kyndryl

耐量子暗号への移行戦略

量子コンピューター時代に備えるサイバーレジリエンシー

目次

はじめに：なぜ量子コンピューターが脅威となるのか

暗号解読時間の短縮化がもたらす脅威

現在、インターネット通信やデータ保護の大部分が、RSA 暗号や楕円曲線暗号（ECC）の技術に基づく「公開鍵暗号方式」に依存しています。これらは、数学的に最適な計算方法が存在していないために解読に非現実的な時間がかかるという性質を利用した暗号方式として長らく利用されてきましたが、量子コンピューターの登場によって、現実的な時間で解読できるようになると予測されています。量子コンピューターは量子力学の原理を応用した新たな計算機として、現在はまだ汎用的な計算能力を獲得しているわけではないものの、一部の問題に非常に優れた計算能力を発揮します。まさに上述した方式の暗号解読もその 1 つと目されています。

量子時代では新たなサイバー攻撃が懸念されています。その代表例の 1 つが「今収集し、後で復号する（Harvest Now, Decrypt Later：HNDL）」攻撃です。今の技術では解読できない暗号化データを今のうちに保管し、量子コンピューターによる技術が確立されてから復号化を試みるという手法です。ほかにも「量子ブルートフォース攻撃」も懸念されています。これはいわゆる総当たり攻撃ですが、量子コンピューターでは、「グローバーのアルゴリズム」によって従来のコンピューターよりも少ない試行回数で総当りが可能になるというものです。

実用化のタイムリミットは 4 年

量子コンピューターの登場は机上の空論ではありません。例えば量子コンピューターの開発を手掛ける 1 社として知られる IBM は 2029 年までに 200 論理量子ビットの耐障害性を備えた量子コンピューターを実現予定です[1]。Google も実用的な量子コンピューターの実現を 2030 ～ 35 年としています。キンドリルにおける別の予測[2]では、2029 年までに国家支援を受けたある情報機関が、戦略的価値を有する暗号化データセットを解読可能であることを秘密裏に実証するという見立てもあります。

もしこうしたブレイクスルーとなる出来事が世に知られてしまえば、世界中で市場が混乱し、組織としては対応に追われることとなるでしょう。そこでは量子コンピューターに「備えている組織」と「備えていない組織」の格差が生じることになります。

タイムリミットは最短 4 年後と、一見すると猶予があるように考えられますが、システム全体に上述の対策を行き渡らせるためには、暗号資産の全体把握や移行ロードマップの策定から実際の対策までかなりの時間を要します。今すぐにでも着手しなければ間に合わないと考えるべきでしょう。

想定される 3 つのセキュリティ被害

量子コンピューターを用いた攻撃が行われるようになると、実際にどのような被害が生じうるでしょうか。例えば、もし公開鍵暗号方式が突破されれば、TLS/SSL などのセキュアチャネルが解読され、インターネットバンキング、API 通信、社内通信など広範囲に通信傍受の被害が生じる恐れがあります。ほかにも、デジタル署名の偽造によって、取引の改ざん、ソフトウェアアップデートの乗っ取り、法的な否認防止（行為を後から否定すること）の信頼性喪失が懸念されます。また、暗号化データが解読され、長年蓄積された機微情報（PII、企業戦略、取引履歴など）が流出する恐れもあります。

これらはあくまで一例ですが、いずれにしても量子コンピューターの実用化はセキュリティの根幹を揺るがすパラダイムシフトを引き起こしかねません。そのため、将来の暗号課題に対応できる「暗号アジリティ（Crypto Agility）」を備えた基盤の構築が急務です。

耐量子暗号の必要と
グローバルの動向

耐量子暗号とは

このようなセキュリティの危機に対して、注目されるキーワードが「耐量子暗号（PQC：Post-quantum Cryptography、ポスト量子暗号とも）」です。これは量子コンピューターの攻撃にも耐えられる暗号技術の総称です。公開鍵暗号方式が素因数分解や離散対数にまつわる計算の困難さに基づいていたのに対し、PQC は量子コンピューターでも容易に解けないとされる格子問題や符号ベース暗号などの数学的理論に基づいています。

米国国立標準技術研究所（NIST）は、2024 年に PQC 標準（ML-KEM、ML-DSA、FALCON、SPHINCS+）を発表しました。事実上のグローバル基準として位置づけられており、日本の金融庁を含め、各国の規制当局、標準化機関や業界が参照し、合流しつつあります。現在は FIPS 準拠版を策定中で、政府調達・商用環境への導入を推進しています。

米国の PQC 移行計画

米国政府は、2035 年までに重要インフラの PQC 移行完了を目指しています。2022 年には「量子コンピューティング・サイバーセキュリティ準備法」が制定され、暗号資産の可視化と、NIST 基準に沿った PQC 移行計画の策定が義務化されました。また「国家安全保障覚書（NSM-10）」では、HNDL 攻撃に備え、早期の暗号移行と通信経路見直しが指示されています。具体的には、2024 年に NIST 標準発表、2025 年から 2030 年にかけて連邦機関がパイロット実装を開始、2035 年までに重要インフラの完全移行を完了する計画です。

また、米国サイバーセキュリティ・インフラ庁（CISA）は 2023 年に「PQC 移行イニシアチブ」を設立しました。官民連携により、暗号リスク評価、CBOM（Cryptography Bill of Materials：暗号部品表）作成支援、ロードマップ策定、実装 PoC を推進しています。CISA は米国国家サイバーセキュリティセンター（NCCoE）と連携し、量子関連のベンダーと協力して移行ガイドラインを共同整備中です。

その他諸外国における移行計画

欧州委員会（EU）が 2024 年 4 月に協調実施ロードマップを勧告し、加盟国に 2 年以内のロードマップ公表を求めました。2026 年末までにすべて加盟国が初期の移行計画を策定し、高リスクケースは 2030 年、中リスクケースは 2035 年までに移行を完了するスケジュールが示されています。

英国は 2028 年までに移行目標の定義と調査実施、2031 年までに最重要資産の保護完了、2035 年までに全システムの移行完了を目指しています。カナダは 2026 年 4 月までに移行計画策定、2031 年までに優先度の高いシステム、2035 年までに残りのシステムの移行完了を計画しています。

日本の PQC 移行計画

日本では 2024 年 11 月に、金融庁にて「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」が行われ、特に金融機関において量子コンピュータがもたらすリスクに言及し、PQC 対応の実行計画が必要である旨を示しています。また、政府機関等における PQC 対応に関し、2025 年 11 月に「政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議」が「政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）」を公表し、政府機関における移行は原則として 2035 年までに行うことを目指すこととされ、2026 年度に工程表（ロードマップ）を策定することとされました。

企業に求められる
5つのフェーズでのPQC対応

企業にとって、PQC への対応は今後避けられない重要課題です。暗号資産の可視化からセキュリティ運用の構築まで、段階的かつ戦略的な移行が求められます。こうした包括的なアプローチを実現するために、キンドリルでは、5 つのフェーズに基づく包括的な移行を推奨しています。

フェーズ 1：暗号資産の可視化と棚卸し

PQC 移行の第一歩は、組織内のすべてのシステムで使用されている暗号資産を把握することです。どこでどのような暗号化方式が用いられているかを調査し、CBOM（Cryptography Bill of Materials：暗号部品表）と呼ばれる暗号資産の「台帳」を作成します。オンプレミスからクラウドまで調査し、暗号が利用されている箇所をすべて洗い出します。全体像を把握することで、リスク管理の土台を作り上げます。

フェーズ 2：リスクとビジネスインパクトの評価

次にどのシステムから対応すべきかを判断するため、リスク評価を行います。主に「CIA フレームワーク」を用いて評価します。機密性（Confidentiality）では量子解読により秘匿データが漏洩するリスク、完全性（Integrity）ではデジタル署名の偽造による取引・コード改ざんリスク、可用性（Availability）では暗号切替や鍵管理不備によるサービス停止リスクを評価します。例えば認証システムや決済システム、業務システムを分析し、事業継続性を始めとするビジネスインパクトを評価したうえで優先度を決定します。

フェーズ 3：アーキテクチャ設計と PQC 戦略

「暗号アジリティ」の実現に向けた暗号資産の管理基盤を構築します。暗号機能を 1 つにまとめ、各アプリケーションから独立させることで、将来的に新しい暗号方式に切り替える際の影響を最小限に抑えます。また、各サービス・基盤ごとに暗号の管理をベンダーに任せるのか、自社でまかなうのかを明確にし、各ベンダーの対応計画を確認しながら、自社の対応計画にも反映させます。

フェーズ 4：PoC と性能検証

本番環境に導入する前にテスト環境で PQC 対応の影響を検証します。新しい暗号方式を使った場合、通信速度がどれほど遅くなるか、システムの処理能力にどのような影響があるかを測定し、業務への影響を数値で把握します。そのために代表的なユースケースで TLS 1.3 や署名処理を含むハイブリッド環境を構築します。移行に伴うリスクをあらかじめ特定し、対策を講じることが可能です。

フェーズ 5：移行ロードマップとガバナンス

最後に具体的な移行計画と運用体制を整備します。どのシステムをいつ、どの順番で移行するかスケジュールを作成し、必要な人員や予算を見積もります。まずは業務影響の低いシステムで入念な移行検証を実施した後に、インターネットに接続しているシステムや決済システムなど、リスクの高いものから優先的に移行する計画を立てます。また、移行後の運用ルールを定め、開発者への教育、問い合わせ対応の体制、問題発生時のエスカレーション手順などを整えます。継続的な改善の仕組みを作ることで、長期的に安全な暗号管理が可能になります。

PQC対応に欠かせない CBOM生成

社内で用いられている暗号技術を可視化

フェーズ1「暗号資産の可視化と棚卸し」でも触れたCBOMとは、企業のシステムで使用されている暗号技術の使用状況をまとめた台帳（インベントリ）です。具体的には、暗号アルゴリズム、プロトコル、暗号ライブラリ、証明書、デジタル署名、ハッシュ関数などの暗号資産を記録したものです。

ソフトウェア部品表（SBOM）はソフトウェアコンポーネントの可視化を目的としていますが、CBOMは暗号技術のみを対象とします。どのシステムの、どの部分でどのような暗号方式が使用されているかを明らかにすることでPQC対応にて優先するべき領域を的確に定めることができます。

CBOM生成で重要なポイント

CBOMを構築するためには、企業が保有する暗号資産を確実かつ効率的に洗い出すことが不可欠です。こうした取り組みを支えるためには、体系的なプロセスと専門的な支援が求められます。

・ハイブリッド型の手法による網羅的な解析

ツールを用いた自動スキャンとエンジニアによる手動でのソースコード解析を組み合わせた「ハイブリッド型」の手法で暗号資産を可視化・棚卸しします。例えば、インターネット公開系システムには自動スキャンを適用し、メインフレームや基幹システムといったクローズドかつ複雑な要件が含まれがちな環境には手動でのコードレビューを組み合わせることで、短期間で網羅的な解析を行います。

自動スキャンでは、専用のセンサーを使ってトラフィック、アプリケーション、ファイルシステムの3方向から観測し、どこでどのような暗号が使われているかを自動的に把握します。特に攻撃対象になりやすいのは、インターネット接続されているシステムの通信です。

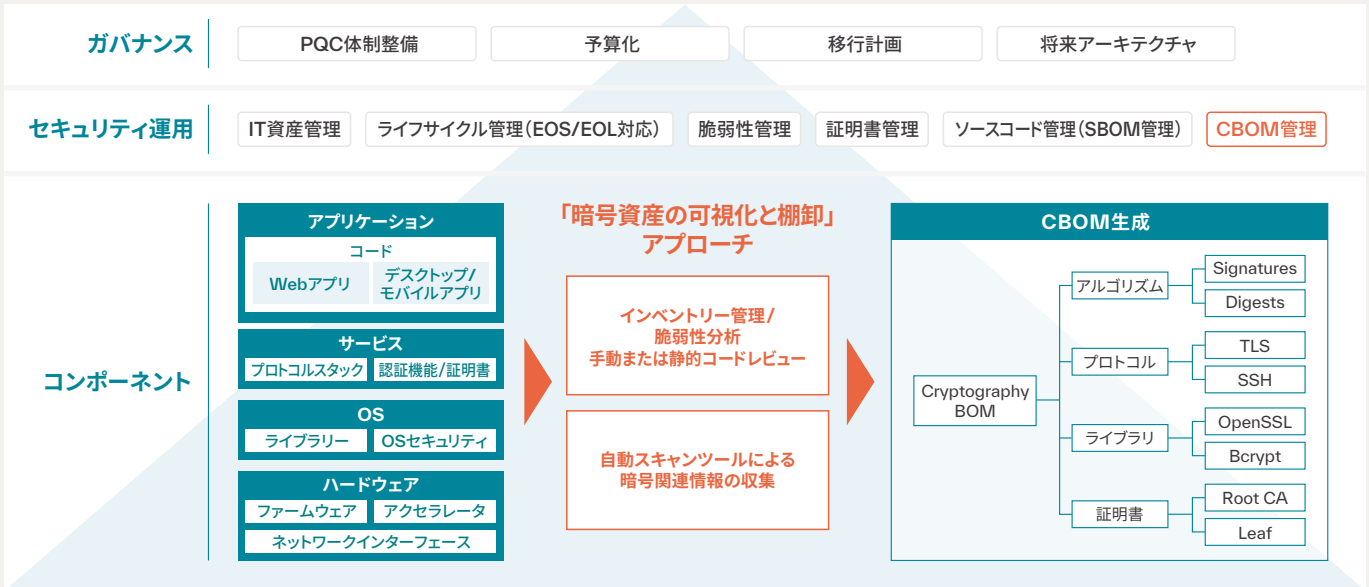
一方で、インターネットなど外部からのアクセスが制限された基幹システム（メインフレームのシステムも含む）には、センサーを設置できない場合があります。こうした環境では、ソースコードの静的解析、担当者へのインタビュー（開発チームや設計担当者への聞き取り）、構成レビュー（各種設定情報の確認）といったマニュアル作業を組み合わせます。重要システムの個別対応は進んでいるものの、何百何千という全システムを網羅したCBOM化に苦慮している企業に、早期かつ現実的に実行可能なアプローチを提供できるのがキンドリルの強みです。

・セキュリティライフサイクルに組み込んだ CBOM管理

CBOMを構築するにあたりもう1つ重要なのは、それを単独の取り組みで終わらせないことです。多くの日本企業ではサポート終了やライフサイクル終了を迎えたレガシーシステムが稼働し、PQCに対応できないケースがあります。

CBOM構築の段階から、レガシーシステムのモダナイゼーションやクラウド移行を含めた将来のインフラ全体を視野に入れることが大切です。他のIT資産管理やライフサイクル管理、脆弱性管理などと同じレイヤーでCBOMの管理を行う必要があります。具体的には、CBOM構築後も定期的なトラフィックスキャンを実施することで、システム変更や設定ミスによって弱い暗号が使われてしまった場合にも、すぐに検出して対応できる仕組みを構築します。

CBOM管理は、既存の運用に無理なく組み込み、追加コストを抑えながら確実に機能させることが重要です。特に、ミッションクリティカルなシステムを抱える企業にとって、運用保守やセキュリティ運用の知見を活かした仕組みづくりが求められます。



システムやセキュリティの運用で豊富な実績を有するキンドリルでは、既存の運用体制に無理なくCBOMを組み込む支援が可能

PQC対応を成功に導くための エコシステム構築

グローバルパートナーとの協業で 最新技術を活用

先述したツールによる CBOM 生成を含む PQC 対応の IT ソリューションに関して、現在ではすでにグローバルに複数の企業が存在しており、これらの企業は米国や欧州の政府機関との技術連携や PoC を行うなど確かな実績があります。キンドリルでは、標準化団体への寄与、業界専門性、技術的専門性、柔軟性など厳格な評価基準に基づいてパートナー企業選定を行い、強固なアライアンス体制を構築しています。

実際に、このような PQC ソリューションでは、どのようなことを実現できるのか、PQC において先進的な取り組みを行うパートナーとキンドリルが提供するソリューションを例に紹介しましょう。このソリューションでは、統合型暗号管理プラットフォームとして、企業の暗号資産 (鍵、証明書、アルゴリズム、暗号ライブラリ、暗号操作など) のインベントリ (CBOM) や量子耐性プロトコルのポリシー管理を含め可視化・制御・保護を実現できます。

特に、証明書のうち SSL/TLS サーバー証明書の有効期限に関しては、業界標準として「最大 47 日」への短縮に向けた動きが進んでいます。これにより更新頻度が激増するため、従来の手動管理は限界を迎えます。PQC 対応と同時にこの証明書の対応に追われないようにするためにも、新たな管理体制の構築を早めに着手することが肝要です。

暗号資産を可視化・制御・保護する仕組み

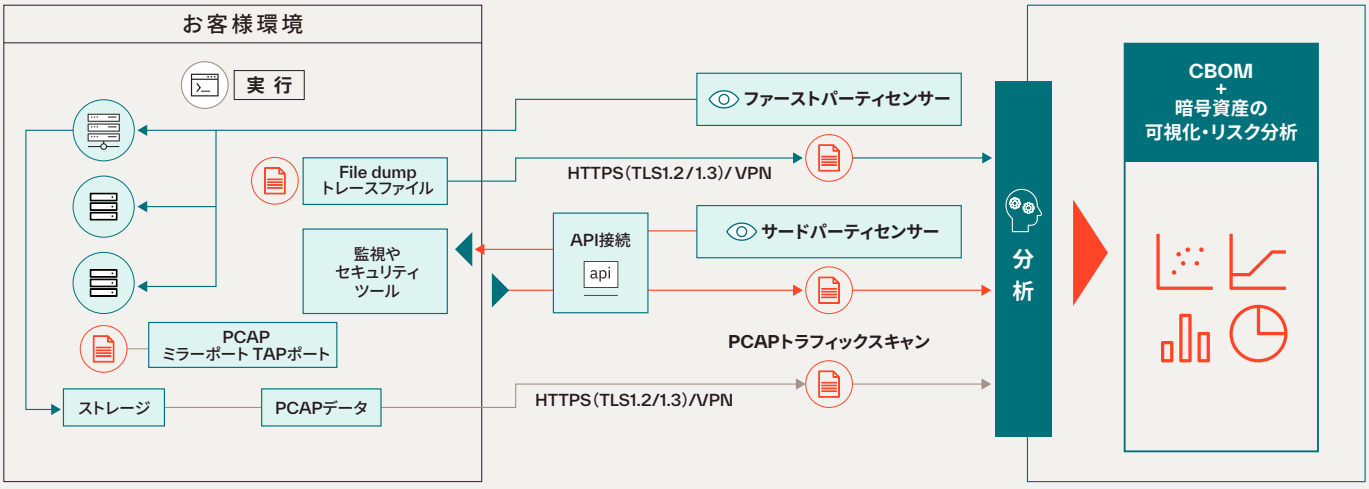
このプラットフォームは 3 つの主要コンポーネントで構成されます。まず「暗号資産検出」を担うコンポーネントでは、複数の検出メカニズムにより包括的な可視性を実現します。例えばネットワーク層では通信中の暗号を識別し、アプリケーション層では暗号ライブラリの検出と脆弱性特定を行い、ファイルシステム層ではローカル環境の暗号資産の検出・解析を実施します。

次に「統合管理」を担うコンポーネントです。暗号インベントリの統合ダッシュボード表示機能を提供し、ポリシー違反の自動修正、非準拠アルゴリズムの特定と継続的な監視といった機能を実装しています。

「暗号制御」は、ポリシー違反への対応と管理された適用を実現します。動的な暗号方式の切り替え機能、API を活用したカスタム統合などの機能を提供します。

カテゴリ	取り込まれる主な項目
鍵 (Keys)	・鍵の種類 (対称/公開鍵等) ・アルゴリズム (AES,RSA,ECC,PQC等) ・鍵長 ・格納場所 (HSM,KMS,ファイル,DB等) ・有効期限・利用状況
証明書 (Certificates)	・証明書種別 (サーバー/クライアント/CA等) ・署名アルゴリズム ・有効期限 ・発行者・サブジェクト情報 ・証明書チェーン ・格納場所
アルゴリズム/ 暗号スイート	・利用アルゴリズム (暗号/ハッシュ/署名) ・TLS暗号スイート ・推奨/非推奨アルゴリズムの利用状況
暗号ライブラリ/ プロバイダ	・利用中の暗号ライブラリ (OpenSSL, Bouncy Castle, liboqs等) ・バージョン情報 ・プロバイダの種類
暗号操作 (Operations)	・暗号API呼び出し (encrypt, decrypt, sign, verify等) ・実装箇所 (どのサービス・アプリで利用されているか)

インベントリとして管理する暗号資産の例



PQC ソリューションの自動スキャンを用いたデータ収集の仕組み

PQC対応に
キンドリルが選ばれる理由

PQC 対応におけるキンドリルの強み

キンドリルは、世界各国の政府機関や主要企業の PQC 対応を手掛けるグローバルパートナーと連携し、最先端のツールやソリューションへのアクセスを実現しています。これにより、全方位的な PQC 対応の実装など、幅広い領域で支援を提供できます。

第二にグローバルの専門家チームによる先進知見の活用です。米国・英国・欧州の量子暗号専門家が日本のプロジェクトを支援し、NIST 準拠の最新動向や各国規制・業界標準に基づいた戦略設計が可能です。グローバルで先行する事例や知見を日本市場に直ちに展開できる体制を整えています。

さらに、キンドリルはメインフレームを含むエンタープライズ企業のミッションクリティカルなシステムに関する豊富な知見を有しており、金融機関など機密性の高い業界にも現実的かつ段階的なアプローチで支援が可能です。PQC 対応を契機として、IT 資産管理やガバナンスの高度化まで、企業の変革を伴走できるのがキンドリルの最大の強みです。

PQC 対応ロードマップ：
1、2 年後の着手では間に合わない

キンドリルでは、PQC 対応の今後のロードマップとして、2025 年から 2035 年までの 10 年計画を想定しています。これはまだ非常に猶予があるように思えますが、米国や欧州の PQC 移行計画を見据えると、2035 年までに対応を完了させるには今すぐにでも着手しなければなりません。特に大手金融機関では、基幹系システムやメインフレーム環境を含む全システムの暗号資産を可視化し、リスク評価を完了させるだけでも数年を要することが想定されます。また、実際のシステム移行にはベンダーとの調整、開発リソースの確保、テスト環境の構築、段階的なリリース計画など複数年にわたる準備が欠かせません。

量子コンピューターの実用化は、社会に対する大きなブレイクスルーをもたらす期待がかかる一方で、セキュリティ対策にも抜本的な変革が求められます。脅威が発生してからの対応ではときはすでに遅く、今から備えるべき重要なテーマであるのです。

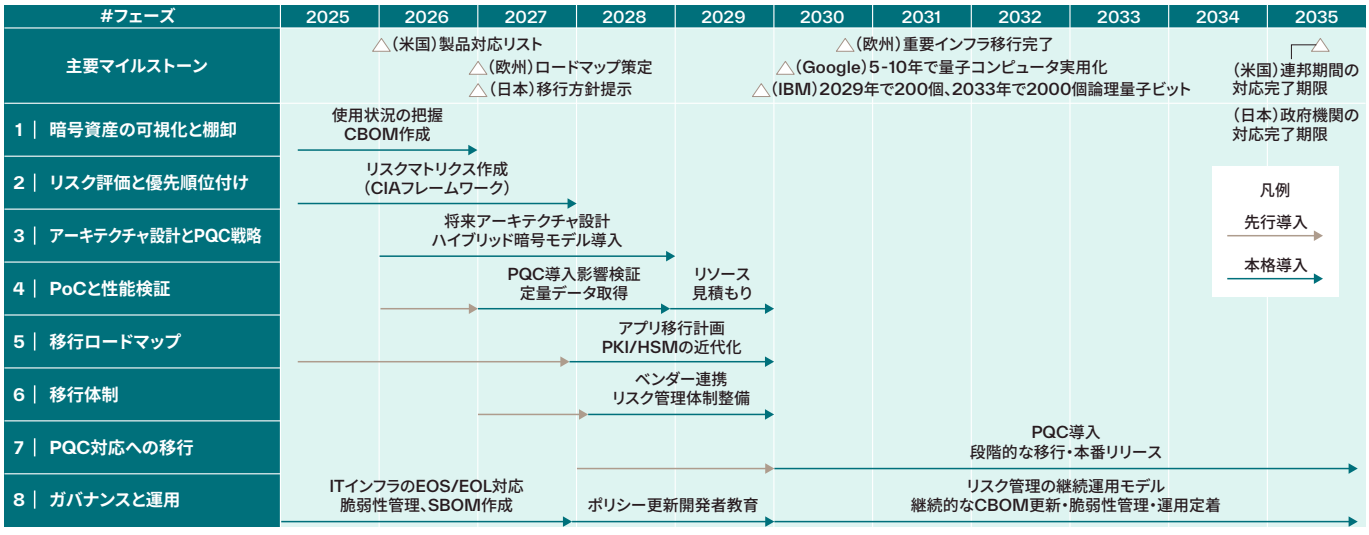
PQC 対応プロジェクトで
キンドリルが提供する成果物

キンドリルは、現状の把握から将来の計画まで一連の PQC 対応を支援しており、主に以下の成果物を提供します。

1. 暗号資産データベース：
CBOM により重要サービスに紐づく暗号資産の全体像を整理したデータベースの構築

2. リスク評価レポート：
CBOM を基に量子リスクの全体像を明示するレポートの作成

3. 移行ロードマップとガバナンス計画：
リスクと重要度に応じた段階的移行に向けた計画の策定、および 2035 年までの実際の PQC 移行に向けた各システムベンターとの綿密な連携支援



2025 年～ 2035 年までの PQC 長期ロードマップ例

執筆

増田 博史
セキュリティ&レジリエンシー事業部 事業部長

成尾 明久
コンサルト・プラクティス事業本部 金融事業部長

吉田 卓
セキュリティ&レジリエンシー事業部
コンサルト・プラクティス・リーダー

詳細情報

最新情報やサービス内容については、キンドリルのウェブサイトをご覧ください。

サイバーレジリエンス
kyndryl.com/jp/ja/services/cyber-resilience

Kyndryl Consult
kyndryl.com/jp/ja/consulting

キンドリルジャパン株式会社
106-6143東京都港区六本木6丁目10-1　六本木ヒルズ森タワー43階

出典

1　IBMが世界初の大規模フォールト・トレラント量子コンピューターを構築する方法

2　歴史的転換点を迎えたサイバーセキュリティ：デジタル時代の複合的脅威への対応