Emerging Technology Insight

不確実性戦略でとらえる耐量子暗号移行【前編】

2025 年 9 月

耐量子暗号移行の「技術的困難性」と 3 つの「移行トリガー」

はじめに：耐量子暗号移行の「複雑性」と「不確実性」

情報通信の安全を支える暗号技術が大きく変わろうとしている。その背景には、量子コンピューターの発展によって、現在広く使われている暗号技術が破られる可能性が現実味を帯びてきているという事実がある。量子コンピューターは特定の問題に対して指数的に高速な計算能力を持つとされており、既存暗号を短時間で解読できる事態が想定されるためだ。この脅威を軽減するために、量子攻撃に対して耐性があると考えられている、あるいは確実に耐性があるとされる新しい暗号技術を採用する必要が出てきた。これが、「耐量子暗号（Post-Quantum Cryptography：以下 PQC と記載する）移行」問題である。

本稿では、PQC 移行問題を「複雑性」と「不確実性」という観点から分析し、問題解決への道筋を示したい。第一に、組織のセキュリティの担い手にとって、PQC 移行は考慮すべき点が多い。移行判断には、新暗号技術特性の把握、自社への影響度と範囲、移行タイミングの見極め、関係者との合意形成などの要素が複雑に絡み合う。第二に、外部環境の見通しが立ちづらい。現時点で確実なのは「いつか PQC への移行が必要である」ということだが、Q-Day[1]の到来予測に幅があったり、PQC アルゴリズムの変更も考慮すべきだったりといった「不確実性」と向き合わなければならない。したがって、ビジネスとして PQC 移行を成功させるためには、「複雑性」の正しい理解と「不確実性」に対する戦略が必須となる。

本シリーズは、組織の情報セキュリティ責任者（CISO）ひいては経営層に対して、組織における PQC 移行戦略策定の枠組みを提供することを目的とし、前編と後編で構成される。前編では PQC 移行の「複雑性」の正確な理解に焦点を当て、後編では PQC 移行に「不確実性戦略」を導入し、組織が実施すべきことを提示する。前編となる本稿では、第 1 節で PQC 移行の技術的・構造的難易度について詳細に論じ、従来の暗号移行との本質的な違いを明らかにする。第 2 節では、移行開始のトリガーとして企業が見逃してはならないイベントを体系的に 3 カテゴリーに分けて整理する。

[1] Q-Day：「Y2Q（Year to Quantum）」とも呼ばれ、量子コンピューターが従来の暗号技術を破る能力を持つようになるとされる日。現在のデジタルセキュリティが根本的に脅かされる転換点を示す。

第1節　アルゴリズム特性がもたらす PQC 移行の困難性

過去の暗号移行と PQC 移行の違い

PQC への移行は、情報システムにおける暗号技術の単なる更新よりも難易度が高い。暗号移行には過去にも、DES から AES、RSA 鍵長の拡張、SHA-1 から SHA-2 への移行などあったが、PQC 移行はそれらの事例とは次元が異なる[2]。その理由は、PQC は単なる「暗号強度の向上」ではなく、暗号の根本的な設計思想や前提を覆すものだからである。**図表 1** に、過去の暗号移行と PQC 移行における留意点の差異をまとめた。

図表 1　過去の暗号移行と PQC 移行における留意点の差異

移行時の留意点	従来技術内での暗号移行	PQC への移行
処理速度への影響	限定的	影響を考慮する必要あり
影響範囲	限定的	広範囲（TLS、SSH、IPsec／VPN、S／MIME など）
実装の互換性	高い	低い（再設計が必要）
計算コスト	低～中	高い（特に組込み機器で問題）
技術の信頼性	従来技術のため信頼性が高い	歴史が浅いため長期の検証が必要
移行の猶予	攻撃後でも対応可能	攻撃前に完了しないと意味がない

（出所）著者作成

組織経営層は従来暗号アルゴリズムや PQC の技術的詳細を理解する必要はないが、上記の通り「PQC 移行の難易度は今までと次元が異なる」と認識されたい。例えるなら、過去の暗号移行が「自動車のエンジンを強化する」ことであったのに対し、PQC 移行は「ガソリン車から電気自動車に切り替える」ようなものと言える。

PQC の技術的特徴：「データサイズ」と「影響範囲」

PQC 移行の難易度を上げている技術的特性の一つは、そのデータサイズである。PQC アルゴリズムは RSA などと比較して鍵長や署名サイズが数倍から数十倍大きくなり、既存のプロトコルや証明書仕様が前提とするメッセージ長や処理能力の限界を超える可能性がある。つまり、PQC のデータサイズが原因で、通信・処理・保存のすべてに負荷がかかり、既存システムの設計を根本から見直す必要が出てくるということだ。NIST 推奨アルゴリズムである CRYSTALS-KYBER は暗号化および鍵交換、DILITHIUM は署名に用いられ、それぞれにおいてデータサイズが大きくなる。128bit 安全相当でもおよそ 1000～2000 バイトであり（**図表 2**）、256bit 安全相当になるとデータ

[2] IETF-Internet Engineering Task Force (2023) *"Post-Quantum Cryptography for Engineers"* https://www.ietf.org/archive/id/draft-ietf-pquip-pqc-engineers-05.html（2025 年 9 月 16 日にアクセス）

サイズはさらに大きくなる。したがって、PQC アルゴリズムを実装するシステムは、従来と同程度の安全性を得るために、より大きなデータサイズを処理することを前提に設計される必要がある。

図表 2　128 ビット安全相当の暗号アルゴリズムの比較

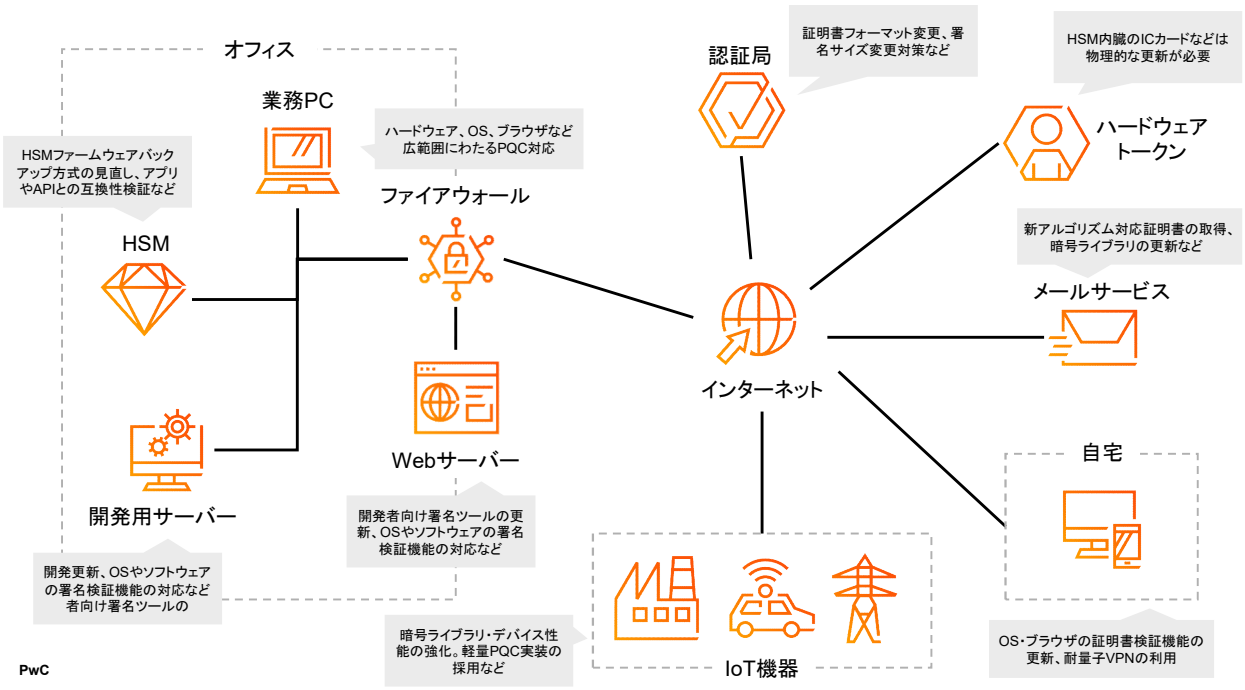
カテゴリー	従来暗号／PQC	アルゴリズム	公開鍵サイズ	暗号文／署名サイズ	移行／運用上の留意点
公開鍵暗号 KEMs	従来暗号	RSA-3072	384 バイト	384 バイト（暗号文）	公開鍵暗号は通信に多用されるためハーベスト攻撃の影響が大きく、早期の移行が望ましい。ただしPQCは実装実績が限られているため、従来暗号とのハイブリッド利用によるリスク分散も有効な選択肢となる。
	PQC	**CRYSTALS-KYBER**	**800 バイト**	**768 バイト（暗号文）**	
デジタル署名	従来暗号	ECDSA P-256	32 バイト（圧縮形式）	64 バイト（署名）	署名サイズが大きくなるため、既存プロトコルやストレージ設計の見直しが必要になる可能性。
	PQC	**CRYSTALS-DELITHIUM**	**1312 バイト**	**2420 バイト（署名）**	

（出所）NIST PQC 関連情報[3]をもとに著者作成

また、前述の「鍵が大きい・署名が重い」という構造的違いに加えて、暗号技術がデジタル環境の至るところで適用されているという事実も、PQC 移行の難易度が高いとされる所以である。**図表 3** に、暗号技術の適用範囲と PQC 移行のポイントを例示した。巻末の参考資料「暗号アルゴリズム変更例の詳細」と併せて参照されたい。

[3] NIST *"Post-Quantum Cryptography Standardization"* https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization（2025 年 9 月 16 日 にアクセス）

図表 3　PQC 移行が想定される範囲例



（出所）筆者作成

こうした要素を見ると、PQC 移行は単に暗号モジュールの入れ替えに留まらず、証明書 1 枚からネットワークプロトコル、デバイス、運用ポリシーに至るまで広範囲に及ぶ変化を伴うことがわかる。すでに日本でも PQC 移行への早期対応とロードマップの策定、暗号インベントリの重要性が強調されているが[4]、これはハーベスト攻撃[5]といったいわゆる量子脅威だけが理由なのではなく、暗号アルゴリズムの技術構造と影響範囲に起因しているという理解が、経営層にとっては肝要である。

また、PoC（概念実証）から本番導入へのプロセスも平坦ではない。PQC 導入がシステム全体の性能に与える影響、外部ベンダーとの相互運用性、PKI（公開鍵基盤）[6]の再設計、証明書更新のタイミング調整など、検討すべき課題は山積している。特にパフォーマンスやレイテンシに敏感な業務領域（金融取引やリアルタイム医療診断など）においては、PQC の実装が実務に与えるインパクトを定量的に評価する必要がある。こうした課題に対する投資も極めて大きい。米国政府機関の場合、全連邦システムの優先資産を対象に各省庁からの移行コストの見積を集計したところ、2025～2035 年で約 71 億ドルの予算が必要だと試算された[7]。このほどの予算規模からも推

[4] 金融庁（2025）“預金取扱金融機関の耐量子計算機暗号への対応に関する検討会報告書” https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf（2025 年 9 月 16 日にアクセス）

[5] ハーベスト攻撃：将来的に暗号を解読できる技術の登場を見越して、現在の暗号通信を大量に収集・保存しておく攻撃手法

[6] PKI（公開鍵基盤）：安全な通信や認証を実現するために、公開鍵と秘密鍵を管理し、信頼性を保証する仕組み

[7] Executive Office of the President of the United Sates (2024) *“Report on Post-Quantum Cryptography”* https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf（2025 年 9 月 16 日にアクセス）

察できるとおり、PQC 移行は数年規模の全社的な取り組みになることは間違いなく、段階的な導入体制の整備が推奨される。

このような複雑性を考慮すれば、PQC 移行は「プロジェクト」というよりも「長期的なプログラム」であると捉えるべきと言える。本節では、PQC移行があらゆる技術層と運用プロセスに波及する構造的改革であることを分析した。この本質は、「いつから何を実施するべきか」を判断する前提でもあり、PQC移行には組織戦略が不可欠であることの理由でもある。次節では、このような高難易度の移行において、企業が見逃してはならない「着手の契機」を整理する。

第2節　PQC 移行におけるトリガー認識の戦略的意義

POC 移行は可能な限り速やかに着手することが望ましいが、より現実味を帯びて現れる課題は「いつ移行すべきか」という問いである。これは、移行に際して「逃してはならないトリガー」を見極める戦略であるとも言える。場当たり的な追い込みで移行を図れば、システムに不備やセキュリティ上の抜け穴が生じかねないため、移行の「トリガー」を戦略的に捉える必要がある。本節では PQC 移行計画に組み込むべき「トリガー」を体系的に整理し、その戦略的意義を論じる。

PQC 移行における主要な移行トリガー

以下に PQC 移行における 3 種類のトリガーを提示する。いずれのカテゴリーも年単位の周到な準備を必要とするため、前もって計画に組み込まなければ機会を逸し、結果的に二重投資が生じるリスクがある。

I.　システム・証明書・製品ライフサイクルの更新

自社システムの大規模アップグレードや PKI 証明書の更新時期は、PQC 対応を織り込む機会である。基幹系システムや長期利用される機器の更改サイクルは数年～十数年スパンで訪れるが、その更新時に量子耐性を考慮しないと、次回更新までに暗号が陳腐化する恐れがある。証明書についても、有効期限が 2030 年代に及ぶようなものは量子安全なアルゴリズムで再発行する計画が不可欠となる。また、自動車など 10 年以上の利用が想定される製品にも、企画段階から量子耐性を考慮した設計が求められる。したがって、通常サイクルで訪れるシステム刷新や証明書更新、新規プロダクト設計のタイミングは、PQC 移行を組み込むべき重要トリガーであると言える。

II.　パートナー要件・サプライチェーンの要請

取引先やサプライチェーンからのセキュリティ要件も重要なトリガーとなる。他組織が量子耐性を要求し始めると、自社だけ従来暗号のままでは接続や取引移行に支障を来す可能性がある。例えば米国政府調達契約では 3 年以内に PQC 対応が明示的に求められるという見方もあり[8]、米国政府は PQC に対応した製品が広く流通している製品カテゴリーリストを、2025 年 12 月 1 日までに作成・公開することとしている[9]。また、米国金融業界では決済カードのインフラ全体で量子耐性確保に向け多数のステークホルダーが参加する取り組みが

[8] Post Quantum (2024) *"NIST Unveils Post-Quantum Cryptography (PQC) Standards"* https://postquantum.com/industry-news/nist-pqc-standards/（2025 年 9 月 16 日にアクセス）

[9] The White House (2025) *"Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144"* https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/（2025 年 9 月 16 日にアクセス）

進んでおり[10]、一部でも対応が始まれば系列企業にも波及する見込みがある。こうした動きは日本を含む他国の金融機関にも影響を与える可能性があるため、グローバルなサプライチェーンの一環として注視すべきである。

III. 規制・標準への準拠義務の発生

政府規制や業界標準の改定による道守業務の発生は、強制力を伴う明確なトリガーである。米国ではホワイトハウスの国家安全保障メモランダム NSM-10 に基づき、連邦機関が 2035 年までに量子耐性暗号への移行を完了する計画が進められている[11]。さらに 2024 年には NIST により PQC 標準が正式策定され、今後は政府・規制当局が量子耐性を要求することが既定路線となった[12]。欧州でも 2025 年に EU 加盟各国が協調して重要インフラを 2030 年までに耐量子暗号へ移行させるロードマップを発表しており[13]、各国で金融や通信などへの法令・指針として具体化が始まっている、業界標準においても、たとえば国際決済カード規格（PCI）はもちろん、自動車のサイバーセキュリティ規格（ISO/SAE21434）のアップデートで量子耐性が織り込まれる可能性が高い。こうした外部から課される遵守期限は見逃せないトリガーであるため、各業界における法規制およびガイドラインの動向の定期的な情報収集が必要になるだろう。また、日本においても PQC 移行への動きが活発化している。金融庁も報告書の中で「各組織内の優先度の高いシステムは、技術進展や海外規制動向を注視しつつ、2030 年代半ばを目安に耐量子計算機暗号のアルゴリズムを利用可能な状態にすることが望ましい」としている。[14]政府発行の「サイバーセキュリティ2025」にも「政府機関等における耐量子計算機暗号（PQC）への移行の方向性について、次期サイバーセキュリティ戦略に盛り込む」と明記[15]されている。

これらの移行トリガーカテゴリーの区分けをより実践に近づけるために、PQC移行対応の影響が大きい主要業界（金融、防衛、公共インフラ、ヘルスケア、自動車）を例にとり、各カテゴリーの具体を洗い出してみたい。**図表 4** は、業界別の代表的なトリガー事例をカテゴリーごとに整理したものである。

---

[10] FS-ISAC *“Post Quantum Cryptography Implications for the Payment Card Industry”* https://www.fsisac.com/pqc-payment-card-industry (2025 年 9 月 16 日にアクセス)

[11] Executive Office of the President of the United States (2024) *“NSM-10 and the Transition to Post-Quantum Cryptography”* https://csrc.nist.gov/csrc/media/Presentations/2024/u-s-government-s-transition-to-pqc/images-media/presman-govt-transition-pqc2024.pdf (2025 年 9 月 16 日にアクセス)

[12] NIST *“Post-Quantum Cryptography Standardization”* https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization (2025 年 9 月 16 日 にアクセス)

[13] European Commission (2025) *“A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography”* https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography (2025 年 9 月 16 日にアクセス)

[14] 金融庁（2025）“預金取扱金融機関の耐量子計算機暗号への対応に関する検討会報告書” https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf (2025 年 9 月 16 日にアクセス)

[15] サイバー統括室（2025）“サイバーセキュリティ 2025（2024 年度年次報告・2025 年度年次計画）” https://www.nisc.go.jp/pdf/policy/kihon-s/cs2025.pdf (2025 年 9 月 16 日にアクセス)

図表 4　主要業界別の移行トリガー事例

業界	システム・証明書・ 製品ライフサイクルの更新	パートナー要件・ サプライチェーンの要請	規制・標準への 準拠義務の発生
金融	勘定系システム刷新 PKI 証明書更新	決済ネットワークからの量子耐性通信要請 取引先のセキュリティ条件更新	監督指針や FISC の安全対策基準の適用開始 PCI 標準の改定要求
防衛	防衛通信ネットワーク更改 長寿命装置の暗号更新	同盟国との安全通信プロトコル要請 防衛調達契約条件	政府通達による遵守義務 国家安全保障暗号基準の改定
公共インフラ	制御システム（OT）設備の更新 認証基盤更改	パートナー企業との安全通信要件 電力・交通などの系統連系条件の変更	政府の重要インフラ指針の適用開始 EU 指令（NIS2）順守義務
ヘルスケア	医療情報システム刷新 医療機器ソフトウェア更新	医療データ連携に関する安全要件 機器サプライヤーからのアップデート通知	医療機器規制（FDA ガイダンス）への対応 個人情報保護規則の改定
自動車	車載システムの刷新 車載 PKI 証明書更新	コネクテッドカー通信標準要件 共同開発パートナーからの安全性要求	自動車サイバー規制（WP.29）適合義務 業界標準（ISO 21434）への対応

（出所）筆者作成

■ **金融**

金融はサイバー攻撃者の主要標的であり、取引の長期安全性確保のため量子コンピューター対策を最も早急に迫られる業界の一つである。例えば国際的な決済ネットワークや資金・証券決済システムが量子耐性通信を要求し始めれば、各金融機関は対応を余儀なくされる。金融システムの多くはミッションクリティカルで更新サイクルも長いため、次の基幹系刷新や証明書更改の機会を逃さず PQC 対応を織り込むことが、将来のリスクとコストを大きく削減する戦略ポイントとなる。

■ **防衛**

防衛・宇宙分野では、国家安全保障と直結する通信や機密データの保護が最重要であり、政府主導の量子耐性化ロードマップに従った計画的移行が不可欠となる。防衛分野のシステム（例：衛星通信、暗号装置、兵器システム）は運用期間が数十年に及ぶ長寿命のものが多く、次期システム更改時に量子耐性を組み込まなければ将来の作戦通信や機密保持が危殆化する恐れが高い。また NATO をはじめとする同盟国間で安全な量子耐性通信プロトコルの策定が進めば、自国の防衛通信もそれに合わせる必要がある。

■ **公共インフラ**

エネルギー、交通、通信、水道など公共インフラは国民生活を支える基盤であり、国家運営と密接に関わっているため、法規制や標準準拠が強く求められる。インフラ事業者は多くの場合ネットワークを相互連携しているため、一部でも PQC 移行が進むと全体で対応が必要になる。さらに各国政府による重要インフラ防護の法制

度（例えば NIS2 指令[16]や米国 CISA ガイドライン[17]）は事業者に対し量子技術を見据えたリスク管理を義務付ける方向にあり、監督当局から計画提出を求められる可能性もある。

■ **ヘルスケア**

ヘルスケア分野（医療機関や医療機器メーカー等）では、患者の個人情報や医療データを長期にわたり守る必要があるうえ、人命に直結する機器の安全性確保という観点からも PQC 移行の緊急度が増している。FDA（米国食品医薬品局）の 2023 年発行のガイダンス[18]では、耐量子暗号アルゴリズムの使用を義務付けていないが、医療機器メーカーに対して以下を要請している：現在使用している暗号技術を理解していること、必要に応じてその暗号技術を更新・交換できること、特に 10～15 年以上市場に残る可能性のある機器については暗号技術の進化に対応する計画を示すこと。

■ **自動車**

自動車産業では、コネクテッドカーの普及により、V2V（vehicle-to-vehicle）／V2X（vehicle-to-everything）通信の暗号強度が今後 10 年以上先を見据えて求められる状況にある。車両製品はモデルチェンジ後も長期間にわたり公道を走り続けるため、今採用している暗号が 2030 年以降に陳腐化すると車両のセキュリティをリコールなしで維持することは困難となる。このため、次世代車載プラットフォームの設計時に PQC やハイブリッド暗号（従来暗号＋量子安全暗号）を組み込むことなどの対応が必要となる。さらに自動車はグローバルなサプライチェーンで構築されるため、主要な半導体・ソフトウェア供給元が量子耐性機能を提供し始めると、それを搭載することが競争力や契約上の必須条件となり得る。したがって、自動車業界ではモデルチェンジやコネクテッド機能拡充のタイミング、および業界規制や標準の改定動向を中心にトリガーを見極め、製品設計段階から PQC 移行を計画に織り込む先行投資が戦略的に重要となる

以上、PQC 移行トリガーについて 3 つのカテゴリーに分類して述べた。これらの各局面が、PQC 移行を「一石二鳥」にするか「二度手間」にするかの境目となり得る。各組織は戦略的にこれらトリガーを見極めることで、時間差で訪れる「許容できないリスク」と「追加コスト」を低減・回避する機会を得られる。

まとめ：PQC 移行は「技術対応」ではなく「戦略判断」である

本稿では、PQC移行の「複雑性」に焦点を当て議論してきた。PQC 移行は、単なる暗号アルゴリズムの更新ではなく、企業の情報システム全体に及ぶ構造的な変革である。鍵長や署名サイズの肥大化、既存プロトコルとの非互換性、インフラ全体への影響など、技術的困難性は従来の暗号移行とは次元が異なる。さらに、移行のタイミングを見極めるためには、3 つの「移行トリガー」――①システム・証明書・製品ライフサイクルの更新、②パートナー要件・サプライチェーンの要請、③規制・標準への準拠義務――を戦略的に捉える必要がある。こうした背景から、PQC 移行は「技術部門に任せておけばよい」ものではなく、経営層による戦略判断が不可欠な課題となる。特に、移行に伴う費用は数年規模・全社的な投資となる可能性が高く、PoC（概念実証）から本番導入までのコスト見積もりは、経営判断の中核を成す。PQC 移行は、技術的な準備だけでなく、経営戦略、業界動向、社内成熟度を踏まえた経営意思決定に収斂していく。

---

[16] European Commission (2025) “NIS2 Directive: securing network and information systems” https://digital-strategy.ec.europa.eu/en/policies/nis2-directive（2025 年 9 月 16 日にアクセス）

[17] CISA “Post-Quantum Cryptography Initiative” https://www.cisa.gov/quantum（2025 年 9 月 16 日にアクセス）

[18] US. Food & Drug Administration *“Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions”* https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions（2025 年 9 月 16 日にアクセス）

最後に、PQC 移行にあたり経営層が実施すべきアクションを**図表 5** に整理した。これは、本稿での議論を、経済産業省の「サイバーセキュリティ経営ガイドライン Ver3.0[19]」に示されている 3 原則と 10 の指示に則って再構成したものである。経営層が PQC 移行を検討する際の指針として参考されたい。

図表 5　経営層が実施すべき PQC 移行アクション

カテゴリー	ガイドライン項目	PQC 移行におけるアクション	アクションのキーパーソン
原則	① 経営者が主導的に関与すること	PQC 移行を「技術対応」ではなく「戦略判断」として位置づけ、経営層が意思決定に主体的に関与する	CEO、CISO、CTO
	② 経営者がリスクを認識し、対策方針を策定すること	Q-Day やハーベスト攻撃などの量子脅威を踏まえ、移行トリガー（システム更新、規制対応等）を戦略的に捉えた方針を策定する	CISO、CRO、CIO
	③ 経営者が体制整備と資源確保を行うこと	PQC 移行に必要な予算、人材、外部ベンダーとの連携体制を整備し、長期的なプログラムとして推進する	CIO、CISO、CTO、パートナー企業
指示	① リスク認識と対応方針の策定	PQC 移行の技術的・構造的リスクを経営層が理解し、対応方針を明文化する	CISO、CRO
	② リスク管理体制の構築	情報システム部門、法務、調達などを含む横断的な移行推進体制を構築する	CIO、CISO、CRO
	③ 資源（予算・人材）の確保	PoC～本番導入までの費用を見積もり、必要な人材（暗号技術、PKI、IoT 等）を確保する	CIO、CTO、CFO
	④ リスク把握と対応計画の策定	自社インフラへの影響範囲を洗い出し、段階的な移行ロードマップを策定する	CTO、CISO、CIO
	⑤ 対応仕組みの構築	PQC 対応証明書、TLS 拡張、IoT 軽量暗号などの技術的対応策を整備する	CTO、CISO、CIO
	⑥ PDCA による継続的改善	PQC 移行の進捗を定期的にレビューし、技術標準や規制変更に応じて計画を更新する	CIO、CISO、CRO
	⑦ 緊急対応体制の整備	PQC 未対応によるセキュリティインシデントに備えた緊急対応体制を整備する	CISO、CRO

[19] 経済産業省 独立行政法人 情報処理推進機構 “サイバーセキュリティ経営ガイドライン Ver.3”
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf（2025 年 9 月 16 日にアクセス）

⑧ 事業継続・復旧体制の整備	PQC 移行に伴うシステム停止リスクに備え、BCP（事業継続計画）を見直す	CIO、CRO
⑨ サプライチェーン対策	ベンダーやパートナー企業の PQC 対応状況を把握し、契約条件に反映する	CISO、調達部門、パートナー企業
⑩ 情報共有・開示の促進	PQC 移行の方針や進捗を社内外に共有し、業界標準化や共同対応を促進する	CISO、広報、業界団体

（出所）著者作成

シリーズ前編となる本稿では、PQC 移行の「複雑性」、すなわち技術的困難性と戦略的トリガーについて論じた。後編では「不確実性」に焦点を当て、企業が取り得る戦略姿勢の分類と、実践的な着手方法についてさらに深掘りし、PQC 移行の全体像を描く。

【著者】

石原　陽平
シニアアソシエイト　PwC Intelligence　PwC コンサルティング合同会社

三上　雄一郎
マネージャー　Technology Laboratory　PwC コンサルティング合同会社

丸山　満彦
パートナー　PwC Intelligence　PwC コンサルティング合同会社

【監修】

三治 信一朗
パートナー　Technology Laboratory　PwC コンサルティング合同会社

長嶋 孝之
パートナー　Technology Laboratory　PwC コンサルティング合同会社

一山 正行
パートナー　Digital & AI Transformation　PwC コンサルティング合同会社

北野 剛史
シニアマネージャー　Technology Laboratory　PwC コンサルティング合同会社

柳川　素子
マネージャー　PwC Intelligence　PwC コンサルティング合同会社

PwC Intelligence　統合知を提供するシンクタンク

https://www.pwc.com/jp/ja/services/consulting/intelligence.html

PwC コンサルティング合同会社

〒100-0004　東京都千代田区大手町 1-2-1 Otemachi One タワー　Tel：03-6257-0700

【参考資料】 暗号アルゴリズム変更例の詳細

インフラ要素	必要となる変更・再設計ポイント	背景・理由
PKI（証明書／CA）	新アルゴリズムの OID（オブジェクト識別子）追加。証明書フォーマット変更（複合鍵・署名への対応）。証明書・CRL（失効リスト）サイズ肥大への対策。	PQC で使用される鍵や署名はサイズが大きく、既存の X.509 証明書構造では非効率または不適合となる場面が多くなっている。証明書や CRL の肥大化は避けられず、メール、TLS ハンドシェイク、コード署名などに影響が出る。
TLS 等の通信プロトコル	ハンドシェイク拡張（複数鍵交換の許容）。メッセージ長制限の緩和・分割送信実装。新しい暗号スイート定義（PQ-KEM）。	TLS はインターネット通信のセキュリティ基盤であり、HTTPS、SMTP、IMAP、VPN など多くのプロトコルで使われている。現行の TLS1.3 は既存暗号アルゴリズムでの鍵交換・認証を前提に設計されているため、PQC 対応には構造的な拡張が必要。
VPN／IPsec	IKEv2 でのハイブリッド鍵交換の実装。装置ファームウェアの更新。	現状、中核技術の IKEv2 は Diffie-Hellman や ECDH など、量子コンピューターで破られるリスクのある鍵交換方式を採用している。VPN 通信に対するハーベスト攻撃が懸念される。多くのエンタープライズ VPN はハードウェアアプライアンスを仕様しているため、メーカー側の更新対応が必須。
IoT 機器／プロトコル	暗号ライブラリ・デバイス性能の強化。軽量 PQC 実装の採用。プロトコル手順の簡素化。	IoT 機器は CPU 処理能力、メモリ容量、消費電力の面で制限が大きい。従来の暗号に比較してデータサイズが大きい PQC アルゴリズムの処理は、IoT 機器には基本的に重すぎる。
クライアント証明書認証	OS・ブラウザの証明書検証機能のアップデート。スマートカード等のハードウェアトークンの刷新。	サーバ側だけでなくクライアント側（利用者）も証明書を提示して相互認証を行う「クライアント証明書認証」が一般化。カーネルやミドルウェア層での対応が必要。HSM（ハードウェアセキュリティモジュール）内臓の IC カードなどは物理的な更新が必要。
S／MIME（電子メール暗号化）	メールクライアント／サーバの暗号ライブラリ更新。新アルゴリズム対応の証明書の取得・配布。ゲートウェイや中継装置の検証ロジック見直し。	送信側の秘密鍵で署名、受信者の公開鍵で暗号化という構成のため、双方を PQC に移行する必要がある。S／MIME 証明書の認証局側でも対応が必要、さらに証明書の配布方法も再検証が必要。多くの企業で利用されている中継機器（DLP やメールセキュリティゲートウェイ）の更新も重要。
コード署名／ソフト更新	開発者向け署名ツールの更新。OS やソフトウェアの署名検証機能の対応。署名フォーマットの拡張。信頼ストアの再構成。	署名が埋め込まれる形式（PE ファイル、MSI、JAR など）はフォーマット構造が固定長や制限付きで、署名サイズと合わせる必要がある。開発者が利用する署名ツールの PQC 対応と、OS 内臓のルート証明書ストアの刷新が必要。

鍵管理（HSM／鍵保管）	HSM（ハードウェアセキュリティモジュール）デバイスの更新または置換。PQC 鍵のバックアップ・移行手順の新設。鍵長、鍵形式の変化に伴う HSM 内メモリ設計や API 更新	秘密鍵の生成・保存・使用は HSM で行うことが多くの業界（金融、医療、政府など）で標準的。HSM ファームウェアバックアップ方式の見直し、アプリや API との互換性検証が必須。

（出所）PQC 関連資料[20] [21] [22]を参考に著者作成

[20] NATO CCDCOE (2024) “Identifying Obstacles of PQC Migration in E-Estonia” https://ccdcoe.org/uploads/2024/05/CyCon_2024_Vakarjuk_Snetkov_Laud-1.pdf（2025 年 9 月 16 日にアクセス）

[21] Open Quantum Safe Project “Open Quantum Safe - software for the transition to quantum-resistant cryptography” https://openquantumsafe.org/（2025 年 9 月 16 日にアクセス）

[22] Liu et al. (2024) “Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization”