拠した PQC のサポートをベンダーが含むことを保証する条項がある。
- 暗号モジュールは、暗号モジュール妥当性確認プログラムによって認定されている。

- 将来の構成変更を可能にする暗号アジリティのサポート

PQC が早期に調達条項に盛り込まれるほど、各部門が移行中に直面するコストは低くなる。

3.1.5 識別のためのアプローチを計画する

このロードマップの次の段階は、IT システムで暗号が使用されている場所の特定である。暗号の発見と呼ばれることもあるこの特定は、移行が必要なシステムのインベントリを作成するために必要である。部門の PQC 移行計画には、システムを識別し、このインベントリを構築するために実施するアプローチを含める必要があります。識別の詳細については、次のセクションで説明する。

3.2 識別

暗号がどこでどのように使用されているかを識別することは、PQC への移行プロセスにおいて重要 なステップである。暗号を使用するシステムには以下が含まれる：

- ネットワークサービス
- オペレーティング・システム
- アプリケーション
- コード開発パイプライン
- 以下のようなすべての物理的 IT 資産
    - サーバーラック
    - デスクトップ
    - ノートパソコン
    - 携帯電話
    - ネットワーク・アプライアンス
    - プリンター
    - ボイス・オーバー・インターネット・プロトコル
    - ハードウェア・セキュリティ・モジュール
    - スマートカード

- ハードウェア・トークン

これらは、オンプレミス、契約 IT プラットフォーム内、クラウド・サービス・プロバイダ、あるいは従業員が所有している場合がある。範囲が広いため、識別は困難な作業となる。

このフェーズで収集された情報は、システムごとに以下の情報を含むインベントリの作成に使用される：

- 暗号を使用するシステム・コンポーネント
- 各コンポーネントのベンダーと製品バージョン
- 識別された暗号に依存するセキュリティ管理策[4]
- 該当するネットワーク・セキュリティ・ゾーン
- 現在の暗号化設定
- ホスティング・プラットフォーム
- システムの依存関係
- 関連するサービス契約と有効期限
- システムまたはそのコンポーネントの更新予定年
- 担当部門の窓口
- システムの移行を優先すべき場合

インベントリに含めるべきその他の技術情報が関連する場合がある。サイバーセンターは、GC での経験が増えるにつれて、部局に追加のガイダンスを提供する。

各部門は、PQC への移行の優先順位が高いシステムを特定しなければならない。公衆ネットワークゾーン（[5] ）を経由する情報の機密性を保護するシステムは、HNDL（Harvest Now, Decrypt Later）の脅威により、予想よりも早くリスクにさらされる可能性がある。HNDL 脅威とは、脅威アクターが暗号化された情報を傍受し、それを保存し、十分に強力な 量子コンピュータが存在する将来に復号化することである。HNDL の脅威の影響を受けやすいシステムは、PQC への移行の優先順位を高くすることが推奨される。その他の考慮事項としては、情報の寿命、暗

---

[4]IT セキュリティ・リスクマネジメント（ITSG-33）：附属書 3A - セキュリティ管理カタログ：
https://www.cyber.gc.ca/en/guidance/annex-3a-securitycontrol-catalogue-itsg-33

[5]ネットワーク・セキュリティ・ゾーンの基本セキュリティ要件（ITSP.80.022）：
https://www.cyber.gc.ca/en/guidance/baseline-securityrequirements-network-security-zones-version-20-itsp80022

号の俊敏性のサポート、漏洩の影響などがある。システムに適切な優先順位が付けられるように、量子の脅威に対するリスクアセスメントを完了することは価値があるかもしれない。

脆弱性暗号を含むシステムの発見には、複数の手法を活用する必要がある。組織内の既存の IT サービス管理（ITSM）プロセスを活用することは、部門別の初期インベントリを作成する効率的な方法である。ライフサイクル管理委員会と変更管理委員会は、インベントリ・システムのエントリに必要な多くの情報を持っているはずである。しかし、実際には、ITSM の成熟度は部門によって異なる可能性がある。

暗号の検出を完了するには、ソフトウェア・ツールとサービスが必要である。これには、セキュリティ情報・イベント管理（SIEM）ソリューション、ネットワーク監視・検査、エンドポイント検知・対応（EDR）テクノロジなど、既存のサイバー・セキュリティ・サービスを活用することができる。これらのサービスでは、暗号の使用を識別するために、設定の変更、サードパーティのプラグイン、またはフィルタの追加が必要になる場合がある。 暗号発見のための独立したツールは、ネットワーク、ホスト、ログファイル、またはソースコードをスキャンする技術を採用する。サイバー・センタのセンサ・プログラムは、各部門の識別を支援するツールとして期待されている。暗号発見ツールやサービスに関する追加ガイダンスは、TBS、SSC、サイバー・センターを含む IT セキュリティ三部会が部局に提供する。

ディスカバリを完了させる上で重要なことは、輸入事業者に負担をかけないことであり、最初の不完全なインベントリから開始し、データを反復的に改善するための行動をとることである。

特定段階では、部門はインベントリを利用して関連する IT ベンダーや請負業者に働きかけ、自社の製品やサービスに PQC を導入する計画を決定する。どのシステムコンポーネントがアップグレードの対象になるのか、またはリプレースの対象になるのかを理解することは、移行計画を策定する次の段階を支援することになる。

3.3 移行

移行フェーズでは、特定フェーズで作成されたインベントリを活用して、システムのアップグレード、交換、トンネリング、および／または分離を計画し、実行する。

計画は、インベントリデータに加え、ソリューションの特定とアセスメント、必要な調達、テスト、展開のための部門リソースを考慮しなければならない。各システムの計画は、通常、複数の段階を必要とし、以下を含む適切な準備を確実にするために、既存の IT 変更管理プロセスと統合されるべきである：

- 影響アセスメント
- ロールバック・プレイブック
- 変更をテストするためのステージング環境
- 移行後の正常な運用を確認するためのモニタリング

各システムについて、技術チームは PQC を組み込んだり、量子の脅威を緩和したりするソリューションを特定し、アセスメントする必要がある。PQC 対応製品は初期段階では限られているかもしれないが、プロトコル標準の更新が完

了するにつれ、ベンダーは PQC を急速に採用している。ソリューションは、準備段階（調達方針 3.1.4）で確立されたすべての調達要件を満たすべきである。

多くのシステムは、一定期間、非移行システムとの継続運用を可能にするため、後方互換性を維持する必要がある。システム移行の第一段階は、PQC の使用をサポートすることであり、次いで第二段階として脆弱性 のあるレガシー暗号を無効にすることが考えられる。

一部のレガシー・システムでは、システムの全面的なリプレースなしに PQC を使用するように移行することは実行不可能な場合がある。移行のマイルストーンを達成するためには、そのようなシステムをネットワーク上に隔離するか、PQC で保護されたカプセル化レイヤー内にトラフィックをトンネルする必要があるかもしれない。このような決定は、移行フェーズの計画中に行うべきである。

部門別 PQC 移行計画の初期バージョンでは、移行フェーズの詳細が限定されている場合がある。

4 マイルストーンと成果物

連邦省庁のマイルストーンと成果物は以下のとおりである：

- 2026 年 4 月：最初の部局別 PQC 移行計画を策定する。
- 2026 年 4 月以降、毎年 PQC 移行の進捗状況の報告
- 2031 年末：優先度の高いシステムの PQC 移行完了
- 2035 年末残りのシステムの PQC 移行完了

これらの移行完了のマイルストーンは、量子脆弱性アルゴリズムが無効化、分離、トンネリングされることを意味する。つまり、単に PQC をサポートするのではなく、量子リスクが緩和されていることを意味する。各省庁は、マイルストーンの期日に間に合うよう、できるだけ早期にシステムを移行するため、各省庁の PQC 移行計画を作成し、修正し、それに従うことが重要である。

進捗状況の報告に関する期待については、次のセクションで詳しく述べる。

5 ガバナンスと調整

5.1 カナダ政府の関連ガバナンス団体

各省庁は、それぞれのプログラム分野におけるサイバーセキュリティリスクのマネジメントに責任を負う。しかし、PQC への移行のような政府全体の取り組みでは、TBS の政策文書に概説された説明責任に従って、エンタープライズ・レベルで管理される政府全体のアプローチが必要となる。

IT セキュリティ三部会は、TBS、SSC、サイバーセンターで構成される。三部会は、GC の PQC への移行など、GC 全体のサイバーセキュリティ・イニシアチブに関する助言、指導、監督、指示を提供する中央団体である。三部会は、TBS の権限下にある各省庁を支援している。

GC Enterprise Architecture Review Board（GC EARB）は、提案されたエンタープライズシステムが GC Enterprise Architecture の枠組みに整合しているかどうかを評価するガバナンスメカニズムを提供します。この枠組みは、ビジネス、情報、アプリケーション、技術、セキュリティ、プライバシーの各アーキテクチャ領域が、サービスおよびデジタルターゲットのエンタープライズアーキテクチャに適合していることを保証する。サイバーセンターの暗号推奨事項への準拠などのサイバーセキュリティ要件は、TBS 全体の戦略的方向性と TBS の政策文書に沿った GC ターゲット・エンタープライズ・アーキテクチャの一部である。

GC GC には、努力を同期させ、量子科学技術におけるカナダのリーダーシップを維持するため に、上級幹部レベルで構成される省庁間の量子科学技術（S&T）調整委員会がある。これらの委員会は、量子通信とポスト量子暗号に関する NQS ロードマップを含む、カナダの国家量子戦略（NQS）を支援する連邦政府の行動を監督している。

5.2 進捗状況の報告

GC 2011 の PQC への移行の進捗を監視することは、効果的な活動の監視とガバナンスに不可欠である。これにより、説明責任とマイルストーンの完了が保証される。TBS は、コンプライアンス管理のための財務省理事会の枠組みに従い、政策文書へのコンプライアンスを監督する。TBS はまた、「サービスとデジタルに関する方針」で義務付けられているサイバーセキュリティを含む、サービスとデジタルに関する部門計画の進捗状況も追跡している。各部門の進捗状況および PQC への移行を完了するために必要な活動に関する報告は、サービスおよびデジタルに関する部門計画の年次提出書類の一部として、TBS によって要求され、収集される。

5.3 追加のリソースとサポート

TBS の GCxchange プラットフォームは、PQC への移行を支援するため、連邦省庁との成果物の共有に活用される。サイバーセンターは、組織向けのガイダンスと推奨事項をサイバーセンターのウェブサイトで引き続き公表する。

量子脅威、PQC、またはこのロードマップに関する詳細情報をご希望の方は、このページの上部にあるサイバーセンターの連絡先情報をご利用ください。