CEPS

EU の量子安全な世界への移行を強化する

技術、市場、ガバナンス、政策上の課題

CEPS はブリュッセルに拠点を置く独立系シンクタンクである。その使命は、欧州と世界が直面する課題に対する建設的な解決策につながる、確固たる政策研究を生み出すことである。

本 CEPS タスクフォース報告書は、「量子安全な世界への EU 移行強化」に関する CEPS タスクフォースの議論を基に作成された。タスクフォースは、産業界の専門家、欧州機構・機関の代表者、学者、研究者、市民社会組織、実務家で構成された。グループの活動は 2025 年 4 月に始まり、5 回に分けて会合を開き、2025 年 11 月まで継続した。

タスクフォースのコーディネーターは、参加者全員の貴重な貢献に感謝する。また、諮問委員会のメンバーであるデンマーク外務省のソフィア・リンドスコフ・ハンセン、ウォータールー大学のミケーレ・モスカ、チューリッヒ IBM ディビジョンのマイケル・オズボーン、ルーヴェン・カトリック大学のバート・プレネル、ロンドン・アラン・チューリング研究所のティム・ワトソンにも謝意を表する。 また、報告者であるスワン・アッシュワース、カロリナ・ポリート、アフォンソ・フェレイラにも感謝する。さらに、報告書ドラフトに対して広範なコメントを寄せたハイメ・ゴメス・ガルシア、マティアス・シュンター、ケビン・ライフステック、ジョン・マットソン、ライマ・ヤンチュテにも謝意を表する。最後に、編集の専門性を発揮したデボラ・マルハーン、ジュリアン・リベール、ダニエル・キャシディ＝デケテラールにも謝辞を述べる。

本報告書の推奨事項は、タスクフォース全メンバーによる共通見解を必ずしも反映するものではない。また、いかなる形においても、各メンバーの所属機構の見解を代表するものではない。メンバー一覧、会議記録、講演者リストは附属書に掲載されている。

推奨引用：Pupillo L. et al. (2025), *Strengthening the EU transition to a quantumsafe world. Technology, market, governance and policy challenges*, Task Force Report, Centre for European Policy Studies, Brussels.

978-94-6138-799-8
© Copyright 2025, CEPS
画像クレジット：www.vecteezy.com

無断複写・転載を禁じる。欧州政策研究センター（CEPS）の事前の許可なく、本書の一部または全部を、電子的、機械的、複写、録音その他のいかなる形式または手段によっても、複製、検索システムへの保存、送信することはできない。

CEPS
Place du Congrès 1, B-1000 Brussels
電話: 32 (0) 2 229 39 11 メール: info@ceps.euwww.ceps.eu

目次

エグゼクティブサマリー 11

1. 一般的な推奨事項 14
2. 金融セクター向け追加のセクター固有の推奨事項 16
3. 公共セクター向け追加の分野別推奨事項 17
4. 防衛セクターにおける追加的な分野別推奨事項 18

第 I 部 序論 20

第 II 部 量子耐性環境における PQC、QKD、QRNG の現状 23

1. 耐量子暗号 23
2. 量子鍵配送（QKD） 23
3. 量子乱数生成器と古典的乱数生成器 25

第 III 部 量子耐性移行モデル 28

1. リスクベースアプローチ 28
2. 耐量子暗号（PQC）の最悪の失敗シナリオ：もし PQC が脆弱だと判明したら？ 30
3. 混合暗号化方式 32
4. 量子耐性 への移行における課題 34

第 VI 部 耐量子技術インベントリ 36

1. アプローチ 36
2. 製品インベントリ 37
3. 暗号インベントリ 37

第 V 部 量子耐性への移行状況：欧州連合（EU、フランス、ドイツ、オランダ） 40

1. 序論 40
2. 欧州連合 40
3. ドイツ 43
4. フランス 44
5. オランダ 44

第 VI 部 量子耐性への移行状況：EU 域外（英国、米国、中国） 46

1. 序論 46
2. 英国 46
3. 米国 47
4. 中国 48

第 VII 部 NIS 協力グループロードマップに関するタスクフォースのコメント 50

1. NIS 協力グループロードマップ 50
2. NIS 協力グループロードマップに関するタスクフォースのコメント 51
第 VIII 部 金融セクターにおける PQC への移行 60
1. 序論 60
2. 金融セクターにおける PQC への移行 60
3. 現行の規制環境（EU、英国、米国） 61
4. 金融セクターにおける耐量子暗号への移行モデル 63
5. 金融セクターにおける取り組み 65
6. 金融セクターにおける PQC 移行のボトルネック 67
第 IX 部：公共セクターにおける量子耐性への移行 69
1. 序論 69
2. 公共セクターにおける PQC への移行 69
3. 公共セクターにおける PQC 移行の技術的ボトルネック 74
4. 社会技術的観点からの移行課題 75
第 X 部　防衛セクターにおける量子安全への移行 78
1. 序論 78
2. 防衛セクターにおける量子技術 78
3. 関連する利害関係者及び量子防衛イニシアチブ 80
4. 防衛セクターにおける耐量子暗号への移行 81
第 XI 部　推奨事項 83
1. 一般的な推奨事項 83
2. 金融セクター向けの追加的セクター別推奨事項 88
3. 公共セクター向け追加のセクター固有推奨事項 89
4. 防衛セクター向けの追加的セクター別推奨事項 90
附属書 I. タスクフォースメンバー及び招待講演者リスト 92
附属書 II 用語集 95
タスクフォースの原則と指針 99

図

図 1. 非公式 CRQC タイムライン（サミュエル・ジャック） 21
図 2. 暗号依存性マッピング 29
図 3. ハイブリッド暗号化メカニズムの展開に関するスペイン国家暗号センターによる図解 33

図 4. LGT の暗号優先度レベル 66
図 5. PKI インフラストラクチャ 70
図 6. PKI における機密性と認証 71

ボックス

ボックス 1. 暗号化の俊敏性とハイブリッド暗号化 31
ボックス 2. ハイブリッド暗号化手法：タスクフォースの見解 33
ボックス 3. EU デジタルウォレットの事例 73
ボックス 4. TLS 1.3 の事例 74
ボックス 5.「Q-Day」を超えた PQC の社会技術的視点：誇大宣伝の役割 76

表

表 1. ランダム性のレベル 25

略語一覧

3DES	三重データ暗号化標準
3GPP	第三世代パートナーシッププロジェクト
AES	高度暗号化標準
ANSSI	フランス情報システム保安庁
API	アプリケーションプログラミングインターフェース
AQHKE	認証付き量子安全ハイブリッド鍵確立
ATM	現金自動預け払い機
BIS	国際決済銀行
BSI	連邦情報セキュリティ庁（ドイツ）
C4ISR	指揮、統制、コミュニケーション、コンピュータ、情報、監視、偵察
CENELEC	欧州電気標準委員会
CEPS	欧州政策研究センター
CISA	米国サイバーセキュリティ・インフラセキュリティ庁
CPU	中央処理装置
CRA	サイバーレジリエンス法
CRQC	暗号関連量子コンピュータ
CV-QKD	連続変数量子鍵配送
DEI	多様性、公平性、包摂性
DORA	デジタルレジリエンス法
ECB	欧州中央銀行
ECC	楕円曲線暗号
ECDSA	楕円曲線デジタル署名アルゴリズム
ECDH	楕円曲線ディフィー・ヘルマン
ECDHE	楕円曲線ディフィー・ヘルマン一時鍵交換
EDA	欧州防衛庁
EDF	欧州防衛基金
EDT	新興技術及び破壊的技術
eIDAS	電子識別、認証及びトラストサービスに関する規則
EMV	ユーロペイ、マスターカード、ビザ
ENISA	欧州連合サイバーセキュリティ機関

ETSI	欧州電気通信標準機構
EU	欧州連合
EUROQCI	欧州量子通信インフラ
FCA	金融行動監視機構
FFIEC	連邦金融機関機構検査協議会
FIPS	米国連邦情報処理標準
FN-DSA	NTRU 格子ベースデジタル署名アルゴリズムを用いた高速フーリエ変換
FS-ISAC	金融サービス - 情報共有・分析センター
GDPR	一般データ防御規則
GPS	全地球測位システム
HQC	ハミング準巡回
HSM	ハードウェアセキュリティモジュール
HTTPS	ハイパーテキスト転送プロトコルセキュア
IEC	国際電気標準会議
IETF	インターネット技術タスクフォース
IKEV2	インターネット鍵交換プロトコルバージョン 2
IND-CPA	選択平文攻撃下での識別不能性
IPSEC	インターネットプロトコルセキュリティ
ISACA	情報システム監査・管理協会
ISO	国際標準化機構
ITU-T	国際電気通信連合 – 電気通信標準化部門
KDF	鍵導出機能
KEM	鍵カプセル化機構
LMS	レイトン・ミカリー署名
LTS	長期サポート
MAD	磁気異常検出器
MAD-XR	磁気異常探知機 – 拡張機能
ML-KEM	モジュール格子鍵カプセル化機構
ML-DSA	モジュール格子ベースのデジタル署名アルゴリズム
NATO	北大西洋条約機構
NCCOE	米国国立サイバーセキュリティ・センター・オブ・エクセレンス

NCSC	英国国家サイバーセキュリティセンター
NGCC	次世代商用暗号アルゴリズム
NIS	ネットワークと情報システム
NIS2	ネットワーク及び情報セキュリティ指令 2
NISQ	ノイズの多い中間規模量子
NIST	米国国立標準技術研究所
NSA	米国国家安全保障局
NSM-10	国家安全保障覚書 10
OCSP	オンライン証明書ステータスプロトコル
ORAM	無知ランダムアクセスメモリ
OT	運用技術
OTNSEC	光伝送ネットワーク用独自セキュリティプロトコル
PIR	個人情報検索
PKI	公開鍵基盤
PNT	精密航法・測位
PQC	耐量子暗号
PRNG	擬似乱数生成器
PSK	事前共有鍵
PSI	プライベート共通集合
QDNL	量子デルタ NL
QKD	量子鍵配送
QRNG	量子乱数発生器
研究開発	研究開発
RSA	リベスト・シャミア・アドルマンアルゴリズム
S/MIME	セキュア/多目的インターネットメール拡張
SAGE	セキュリティアルゴリズム専門家グループ
SBOM	ソフトウェア部品表
SD-WAN	ソフトウェア定義ネットワーク
SHA	セキュアハッシュアルゴリズム
SLH-DSA	ステートレスハッシュベースデジタル署名アルゴリズム
SSH	セキュアソケットシェル

SSL	セキュアソケットレイヤー
SWIFT	世界銀行間金融通信協会
TLS	トランスポート層セキュリティ
TQC	大西洋横断量子コミュニティ
TRL	技術成熟度レベル
TRNG	真の乱数発生器
UK	英国
米国	米国
VPN	仮想プライベートネットワーク
WEF	世界経済フォーラム
XMSS	拡張マークル署名方式

序文

本報告書は、欧州政策研究センター（*CEPS*）の「量子耐性世界への *EU* 移行強化タスクフォース」における議論に基づいている。同タスクフォースは、産業界の専門家、欧州機構・機関の代表者、学者、研究者、市民社会組織、実務家らで構成された（参加者リストは附属書 *1* 参照）。グループの活動は *2025* 年 *4* 月に始まり、*5* 回の会合を経て *2025* 年 *11* 月まで継続した。

本報告書は *11* のパートで構成されている。序論で背景を説明した後、パート *II* から *VI* では、欧州連合（*EU*）における量子セキュリティへの移行に関連する主要な課題について、技術、市場、ガバナンス、政策の問題に焦点を当てて紹介する。第 *VII* 部では、ネットワークと情報システム（*NIS*）協力グループが *2025* 年 *6* 月に提出した、耐量子暗号への移行に関する調整実施ロードマップに対するタスクフォースのコメントを紹介する。第 *VIII* 部から第 *X* 部では、金融、公共、防衛の各分野における具体的な移行に焦点を当てる。第 *XI* 部では、*EU* における量子セキュリティへの移行を強化・加速するための政府および企業向けの推奨事項を概説する。

タスクフォースのコーディネーターとして、この作業に参加したすべての関係者による貴重な貢献に感謝したい。諮問委員会のメンバー、デンマーク外務省のソフィア・リンドスコフ・ハンセン氏、ウォータールー大学のミケーレ・モスカ氏、チューリッヒの *IBM* リサーチディビジョンのマイケル・オズボーン氏、ルーヴェン・カトリック大学のバート・プレネル氏、ロンドンのアラン・チューリング研究所のティム・ワトソン氏に感謝する。

また、共同報告者であるスワン・アッシュワース、カロリナ・ポリート、アフォンソ・フェレイラによる多大な労作にも謝意を表する。さらに、報告書ドラフトに対し広範なコメントを寄せてくれたハイメ・ゴメス・ガルシア、マティアス・シュンター、ケビン・ライフステック、ジョン・マットソン、ライマ・ヤンチュテにも感謝する。本作業は共同の取り組みであり、他のタスクフォース参加者も報告書の特定セクションへのコメントを通じて専門知識を直接提供している。また、タスクフォースの議論に貢献した招待講演者にも感謝する。

ロレンツォ・プピッロ
タスクフォース調整役兼報告責任者
上級研究員兼サイバーセキュリティ@CEPS イニシアチブ責任者

CEPS、ブリュッセル
2025 年 12 月

エグゼクティブサマリー

2025 年 4 月、CEPS は「EU の量子安全世界への移行強化タスクフォース」を発足させた。このイニシアチブの目的は、欧州が量子安全へ移行する際に生じる技術的、市場的、ガバナンス的、政策的な課題に注目を集めることだった。

マルチステークホルダー・プラットフォームとして設計された本タスクフォースには、民間組織 11 団体、EU 機構・機関 11 機関、大学・シンクタンク 7 機関、国家研究機関 1 機関、市民社会組織 1 団体が参加した（参加者全リストは附属書 I 参照）。

同グループは、政府と企業が EU の量子耐性強化への移行を加速・強化するための実践的ガイドライン策定を目指した。議論では、このプロセス実施に伴う技術的・管理的・ガバナンス上の課題が取り上げられた。これらの取り組みの結果、EU 機構・加盟国・民間セクター・研究コミュニティに向けた一連の政策推奨事項がまとめられ、欧州の量子レジリエンスへの安全な移行を導く指針となった。

耐量子暗号（PQC）への移行は、欧州にとって差し迫った戦略的課題である。官民双方の慎重な調整と長期的な計画が必要だ。現行の暗号システムを破る量子コンピュータは、早ければ今後 10 年以内に登場する可能性がある。しかし PQC への移行は長期かつ複雑なプロセスである。過去のセキュリティ標準移行の経験から、こうした変革には 10 年から 15 年を要することが示唆されている。

この緊急性にもかかわらず、欧州連合サイバーセキュリティ機関（ENISA）と情報システム監査管理協会（ISACA）による最近の調査では、欧州のステークホルダーの大半が依然として準備不足であることが示されている。 耐量子ソリューションへの投資を開始しているのはごく一部であり、全体的な認識は依然として低い。加盟国レベルでは、ドイツ、フランス、オランダが、国家ロードマップとネットワークと情報システム（NIS）協力グループの両方を通じて、ガイダンスの発行や PQC パイロットプロジェクトの立ち上げなど、主導的な役割を果たしている。しかし、EU 全体の進捗は依然として不均一であり、EU は米国のような首尾一貫した統一的な移行フレームワークをまだ備えていない。

こうした背景から、タスクフォースは、以下の原則に基づき、量子セキュリティへの移行プロセスを強化するよう求めている。

1） 体系的な変革としての量子安全への移行

量子安全な暗号技術への移行は、単なる日常的な技術的アップグレードではなく、システムレベルでの包括的な変革と捉えるべきである。 PQC への移行は、暗号ライブラリの更新だけにとどまらない。新製品のバージョン統合、アプリケーション・プログラミング・インターフェース（API）の変更、ソフトウェア開発ライフサイクルの適応、場合によっては中核的なビジネスプロセスの再設計も伴う。また、サプライヤー、顧客、エコシステムとの関係を積極的に管理することも求められる。これは、長期的な計画、熟練した人材の育成、持続的な組織変革を必要とする、経営上の大きな課題である。

2） 「Q-Day」という物語の枠を超えよ

公の議論では、量子コンピューターが従来の暗号技術を無効化する仮説上の瞬間を「Q-Day」と呼ぶことが多い。この枠組みは注目を集めるが、誤解を招く。量子能力は津波のように一気に到来するのではなく、初期のマシンが特定の鍵を破る段階を経て、より広範な能力が発展する漸進的で不均一なプロセスとして現れる。より現実的な視点は「Q-period」であり、量子技術と標準開発の実際のペースに沿った、均衡のとれた適応的な移行戦略を支えるものである。

3） 移行の中核となる耐量子暗号

PQC（ポスト量子暗号）は量子耐性への移行を支える基盤だ。これらのアルゴリズムは量子コンピューターからの攻撃に耐えるよう設計されており、規制当局や標準化団体から短期的・中期的には唯一の実用可能な解決策として広く認められている。他の量子技術はより専門的な役割を担う：

- 量子鍵配送（QKD）は公開鍵暗号の直接的な代替ではなく、特定の高度なセキュリティ環境向けに多様な階層的保護を提供する補完技術である。

- 量子乱数生成器（QRNG）は認証可能なエントロピー品質を提供し、量子由来の乱数を暗号スタックに組み込み、公認認証スキーム下で妥当性確認することを保証する。

4) リスクベースの移行モデル

数十億台のデバイスを量子耐性標準に移行するには、以下の要素を含む構造化されたリスクベースのアプローチが必要だ：

- 暗号の俊敏性：暗号システムをモジュール式に設計し、暗号コンポーネントの容易な交換を可能にする。

- 暗号技術の依存関係への認識：ほとんどの組織はサードパーティベンダーに大きく依存しているため、サプライチェーンの依存関係を理解し管理することが極めて重要だ。組織はサプライヤーと連携し、量子耐性機能の明確なタイムラインを要求し、サプライチェーンの準備状況を監視しなければならない。

- 暗号技術と製品インベントリ：効果的な計画は、ソフトウェア、ハードウェア、API、サービスを含む内部・外部の依存関係を網羅的に把握することから始まる。重要システムは早期移行の優先対象とすべきだ。

- ハイブリッドソリューション：ハイブリッド暗号として知られる、従来のアルゴリズムと量子耐性のあるアルゴリズムの共存により、相互運用性と冗長性を実現できる。グローバルな相互運用性を確保するためには、標準化団体を通じてハイブリッドソリューションを標準化する必要がある。タスクフォースは、PQC/従来型やPQC/QKD など、複数の暗号メカニズムを組み合わせてレジリエンスを高める「コンテキストを認識し、技術的に包括的なアプローチ」を包含するよう、ハイブリッドソリューションの定義を拡大することを推奨している。

ポスト量子暗号に関する欧州ロードマップ（以下、「ロードマップ」）の設計と実施に関しては、NIS 協力グループロードマップ（本報告書の第 VII 部で入手可能）への具体的な貢献に加え、タスクフォースは、以下の行動の必要性を強調する。

- 量子セキュリティを最初からデジタルシステムに統合する：欧州委員会と加盟国は、デジタルシステム（欧州デジタル ID ウォレットなど）が最初から量子セキュリティに対応するよう設計されていることを保証すべきである。

- ロードマップを量子移行戦略および既存の法律と連動させる：ロードマップはマイルストーンとスケジュールを定義するが、支援戦略は加盟国、ベンダー、機構がそれらをどのように達成するかを明確にする必要がある。

- ロードマップ間の整合性と一貫性を確保すること：EU レベル及び国家レベルで複数の量子耐性ロードマップが策定される中、欧州委員会、加盟国、標準化団体は、タイムライン、依存関係、目標における一貫性を確保するため、取り組みを調整しなければならない。米国及びその他の G7 パートナーとの調整も同様に重要である。

- ロードマップへの並列化強化の導入：ロードマップの現行構造は段階的・直線的アプローチを暗黙に前提としており、意図せずボトルネックを生む恐れがある。本タスクフォースは進捗加速とシステムリスク低減のため、ロードマップへの並列化強化導入を推奨する。

最後に、本報告書は量子安全への移行プロセス全体を通じた認識向上、協力、効果的なガバナンスの重要性を強調する。組織内における能力構築、スキル開発、専門的な暗号管理部門の設置を求めている。

具体的には、本タスクフォースは政策立案者、民間セクター、研究コミュニティに対し、以下の通り要約される推奨事項を行う。[1]

[1] 勧告の拡張版は第 XI 部に掲載されている。

1. 一般的な推奨事項

GR1. 暗号の俊敏性を開発する

量子安全な暗号化を追求するにあたり、数十億台のデバイスの暗号化手法を移行するには、技術的、組織的、政策的な観点からの設計を必要とする特定のモデルが求められる。このような取り組みには、リスクベースのアプローチが不可欠である。このアプローチは、測定されたリスクとニーズに基づく暗号アジリティの原則を中心に据えるべきである。

GR2. 暗号依存性の対応についてサプライヤーと連携する

多くの組織はサードパーティ製品・サービスに大きく依存しており、サプライチェーン上の依存関係が移行の制約と可能性を決定することが多い。重要な製品や依存関係が組織の直接的な管理範囲外にある場合、PQC への移行はしばしば停滞する。 ソフトウェアベンダーやサプライヤーは段階的なアップグレードスケジュールを採用しており、多くの暗号化コンポーネントは複雑にネストされた依存関係の中に埋もれている。この問題に対処するには、組織はサプライヤーとの強固な連携、量子耐性機能に関する明確なタイムライン要求、サプライチェーンの準備状況を追跡する仕組みが必要だ。

GR3. 暗号技術と製品のインベントリ構築・維持

耐量子暗号への移行に備え、組織は暗号資産と製品インベントリの構築・維持方法に注力しつつある。インベントリ構築は優先すべき課題であり、まず最も関連性の高いユースケースに焦点を当てるべきだ。こうしたインベントリの優先順位付けはロードマップ構築を支援し、移行活動の文脈を提供する。 暗号資産のインベントリ作成は重要な作業であり、これまでの分析に基づけば、移行が必要な対象の全体像をより深く理解する助けとなる。そこから生まれるのは厳格な設計図ではなく、初期段階での計画立案、技術チームとガバナンスチーム間の連携、そしてインベントリが何を捕捉すべきか、その理由を明確に理解することで形作られる一連の指針となる実践手法である。

暗号資産のインベントリは、組織のシステム全体で暗号技術がどこでどのように使用されているかを詳細にマッピングするものである。その目的は、現在使用されている暗号アルゴリズムを識別すること（Rivest-Shamir-Adleman アルゴリズム（RSA）、楕円曲線暗号（ECC）、Advanced Encryption Standard（AES））、それらの実装コンテキスト （コード署名、コミュニケーション用トランスポート層セキュリティ（TLS））、 量子耐性ステータス（レガシーまたは PQC）、暗号モジュールと標準の依存関係を特定することにある。

製品インベントリは、組織が使用する外部製品・サービス・ハードウェア（つまりサードパーティプロバイダ）に焦点を当て、これらの製品の暗号特性をマッピングする。新規ソフトウェア・ハードウェア・クラウドサービスを購入する際、組織はベンダーに対し、製品で使用されている暗号アルゴリズムとプロトコルの開示を要求する。これには耐量子アップグレードのロードマップが含まれる可能性がある。

GR4. 量子耐性をデジタルシステムに最初から組み込む

欧州委員会と加盟国は、デジタルシステム（欧州デジタル ID ウォレットなど）が最初から量子耐性を備えるよう設計することを保証すべきだ。言い換えれば、暗号技術を必要とする新たなデジタルサービスやシステム、標準が導入される場合、その暗号技術は初日から量子耐性を持つべきだ。これは、ポスト量子暗号を将来的な後付けとして扱うのではなく、システムアーキテクチャ、認証、調達プロセスに組み込むことを意味する。

GR5. 誇大宣伝を超えて：Q-Day から Q-period へ

PQC に関する議論は、強力な量子コンピューターが古典暗号を無効化する瞬間「Q-Day」の脅威によって頻繁に盛り上がる。動員のための物語としては有用だが、この枠組みは問題を歪めるリスクがある。量子能力は津波のように突然到来するのではなく、漸進的かつ不均一なプロセスとして現れる。 まず少数のマシンが特定の鍵を破り、その後より広範な応用へと拡大していく。したがって、問題を「Q-Day」ではなく「Q-period」として捉える現実的な枠組みは、量子能力の実際の進化と標準の準備状況に合わせた、バランスの取れた移行戦略を支えるだろう。

GR6. 耐量子暗号移行ロードマップ（[2]）と量子移行戦略・既存法規の連携

調整されたリスク認識型移行戦略なしに EU の量子耐性ロードマップを推進することには重大なリスクがある。ロードマップは必要なマイルストーンとその期限を明記すべきだが、加盟国・ベンダー・機構がそれらを達成する方法を定義できるのは支援戦略のみである。標準・ 認証スキーム・相互運用性枠組み・試験インフラが同期しなければ、規制が準備態勢を追い越す恐れがある。

GR7. ロードマップ間の整合性と一貫性を確保する

現在、EU レベルおよび各国レベルで、ポスト量子暗号、量子通信、関連インフラ構想を網羅する量子耐性移行のための複数のロードマップが策定・議論されている。各ロードマップは貴重な優先事項と指標となるマイルストーン（例：2026 年、2030 年、2035 年）を設定しているが、適切に整合されなければ、要求事項や実装が断片化、あるいは互換性を欠く事態を招くリスクがある。 欧州委員会は、加盟国や標準化団体と連携し、タイムライン、依存関係、目標の一貫性を確保するため、ロードマップ間の調整を推進すべきである。

世界的な整合性を確保し分断を回避するため、EU は米国やその他の G7 経済圏とも緊密に連携し、量子耐性移行に向けたロードマップ、技術要件、タイムラインの整合を図るべきだ。

GR8. ロードマップへの並列化の導入

ロードマップの現行構造は、段階的あるいは直線的なアプローチを暗黙に前提としており、特にある分野の進展が別の分野の完了に依存する場合、意図せずボトルネックを生む可能性がある。EU 全域における暗号システムの複雑性と多様性を考慮し、進展を加速しシステムリスクを低減するため、ロードマップへの並列化の強化を推奨する[3] 。

---

[2] 量子暗号移行のための調整済み実施ロードマップ（以下、ロードマップと呼ぶ）

[3] 調整と整合性を維持しながら並行性を高めるための具体的かつ実行可能な提案は、第 XI 部に記載されている。

GR9. 認識向上、協力、ガバナンス強化の促進

サイバー空間では、すべての国家が国境を越えてつながり、相互に依存している。この移行においても同様だ。したがって、加盟国は組織、事業体、関係者が知識と経験を共有できる環境やコミュニティを構築すべきである。

加盟国は透明性のある移行計画で率先垂範すべきだ。政府の移行ロードマップ（タイムライン、マイルストーン、予算を含む）を公表し定期的に更新することで、知識共有とベストプラクティスの促進を図る。ロードマップは「利害関係者」の定義を省庁・規制機関・技術専門家（ ）に限定せず拡大すべきだ。市民社会、マイノリティネットワーク、草の根の多様性・公平性・包摂性（DEI）団体は単なる「相談先」ではなく共同リーダーとして認識されるべきである。

PQC 移行ロードマップは、市民が情報を受け取るだけでなく戦略形成に積極的に関与できる仕組み（市民会議、協議パネル、定期的な透明性ある更新）を確立すべきだ。2030 年までに国境を越えたサービスにおける PQC の相互運用性を検証するため、EU レベルでの共同パイロットプロジェクトを推進する。

ENISA 傘下に官民共同の PQC 移行監視機関を設置し、進捗を監視するとともに、必要に応じてスケジュールの前倒しを推奨することを提案する。

GR10. 技能開発と管理構造の促進

最後に、移行の成功は管理構造とスキル開発にも依存する。暗号技術の移行はもはやニッチな技術専門家の領域ではなく、クロスファンクショナルチーム、透明性のあるガバナンス、明確なプロセス所有権を必要とする。組織は明確な事業レベルの優先事項から始まる、確立され資金提供され権限を与えられたプログラムを持つべきだ。現在の進捗の多くはボトムアップであり、経営陣の支援が不足している。

2. 金融セクター向け追加のセクター固有の推奨事項

FS1. 臨時的な PQC ガバナンス体制を構築する

ガバナンス体制は極めて重要だ。企業は PQC 移行のための運営委員会またはタスクフォースを設置すべきである。この組織は暗号技術の使用状況を把握し、標準を追跡し、事業優先度と規制要件に沿った移行スケジュールを設定する。多くの大手銀行は既にこの目的で内部の「量子リスク」または「暗号技術対応」チームを編成している。

FS2. ベンダーやパートナーとの連携強化

金融セクターの暗号インフラは、単一機構の枠を超えて存在する。ベンダー、サードパーティサービスプロバイダー、ハードウェア製造事業者を含む。これらの主体に依存しているのだ。主要なボトルネックは、技術プロバイダの PQC 対応準備状況である。したがって、企業は早期にベンダーと関わり、ロードマップに PQC サポートが含まれるよう確保すべきだ。新規調達においては、 設計による暗号アジリティを効果的に求めることになる。 金融機関が共通の調達標準で合意できれば、ベンダーのインセンティブが高まり、分断化が軽減される可能性がある。

FS3. 金融セクター基盤インフラのアップグレード

企業は基盤インフラをアップグレードし、ハードウェアセキュリティモジュール（HSM）、暗号ライブラリ、仮想プライベートネットワーク（VPN）アプライアンス、その他の関連コンポーネントが量子耐性アルゴリズムをサポートできるようにする必要がある。重要な推奨事項として、進行中の広範な IT 近代化イニシアチブの一環としてアルゴリズムを近代化することが挙げられる。例えば、銀行がサービスをクラウドに移行したり、コアバンキングシステムを置き換えたりする場合は、暗号の俊敏性に関する考慮事項を最初から組み込むべきである。

FS4. リスクアセスメントに基づく行動の優先順位付け

移行の規模を考慮すると、全てを一度に変更することは不可能だ。どのシステムとデータを優先的に保護すべきかを決定するには、リスクベースのアプローチが不可欠である。このプロセスは暗号資産の棚卸しから始まる。 コストがかかり、実際の移行開始後に陳腐化する恐れのある包括的なインベントリ作成を目指すのではなく、事業レベルのリスクとリターンの分析に基づき、事業の特定部分のみを移行対象とするインベントリを作成するトップダウンかつリスクベースのアプローチを推奨する。特定の依存関係は維持する必要があるものの、これにより移行中に事業の正当性と価値を識別・追跡できる。

FS5. 緩和オプションの費用対効果分析を実施する

解決策は全て同等ではない。ハードウェア変更を伴うもの（ハードウェア上のハイブリッドソリューション採用、量子乱数生成器や QKD リンクの展開）もあれば、純粋にソフトウェアベースのもの（PQC アルゴリズムへの切り替え）もある。 タスクフォースは、大規模銀行における暗号技術の完全移行には数億ドル規模の費用がかかる可能性があると指摘している。取締役会や経営陣にとって、達成されるリスク低減に対して支出を正当化するには、定量化されたリスクアセスメントが不可欠である。何もしない場合のコスト（将来の侵害による潜在的な罰金、損失、評判の毀損など）が移行コストを上回る場合、PQC 投資のビジネスケースは明らかになる。

FS6. 組織的・技術的ギャップの克服

金融機関は全レベルで暗号技術のスキルと認識が不足している。暗号技術は従来 IT 分野のニッチ領域だったが、今や の主流課題となる必要がある。多くの金融機関では暗号技術を静的なユーティリティとして扱う文化が根付いている。この考え方を継続的な暗号技術の改善へと転換することが組織的課題だ。

3. 公共セクター向け追加の分野別推奨事項

PS1. PKI およびデジタル ID エコシステム全体での段階的移行計画を実施する

公共行政機関は、公開鍵基盤（PKI）とデジタル ID システムのアップグレードに、調整されたリスクベースのアプローチを採用すべきだ。 移行は、国民識別登録システム、越境認証サービス、公共の信頼を支える認証局など、最も重要かつ影響力の大きい構成要素から開始し、その後依存システムへ拡大すべきである。行政機関は、依存関係をマッピングし量子リスクに最も晒されている領域を特定するため、包括的な暗号技術インベントリを実施すべきである。このマッピングは、短期的な継続性のためのハイブリッド暗号技術と、長期的な耐量子標準の採用を組み合わせた段階的な移行ロードマップの策定に活用されるべきである。

PS2. 分断化とサービス中断を防ぐため認証層を同期させる

量子移行期における信頼性と相互運用性を維持するため、認証システム、ルート証明書、中間証明書、ブラウザ、失効サービスは連動して進化させる必要がある。欧州委員会と各国当局は移行を調整し、これらの層全体で同時対応を確保すべきだ。これには性能影響のベンチマーク、相互運用性テストと負荷テストの実施、大規模証明書や計算負荷増加に対応するフォールバック機構の確立が含まれる。同期化されたアプローチにより、実装の断片化を防ぎ、サービス停止を最小限に抑えられる。

PS3. 国境を越えたロードマップの調整と国家移行戦略の整合化

欧州委員会と加盟国は、量子耐性移行のための共同ロードマップを策定し、各国の PKI アップグレード、タイムライン、政策枠組みを整合させるべきだ。この調整は国境を越えた相互運用性に焦点を当て、信頼チェーン、認証プロセス、ガバナンスモデルが EU 域内で一貫性を保つことを保証する。定期的な報告と共有された準備状況のベンチマークを制度化し、各国のインフラが同期して進化し相互信頼を維持することを確保すべきだ。

PS4. 量子移行を社会技術プログラムとして調整管理する

公共セクターにおける耐量子移行は、純粋な暗号化アップグレードではなく、エコシステム全体での取り組みとして取り組むべきだ。欧州委員会と加盟国は、技術機関、規制当局、標準団体、産業関係者を結集する調整メカニズムを確立し、移行を導くべきである。移行計画は、レガシーシステムや運用技術上の制約も考慮し、アップグレードのスケジュール設定や並行する標準更新を可能にすることでボトルネックを防止しなければならない。

4. 防衛セクターにおける追加的な分野別推奨事項

DS1. 耐量子移行ロードマップの策定

防衛産業関係者は、政府の政策マイルストーンと産業展開を同期させる耐量子移行ロードマップを策定すべきだ。このロードマップは、包括的な暗号技術インベントリの義務化、ミッションクリティカルかつ高リスクシステムの優先順位付け、PQC 実装のクロスベンダーテストの調整を規定すべきである。共通の移行ベンチマークを開発することで、防衛サプライチェーン全体の相互運用性が向上し、重複作業が防止され、重要な運用を妨げることなく、レガシーな指揮・統制・通信インフラの近代化が可能となる。

DS2. 産業連携の支援

機構関係者は、欧州のバリューチェーンを優先し非 EU サプライヤーへの依存を減らす資金調達メカニズムを通じて、防衛プライム企業、量子産業の中小企業、研究機関間の産業連携を支援すべきだ。

DS3. サプライチェーン依存性の解消

同様に、欧州の関連機構（欧州防衛庁（EDA）、欧州委員会、欧州防衛基金（EDF）など）は、サプライチェーンの依存性に対処すべきだ。現在、いくつかの主要な量子アルゴリズムやハードウェア部品は米国やアジ

アに由来している。欧州の関係者は、欧州における独自の量子アルゴリズム、フォトニクスプラットフォーム、極低温技術の開発を優先すべきだ。

DS4. 官民量子イノベーション枠組みの正式化

国際的・欧州の防衛機構（EDA、NATO、EDF）は、既存の防衛請負業者と新興企業・学術研究所を結ぶ官民量子イノベーション枠組みを正式に構築すべきだ。これらの連携には、共有テストベッド、機密・公開両方の研究開発（R&D）トラック、技術移転加速のための共同出資実証機を含めるべきである。 優先度は、デュアルユースの量子センシングおよびコミュニケーションシステムに置くべきであり、民間 R&D（量子フラッグシップまたは国家プログラムによる）が防衛用途に適応されることを確保する。

DS5. 構造化されたパイロットから認証までの経路を確立する

運用段階に向けた新興量子システムの妥当性確認のため、EU と NATO はパイロットから認証までの体系的な経路を確立すべきだ。OPENQKD のようなプログラムは恒久的な量子防衛試験基盤へと発展させ、企業（例：タレス、レオナルド、中小企業）が軍事条件下でプロトタイプを試験できるようにする。 その結果は、欧州標準化団体（欧州電気通信標準化機構（ETSI）、ENISA）に直接反映され、セキュリティと相互運用性のベンチマークを定義すべきである。これにより、展開までの時間を短縮し、信頼できる欧州のソリューションを確保する。

DS6. 防衛量子技術研究へのインセンティブ

防衛量子技術の研究を促進するには、安全な知識共有メカニズム（機密研究コンソーシアム、モジュール式出版、機密解除期間など）を確立することが不可欠である。これにより、研究者は防衛上の制約に抵触することなく、学術的キャリアを継続できる。

第 I 部 序論

耐量子暗号への移行は、欧州にとって重大かつ緊急の課題であり、官民双方の慎重な調整と長期的な計画を必要とする。現行の暗号標準を脅かす可能性のある量子コンピュータが早ければ次の 10 年以内に実用化される可能性がある一方で、耐量子暗号への移行は決して即座に実現するものではない。セキュリティ標準移行の過去の経験から、このような変革には 10 年から 15 年を要することが示されている（例：トランスポート層セキュリティ（TLS）移行[4]）。

この緊急性にもかかわらず、欧州連合サイバーセキュリティ機関（ENISA）による EU 加盟 27 カ国 1350 以上の組織を対象とした調査（[5]）を含む最近の調査では、欧州のステークホルダーの大半が依然として準備不足であることが明らかになっている。耐量子ソリューションへの投資を開始している組織はごく一部であり、全体的な認知度も低い。これは、導入の遅れというだけのことではない。重要な分野の事業者のかなりの部分が、量子安全対策への投資をまったく計画していないのだ。この認識は、民間部門のデータも裏付けている（量子コンピューティング戦略、量子安全への移行を含む戦略を定義しているのはわずか 4% である）。[6]。欧州では、ドイツ、フランス、オランダが、国家ロードマップとネットワークと情報システム（NIS）協力グループの両方を通じて、ガイダンスの発行とポスト量子暗号（PQC）パイロットプロジェクトの実施において主導的な役割を果たしている。しかし、EU 全体では、これらのロードマップの採用は依然として不均一であり、EU 全体としては、米国に見られるような首尾一貫した統一的な量子移行の枠組みが依然として欠けている。

こうした背景のもと、欧州政策研究センター（CEPS）の「EU の量子耐性世界への移行強化タスクフォース」は、民間セクター代表者、欧州機構、学術界、市民社会間の対話の場を提供した。目的は、欧州が量子レジリエンスへ安全に移行するための技術的道筋、ガバナンス メカニズム、政策推奨事項に関する合意形成を図ることである。

現代暗号を破る完全機能の暗号関連量子コンピュータ（CRQC）の実現にはまだ数年あるいは数十年を要する可能性があるが、リスクの重大性と必要な移行の規模を考慮すれば、即時かつ持続的な準備が不可欠である[7]。量子研究、特にクレイグ・ギドニーの最近の研究では、エラー訂正技術とアルゴリズム技術の進歩により、RSA-2048 を破るのに必要な物理量子ビットの推定数が、2019 年の約 2000 万個から現在では 100 万個未満へと着実に減少している。エラー率が低下しコードが効率化されるにつれ、この圧縮傾向は加速する。つまり、同等の処理能力を発揮する量子ビット数が減少し、リスクの進展がハードウェアのスケールアップを上回る速度で進むことを意味する。改善が続くと仮定すれば、改良が進むごとに必要な量子ビット数は大幅に削減され、物理的な量子ビットのマイルストーンに到達する前から暗号攻撃の可能性が現実味を帯びてくる。サミュエ

---

[4] Brat Preneel プレゼンテーション 2024、https://handouts.secappdev.org/handouts/2024/bartpreneel_the-quantum-threatand-耐量子-暗号化-PQC.pdf。

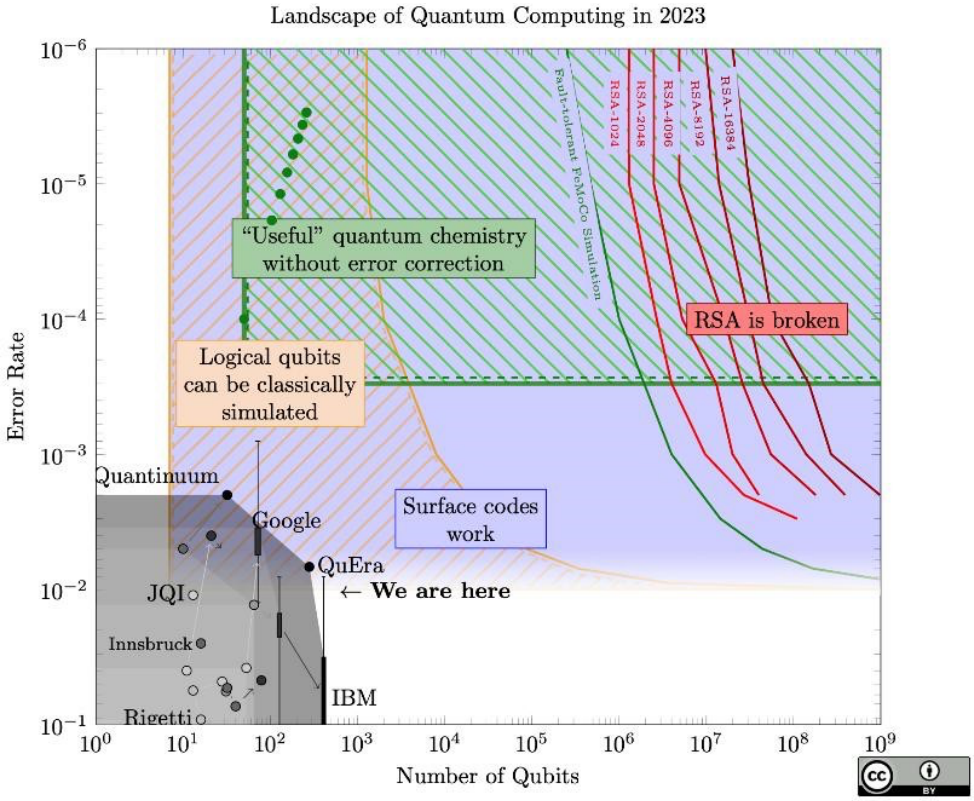
[5] ENISA 2024 年アセスメント、「耐量子暗号技術に投資した組織はわずか 4%」、https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA%20-%20NIS%20Investments%20-%202024_0.pdf。

[6] ISACA による 2,685 社の会員企業調査（地理的データは含まれておらず、一部企業は EU 域外である可能性がある）、https://www.isaca.org/about-us/newsroom/press-releases/2025/quantum-computings-rapid-rise-is-a-risk-tocybersecurity-and-business-stability。

[7] 「明日を守るために、今日行動する：耐量子暗号への移行」18 の EU 加盟国パートナーによる共同声明（2024 年）、https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-jointstatement.pdf?__blob=publicationFile&v=5。

ル・ジャックの CRQC タイムライン[8] は、量子コンピュータの現状（小型でノイズの多い装置）、目指すべき将来像（エラー訂正された大規模システム）、そしてリベスト・シャミア・アドルマン（RSA）アルゴリズムを破る暗号学的に重要な量子コンピュータ実現までの距離を示している（図 1）。彼のタイムラインは、量子コンピューティングの構成要素の改良に関する同様の見解を示しており、CRQC の実現に近づいていることを示している。

図 1. 非公式 CRQC タイムライン（サミュエル・ジャック）



出典：タスクフォース資料、サミュエル・ジャック

[9]今日、大手企業、スタートアップ、研究プログラムは、実用規模の量子コンピュータを開発するため、多様な科学的アプローチを追求している。量子研究開発（R&D）に注ぎ込まれる巨額の投資は、この技術的転換の地政学的・経済的利害関係を反映している。国家戦略もまた、量子コンピューティングからセンシング、コミュニケーションに至る量子技術全体に目を向けている。スペイン、イタリア、デンマークを含む複数の加盟国は最近、投資の優先順位と研究成果の活用メカニズムを概説した専用の国家量子戦略を発表した。EU レベルでは、2025 年 7 月に欧州量子技術戦略が発表された。同様に米国と中国では、それぞれ 37 億ドルと最大 140 億ドル

[8] このタイムラインは、ICANN および Douglas Stebila 教授、Bart Preneel 教授による報告書で使用・参照されている。非公式ながら毎年更新されるこのタイムラインは、ウォータールー大学の Samuel Jacques 教授によって作成されている。2023 年の予測は、誤り訂正量子ビットの増加により、2025 年の更新版よりも楽観的である（出典）

[9] 第 14 次国家経済社会開発計画およびビジョン 2035 には、量子コンピューティングへの強力な投資に加え、量子センシング（例：PNT 分野）およびコミュニケーション（主に都市間ネットワーク向け QKD）への投資も含まれている（出典）。

の投資が、この分野での主導権獲得に向けた深い決意を示している。これらの動きは総じて、量子技術が次世代デジタル変革の中核として台頭しつつあることを強調している。

本報告書では、PQC（ポスト量子暗号）、量子鍵配送（QKD）、量子乱数生成器（QRNG）のそれぞれの役割と能力を検証する。構成は以下の通りである。序論として、各アプローチは量子脅威 に対して異なる角度から対処し、防御の層を形成する可能性がある：PQC は量子攻撃に耐性のある数学的アルゴリズムにより、QKD は物理学に基づく鍵交換により、QRNG は暗号鍵におけるランダム性と予測不可能性を保証する。

この基盤に基づき、量子耐性ソリューションを段階的かつレジリエントに導入可能な、最も実現性の高い移行モデルを提案・アセスメントする。これにはハイブリッド暗号アーキテクチャや暗号アジリティ戦略が含まれ、量子耐性への移行に不可欠な概念である。さらに本報告書では、効果的なリスク緩和とガバナンスの前提条件として、組織が耐量子資産の構築をいかに開始できるかも示す。

これらのモデルは、進行中の国内外の取り組みを考慮して評価される。本報告書は、欧州連合内および国際的な主要国（米国、中国など）における量子技術への備えを、その戦略とビジョンに焦点を当てて分析する。これにより、金融、公共、防衛という 3 つの戦略的分野における特有の課題と機会を検証するセクター別章への基盤が整う。

これらの要素を統合することで、本報告書は技術的根拠と政策関連性を兼ね備えた、一貫性のある量子レジリエンスのロードマップを提供することを目指す。最終章では、この分析に基づく実践的な推奨事項を示し、官民の意思決定者が安全で拡張性があり、タイムリーな耐量子暗号への移行を調整することを支援する。

第 II 部 量子耐性環境における PQC、QKD、QRNG の現状

1. 耐量子暗号

耐量子暗号は、組織が量子耐性へ移行するための主要な手法である。これは（理論上）量子コンピュータおよび古典コンピュータによる将来の攻撃に耐えうる暗号アルゴリズムで構成される。量子耐性への移行において、PQC は規制団体から短期的・中期的には唯一の実行可能な選択肢と見なされている[10] 。

技術的な観点から、耐量子暗号とは量子攻撃に耐えるよう設計された新しい非対称（公開鍵）アルゴリズムを指す。これらは主に二つの形態に分類される：鍵カプセル化機構（KEM）とデジタル署名アルゴリズムである。前者は現在のシステムにおけるディフィー・ヘルマン鍵交換や RSA 暗号と同様に、共有秘密鍵を確立するために用いられるアルゴリズムだ。 PQC KEM はセッション鍵の防御に用いられる。CRYSTALS-Kyber はその一例であり、米国立標準技術研究所（NIST）により信頼性の高い PQC アルゴリズムとして選定されている。デジタル署名アルゴリズムは認証と完全性の確保に用いられ、現在の RSA や楕円曲線デジタル署名方式（ECDSA）の署名に相当する。

過去 10 年間で、国際社会は次世代暗号アルゴリズムの第一世代標準に合意した。例えば米国は、世界的な採用に向けた標準化において最も主導的役割を果たしている。 NIST は暗号化とデジタル署名用の 3 つのアルゴリズムを最終決定した。2024 年には NIST が 3 つの標準（Kyber、Dilithium、SPHINCS+）を確定し、Falcon やその他の候補は後続すると見込まれている。しかし中国や韓国などでの並行する取り組みにより、競合する標準が相互運用性を低下させる可能性があり、世界的な分断は依然として起こりうる。

PQC の正確な技術構造は、国家機関や独立機関による標準開発を通じて進行中のプロジェクトである。現在の議論は、数千に及ぶ製品、証明書、インフラストラクチャへの技術展開方法の決定にも及んでいる。この移行は、ハードウェアやアルゴリズムのアップグレードとしてだけでなく、今後数年にわたりデジタルエコシステムのレジリエンス、主権、安全性を形作る長期的なガバナンス課題として理解されねばならない。

2. 量子鍵配送（QKD）

量子鍵配送（QKD）は、主に光子、あるいは電子やイオンといった量子効果を利用した信号を交換することで、二者間で秘密鍵を共有する技術である。これは鍵合意技術であって、暗号化アルゴリズムではない。物理的なリンクを用いることで、QKD は双方が認識する共有のランダムな鍵材料を生成できる。さらに、量子信号を傍受しようとする盗聴者が介入した場合、QKD プロトコルが完了する前に双方に検知可能な干渉が生じることを保証する。 こうして共同で確立された鍵素材（両当事者だけが知り、第三者は知らない）は、メッセージ暗号化や認証などの他の暗号方式に使用できる。

数学的問題（格子ベース方式など）の計算上の難しさを前提とする PQC（ポスト量子暗号）に基づく鍵合意とは異なり、QKD の安全性は量子力学の法則に由来する。 したがって、CRQC でさえ QKD を破ることはできない。なぜなら、このプロトコルはアルゴリズムの複雑さに依存せず、量子システムの物理的挙動に依存している

[10] 米国国立標準技術研究所（NIST）、https://csrc.nist.gov/projects/耐量子-cryptography。

からだ（[11]）。さらに、QKD システムでは通常、各セッションごとに短命なランダム鍵を使用し、時間とともに継続的に更新する。長寿命の鍵（漏洩や盗難の可能性がある）が存在しないことで、このようなシステムの安全性は高まる。

2.1. QKD - 限界と実装モデル

光ファイバーケーブルなどの QKD リンクは有限の損失を示し、通常は距離とともに増加するため、光子は短距離で最も効率的に伝送される。理論上の利点にもかかわらず、QKD は現在、中～長距離通信リンクにおいて実用上の制限に直面している。現行ネットワークは、損失が鍵生成の遅延や停止を引き起こすため、信頼できるノードに依存することが多く、既存ネットワークへの複雑な統合も課題である。 宇宙空間の真空では損失が低減されるため、信号が大気圏を通過した後は衛星 QKD リンクを長距離化できる。

現在の中間技術成熟度レベル（TRL）にある QKD の進歩は、信頼できるノードなしでは長距離アプリケーション（数百 km 以上）ではまだ機能しない。複製不可能性定理は QKD のセキュリティの一部となり得るが、古典的なネットワークのように増幅器を使用できないことも意味する（商用量子 リピーターは現在も開発中である）。さらに、QKD チャネルは通常、特定のレート（秒あたりのビット数で測定、最大約 Mbit/s だが距離とともに低下）で鍵を生成する。このレートは大量のデータを同時に暗号化する際の制約要因となり得るが、計算複雑性に基づく鍵合意技術で容易に生成可能なレートよりは高い場合が多い。

最高距離と速度を達成するため、QKD は他のデータと多重化せず、ダークファイバー上で展開されることがある。これにより、類似の古典的ネットワークに必要なものを超える追加インフラが求められる場合がある。QKD 装置の設置・保守には多大なコストと複雑さが伴う可能性がある。ただし、多くの QKD 装置は主に通常のコミュニケーション部品で構成されており、適切に設計された QKD 装置は同等の信頼性を提供し、標準データセンター環境で動作できるはずだ。 個々の光子ベース伝送の校正は、一部の QKD 装置設計のセキュリティにとって重要である。こうした考慮事項から、QKD は追加のセキュリティが費用と労力を正当化するシナリオ（政府コミュニケーションや銀行間接続など）での使用が現状である。

技術的制約とは別に、QKD に対する戦略的アプローチは政策面でも民間セクターの投資面でも断片的だ。一部の技術の成熟度が限定的であることから、研究コストに対する価値を考慮すると、QKD 開発への官民双方の投資に疑問が生じる。

こうした課題を踏まえると、QKD を過度に重視することによる機会損失は大きい可能性がある。成熟したソフトウェアベースの PQC アルゴリズムへの資源配分の方が、より迅速かつ拡張性のあるセキュリティ成果をもたらすかもしれない。 この懸念は EU において顕著であり、欧州量子通信インフラ（EuroQCI）のような取り組みが開始されている。これは欧州のハブを量子通信システムで接続することを目指すものだ。また、QKD の能力と、より広範なアーキテクチャにおけるその役割を継続的に評価することも不可欠である。特に、QKD、PQC、古典暗号メカニズムを組み合わせた階層化されたハイブリッドシステムにおいてはそうだ。

要約すると、QKD は一般ネットワークにおける公開鍵暗号の直接的な代替手段ではない。特定の環境下で特定のシナリオのセキュリティを強化する専門サービスと捉えるのが適切だ。 銀行が 2 つの主要データセンター間で

[11] 量子鍵配送（QKD）への量子力学の法則の適用に関する詳細は、Scarani et al., 2009 を参照せよ。

複製トラフィックを保護するために QKD を使用することはあっても、オンラインバンキングへの全顧客接続を保証するために QKD を使用することはない。その場合は PQC の方が適している。しかし競争と革新によって技術が向上し、普及が進む可能性がある。主要な開発分野には、鍵生成速度の向上、通信距離の延長、装置の小型化が含まれる。

量子鍵配送（QKD）の標準化と認証は進行中であり、将来の実装において重要となる。これらは QKD が従来の暗号化を補完し、ハイブリッド通信ネットワークでどのように活用されるかを決定する。これらの標準により、アプリケーションは QKD 装置の内部仕様に関わらず、統一された方法で QKD 装置からの鍵を利用できるようになる。 量子鍵配送のネットワーク統合は 量子ネットワーク構築における別の課題である。欧州電気通信標準化機構（ETSI）や国際標準化機構（ISO）（特に ISO/IEC JTC 1 SC 27）といった標準化団体の取り組みは、調和と相互運用性の原則を通じて、この技術のより広範な採用を可能にする。

3. 量子乱数生成器と古典的乱数生成器

安全な暗号化の基盤には乱数生成が存在する。これは敵対的攻撃に耐えるために真に予測不可能な値でなければならない。 QRNG はこの課題に対する最先端のアプローチであり、光子の挙動や量子位相揺らぎといった量子現象の固有の不確定性を活用して高エントロピーの出力を生成する。決定論的アルゴリズムやノイズの多い物理プロセスに依存する古典的乱数生成器とは異なり、QRNG は量子物理学の法則によって保証されたランダム性を提供する。これにより QRNG は暗号システム向けの高品質なエントロピー源として有望視されている。 しかし QRNG は暗号入力の予測不能性を高める一方で、量子コンピューティングがもたらす広範な脆弱性には対処しない。量子攻撃に脆弱な暗号アルゴリズム内で使用されれば、完全な乱数鍵でさえ破られる可能性がある。したがって真の量子レジリエンスを実現するには、QRNG を耐量子暗号プロトコルと統合する必要がある。

暗号化メカニズムにおいて、選択された入力の十分なランダム性は極めて重要である（表 1 参照）。生成された数値が真にランダムであり、予測不可能であることを保証することが不可欠だ。暗号学において、エントロピーは乱数生成の主要概念である。エントロピーとはシステム内の予測不可能性の度合いを指し、値を推測または再現する難しさを測る。エントロピーが高いほど、攻撃者が予測するのは困難になる。

表 1. ランダム性のレベル

ランダム性のレベル	説明（簡略化）
1. ランダム性の錯覚	パターンはランダムに見えるが、実際にはそうではない。十分な分析により逆算可能である（例：円周率 π の部分列）
2. 機会的ランダム性	予測不能だが制御不能なプロセスに依存する（例：ユーザー入力のタイミング、マウスの動き）
3. 設計されたカオス	複雑な物理システム（例：熱雑音、電波干渉）を用いて、保証が不明確なランダム性を生成する

ランダム性のレベル	説明（簡略化）
4. 定量化された不確実性	量子力学やその他の物理的効果に基づく。物理法則によってランダム性が保証され、定量化可能である

出典：デロイト調査

現在のほとんどのシステムは擬似乱数生成器（PRNG）と真の乱数生成器（TRNG）を使用している：

- 古典的 TRNG は発振器のジッタや大気ノイズといった複雑な古典的物理現象に依存する。アルゴリズム的ではないが、古典系における予測不可能性の仮定に基づいている。時間の経過とともに微妙なバイアスや相関が生じ、悪用される可能性がある。QRNG は単一光子検出、量子位相揺らぎ、量子もつれといった量子現象を利用して乱数を生成する TRNG である。 量子プロセスは根本的に予測不能であるため、QRNG は古典的な複雑性やノイズを仮定せずに乱数を提供できる。これは古典的な TRNG とは異なる点だ。NIST SP 800-90A/B/c などの関連標準が求める品質を満たせば、QRNG は最高レベルの乱数である「定量化された不確実性」を提供できる。

- PRNG はアルゴリズム的かつ決定論的である。通常、（真に）ランダムな「シード」と暗号学的 PRNG アルゴリズムを用いて、一見ランダムなビット列を生成する。 暗号学的 PRNG（NIST DRBG や Fortuna など）は生成数の予測不可能性を保証する。ただしその安全性は、シードの秘密性と品質（すなわちエントロピー）および PRNG アルゴリズムの暗号的強度に完全に依存する。実際には、少量の真の乱数を用いて高速な PRNG 乱数ストリームを生成するハイブリッド方式がよく用いられる。

QRNG を支持する強力な論拠は、物理法則が成立し、その効果が乱数に正しく反映されているならば、隠れた変数や予測モデルでは出力を正確に予測できない点にある。ここでは、物理法則によってシステムの予測可能性が守られているのだ。

モデルは出力を正確に予測できないという点だ。ここでは、システムの予測可能性が物理法則によって守られている。

エントロピー源の標準（NIST SP 800-90B や BSI AIS 31[6] など）は量子由来の乱数を検討し始めており、将来的に QRNG の認証と採用を促進する可能性がある。より専門的な標準が待たれる一方で、既存の QRNG は現行のエントロピー標準下でも認証可能であり、規制対象システムへの展開を可能にする。

PQC、QRNG、QKD の概要は、量子耐性セキュリティを達成する単一かつ画一的な道筋は存在せず、各手法の相対的な成熟度と適用可能性が大きく異なることを示している。各手法は移行の異なる側面を推進し、セキュリティ、相互運用性、性能、コスト、運用管理性の間で固有のトレードオフに直面する。 PQC はアルゴリズムの堅牢性と効率性を、既存インフラへの統合性とグローバルな相互運用性と両立させねばならない。QKD 展開では鍵生成速度・距離・物理インフラ要件と、コスト・拡張性を天秤にかける。QRNG システムは認証可能なエントロピー品質に焦点を当てつつ、量子由来の乱数を既存暗号スタックへ効率的に組み込み、公認認証スキーム下で妥当性確認可能であることを保証する。

これらの規準は相互依存し、時に矛盾する。例えば、性能や統合容易性を最適化すると、アルゴリズムの多様性が低下したり、特定のハードウェアやネットワーク環境に依存する可能性がある。こうした緊張関係は、量子耐

性実装の成功が単一の指標で測れるものではなく、階層的な設計、相互運用性、認証を通じてシステムがこれらのトレードオフをいかに効果的に管理するかで評価されることを示している。 適切な高水準のセキュリティは譲れない基盤である。使いやすさ、コスト、性能の改善は、暗号の健全性や鍵材料への信頼を犠牲にしてはならない。したがって、レジリエンスを実現するには、ハイブリッド展開やフォールバック機構といった階層的な安全策が必要となる。

第 III 部 量子耐性移行モデル

耐量子暗号の実現に向け、数十億台のデバイスの暗号方式移行には、技術的・組織的・政策的な観点からの設計を要する特定の移行モデルが必要だ。 これほど大規模かつ複雑な取り組みにおいては、移行に伴う個々のサブプロジェクトやサブタスクを整理するにはリスクベースアプローチが最適だと考える。このアプローチはトップダウンで推進すべきだ。つまり、最優先の業務アプリケーションやプロセスを移行しつつ、必要な技術的移行について深く掘り下げる。これは、測定されたリスクとニーズに基づいて暗号アジリティの原則を実装することを目指すべきだ。

1. リスクベースアプローチ

耐量子暗号への移行は、単なる技術的なアップグレードではなく、包括的なシステムレベルの変革として理解されつつある。 PQC への移行は暗号ライブラリの更新をはるかに超え、通常は新製品バージョンの統合、アプリケーションプログラミングインターフェース（API）の変更、ソフトウェア開発ライフサイクルの適応、場合によっては中核業務プロセスの再設計を必要とする。また、サプライヤー、顧客、その他のエコシステム関係者の意識的な管理と移行も含まれる。このプロセスには長期計画、専門人材の採用、数年にわたる持続的な組織変革が求められる。

欧州では、規制環境が耐量子暗号の必要性を認識しているものの、明確な移行枠組みは存在しない。 サイバーレジリエンス法やネットワーク・情報セキュリティ指令 2（NIS2 指令）などの規制は、特に重要インフラにおいて、2027 年 12 月までに最先端の暗号化対策の使用を義務付けている。しかし、いずれもエンタープライズ向けの具体的なガイダンスや段階的な実施計画を提供しておらず、組織は PQC 移行の複雑さと規模を管理するための明確なロードマップを持たない状態にある。

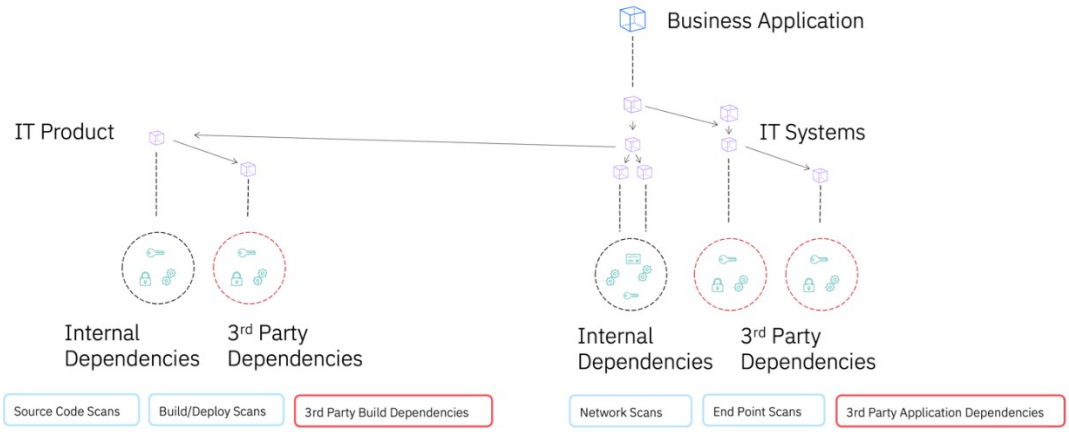
移行戦略は、特定の業界やシステムに合わせて調整する必要がある。過度に一般的なガイダンスは、特に規制上の義務が技術的・市場的な準備の実際のペースと同期していない場合に、混乱、不整合、不必要な負担を引き起こすリスクがある。

これを回避するには、留意すべき具体的な技術的・組織的要素がある。重要な経験則として、従来の暗号技術インベントリよりも依存関係マッピングが優先される点が挙げられる。 暗号在庫リストはリスク 監視には必要だが、移行計画の目的では完全でも実行可能でもない場合が多い。誤検知（暗号コードが存在しても未使用）や見逃し（クローズドなサードパーティ依存関係に埋め込まれた暗号）が生じやすい。つまり、網羅的な暗号在庫リストは完成しない可能性がある。より実行可能なアプローチは、特にハイブリッド環境、クラウドベース環境、高度に相互接続された環境において、システムとソフトウェアの依存関係をマッピングすることだ。

さらに、ほとんどの組織はサードパーティ製品・サービスに大きく依存しており、サプライチェーン上の依存関係が移行の制約と可能性を頻繁に決定づける。重要な製品や依存関係が組織の直接管理外にある場合、PQC への移行はしばしば停滞する。ソフトウェアベンダーやサプライヤーは段階的なアップグレードスケジュールを採用しており、多くの暗号化コンポーネントは複雑にネストされた依存関係の中に埋もれている。 この課題に対処するには、組織はサプライヤーとの強固な連携、量子耐性機能のタイムラインに関する明確な要求、サプライチェーンの準備状況を追跡する仕組みが必要だ。この文脈で実行可能な計画は、内部・外部の依存関係、ソフトウェア、ハードウェア、API、サービスのインベントリ作成（図 2）から始まる。これにより組織はサプライヤーと連携し、アッ

プグレードのタイムラインを要求し、それに応じて計画を立てられる。このマッピングは技術的前提条件であるだけでなく、EU 規制に統合されたサプライチェーンリスクマネジメントツール（例：ソフトウェア部品表（SBOM）要件）との連携を可能にする（[12]）。サプライチェーンパートナーが暗号化詳細を標準化された形式で報告すれば、より信頼性の高い自動化、コンプライアンス、政策立案が可能となる（ポスト量子暗号インベントリの詳細なマッピングは第 IV 部で展開する）。

図 2. 暗号依存性マッピング



出典：タスクフォース資料、IBM。

さらに、量子耐性への移行は現実的に一足飛びには達成できない。暗号プリミティブの段階的な可用性と、レガシーシステム、規制サイクル、サプライチェーン依存といった現実世界の制約の両方が原因だ。ポスト量子暗号ツールのリリースと成熟は段階的に進む。KEM（鍵管理）は一般的に最初に標準化され製品に組み込まれ、次にデジタル署名が続く。最終的には、デジタル ID 枠組みや多要素認証を支えるような高度なプロトコルへの完全統合に至る。

「現在収集、後で復号」リスクを緩和するには、リスクベースの量子移行戦略において耐量子 KEM を優先すべきだ。HNDL は将来の量子攻撃に対する古典的公開鍵暗号の脆弱性を悪用し、長期的な機密性を有する暗号化データを標的とする。PQC KEM は転送中のデータを保護する量子耐性代替手段を提供し、将来の復号化から今日のコミュニケーションを守るために不可欠である。一方、認証は短期リスクが低い。認証情報は通常有効期間が短く、更新が容易だからだ。暗号化と認証の両方が最終的には量子安全アルゴリズムへ移行する必要があるが、高価値データを将来の侵害から守るためには KEM への即時対応が求められる。

複雑なインフラを管理する組織にとって、この段階的な導入は即時の戦略的ジレンマを生む。新機能が利用可能になるたびに部分的な移行を行うと、高コストなアップグレード、運用中断、調整オーバーヘッドが繰り返される可能性がある。しかし、スタック全体が準備・認証された「ワンショット」移行が可能になるまで遅らせると、重要システムが数年間無防備な状態に置かれ、大規模なエコシステム全体での同時アップグレードが失敗・非互換性・依存関係の見落としリスクを高めるため、システム的な危険をもたらす可能性がある。こうした状況下で組

[12] これについては、サイバーレジリエンス法第 I 条第 2 項（脆弱性対応要件）を参照のこと。

織は、情報に基づいたトレードオフを行い、移行期間を埋めるハイブリッド方式を採用せねばならない。具体的には、早期移行可能な業務上重要なアプリケーションと待機が必要なアプリケーションを明確に区分し、段階的導入に対応できるよう調達・アップグレード計画に柔軟性を組み込む必要がある。

移行プロジェクトの実証データは、移行を純粋な技術的「暗号更新」と扱うような不十分な調整が、遅延や資源の浪費、時には重要な依存関係が整わないことによるプロジェクト停滞（例：TLS 移行）を招くことを示している。成功する戦略は、システム視点に立ち、量子耐性移行を通常のデジタル変革や IT ライフサイクル活動と同期させるものだ。 実際、移行が遅れる原因は技術的解決策の不足ではなく、予算サイクル、業務慣性の問題、事業優先順位にあることが多い。 の量子耐性移行を、予定されたアップグレード、事業変革イニシアチブ、定期的な更新サイクルと連動させることで、最高の効率性と合意形成が得られる。大半のアプリケーション所有者にとって、量子耐性移行単体では説得力が乏しく、強化されたサイバーセキュリティ、規制順守、ライフサイクル管理の改善といった広範な価値と統合されなければ受け入れられない。

最後に、移行の成功は管理構造とスキル開発にも依存する。暗号化移行はもはやニッチな技術専門家の領域ではなく、部門横断チーム、透明性のあるガバナンス、明確なプロセス所有権が必要だ。 多くの組織が苦戦しているのは、移行を監督する責任を持つ単一のチームが存在せず、必要なスキルが不足しているためだ。教育、内部の専門センター、チーム間の連携への投資は、摩擦を減らすために不可欠である。即効性のあるインセンティブや経営陣レベルの関心の欠如が、この課題に取り組むためらいを永続させている。組織は確立され、資金提供され、権限を与えられたプログラムを持つべきだ。現在の進捗の多くはボトムアップであり、経営陣の支援が不足している。

暗号レジリエンスを高める上での主な課題は資金不足ではなく、リソースの不整合だ。暗号セキュリティを優先する個人やチームは必要な予算を掌握できていないことが多い一方で、この問題を優先しない他の事業領域には多額の資金が存在する。この乖離は、暗号レジリエンスを監督する中央集権的な権限やプログラムオーナーの不在によって悪化しており、断片的な取り組みと新興脅威に対するシステム保護の進捗不足を招いている。

2. 耐量子暗号（PQC）の最悪の失敗シナリオ：もし PQC が脆弱だと判明したら？

本節では、量子耐性への移行過程で想定される二つの混乱経路を概説し、セキュリティ維持における暗号の俊敏性とハイブリッド暗号化の運用上の必要性を示す。長期的なレジリエンスを確保するには、モジュール化された暗号アーキテクチャやフォールバック機構といった先見的な設計選択が不可欠であることを強調する。

漸進的破綻：新たな数学的知見や暗号解読により、古典コンピュータで PQC アルゴリズムの一つが徐々に破られる可能性がある。このシナリオでは、ハイブリッド方式による多層的なセキュリティにより、先見的なハイブリッドアプローチが暗号化メカニズムの有効性を維持する。例えば Kyber（PQC アルゴリズム）が 5 年後に脆弱であると判明した場合を考えてみよう。 その場合、Kyber で暗号化を実行している組織は、当面の間は安全が保たれる。なぜなら、二つのハイブリッド暗号化スキームのうち一つだけが 破られたに過ぎないからだ。さらに、この文脈では暗号の俊敏性（crypto agility）の原則が極めて重要である。主要アルゴリズムが破られた場合、エンタープライズは大きな困難なく代替手段（例えば NIST 最終候補の別の KEM など）に移行できるべきだ。ベストプラクティスとして、モジュール化された暗号アルゴリズム（プラグアンドプレイ）を備えたシステムが推奨される。

突然の解読：このシナリオでは、量子脆弱性アルゴリズムで保護された通信を、悪意ある主体が検知されずに復号できる量子暗号解読装置（CRQC）が既に開発されている。この場合、情報が公開されたら（仮に公開されるとしても）、代替計画が必要となる。 一つの選択肢は、緊急時に完全な対称暗号化へ回帰する能力を維持することだ。信頼できる宅配便による鍵配送といった手法を採用することが、レジリエンス向上の賢明な手段となるだろう。 したがって、フォールバック（順次）ハイブリッドシステムは、一方の方法が失敗した場合に迅速に代替手段へ切り替えることを可能にする。デュアルレイヤーハイブリッドとは異なり、この方法は二つの暗号化手法の組み合わせを意味せず、機敏性とバックアップを備えることを指す。Advanced Encryption Standard (AES)-256 は鍵サイズが大きいため量子攻撃に対して安全性を保つが、安全な鍵管理（KEM）なしでは独立して機能しない。 したがって、鍵配布や認証を可能にする脆弱性を持つ非対称方式（RSA や楕円曲線暗号（ECC）など）を置き換えるため、耐量子暗号が必要となる。突然の破綻シナリオにおいて、これらの PQC アルゴリズムが侵害された場合、事前共有鍵や物理的に配布された AES ベースの対称鍵へのフォールバックにより、安全なコミュニケーションの継続性が確保される。 例えば仮想プライベートネットワーク（VPN）装置は、主に PQC ベースの鍵交換を用いながらも、脆弱性が公表された場合に事前共有鍵や代替アルゴリズムへフォールバックするモードを備えるべきだ。バックアップ鍵の配布や二次的な安全な通信路の確立といった準備が整っている必要がある。

両シナリオは暗号の俊敏性とハイブリッド方式に依存しており、これは将来の暗号設計に不可欠である。政府と産業界は暗号俊敏性を備えた標準規格と調達慣行を推進すべきだ。システムは想定されるシナリオを考慮し、単一アルゴリズムをハードコードすべきではない。代わりにアルゴリズム更新に対応可能な設計を採用すべきである。この俊敏性は量子暗号の文脈だけでなく、予期せぬ脆弱性（量子・古典を問わず）への対応にも寄与する。

Box 1. 暗号の俊敏性とハイブリッド暗号化

NIS 協力グループの「耐量子暗号への移行に関するロードマップ」で定義されているように、暗号の敏捷性とは「暗号コンポーネントの交換を可能にする、モジュール化された暗号プロトコルおよびシステムの設計」である。

敏捷性を実現するには、アプリケーションの暗号操作を抽象化（コード変更ではなく設定変更でアルゴリズムを変更できるようにするため）し、ライブラリやハードウェアで複数のアルゴリズムをサポートする実装が必要となる。これは、暗号技術上の課題であると同時に、ソフトウェア工学上の課題でもある。

NIST (2025) の最近の研究では、これらの原則をさらに詳しく説明し、暗号の敏捷性をプロトコル、ソフトウェア、ハードウェア、インフラストラクチャにまたがる機能として位置付け、スケーラブルな実装をサポートするためのセクター固有の戦略と共通 API の必要性を強調している。これは、敏捷性は個々のアルゴリズムの機能ではなく、組織やインフラストラクチャの特性として扱うべきであるという新たなコンセンサスを反映している。

これに対しハイブリッド暗号化は、同一の暗号ワークフロー内で古典的（量子脆弱性を持つ）アルゴリズムと PQC アルゴリズムを同時に使用する手法である。これは、PQC アルゴリズムの早期失敗リスクの緩和を実現しつつ運用継続性を維持するため、各国サイバーセキュリティ当局（ドイツ、フランス、オランダ）が広く支持する移行戦略だ。ハイブリッド方式の核心的利点は冗長性にある。一方のアルゴリズムが侵害されても、他方がセキュリティ保証を維持できる。 しかしこの手法は計算複雑性を増大させ、攻撃対象領域を拡大し、特にリソース制約環境において実装とコンプライアンスの負担を増加させる。暗号化手法の組み合わせは、対称暗号と非対称暗号、耐量子暗号、量子鍵配送と古典暗号手法の間でも可能である（後述の「3.混合暗号方式」参照）。ただし、元の用語が示唆する通り、必ずしもハイブリッド暗号化とは見なされない。

両概念は密接に関連するが、運用上は異なる。アジリティとは、長期的な適応性を確保するため、時間経過とともにアルゴリズムを切り替える能力を維持することである。ハイブリッド暗号化は、即時的または予期せぬ脆弱性から保護するため、二つ以上のアルゴリズムを並行して実行することを意味する。この意味で、ハイブリッド展開はアジリティ達成のための過渡的手段と見なせるが、真のアジリティには暗号エコシステム自体の設計にモジュール性を組み込むことが必要である。

関連する懸念事項として、複合証明の安全性が挙げられる。すなわち、少なくとも一方のスキームが安全であれば、二つのスキームの組み合わせが安全であることを証明することである。研究者らは[13]、ハイブリッド鍵交換の安全性を形式的にモデル化している（初期段階の証明として、各 コンポーネントが選択平文攻撃下での識別不能性（IND-CPA）[14] を満たす場合、その組み合わせは INDCPA となる、といったものが存在する。ただし、出力を適切に混合する方法に関する注意点がある）。この研究は、量子耐性ハイブリッド鍵確立に関する ETSI TS 103 744 標準（後述）と同様に、徹底的なレビューを経て標準化される可能性がある。

3. 混合暗号化方式

量子暗号に対するハイブリッドアプローチには 2 種類ある。

1) 古典的と耐量子ハイブリッドである。ボックス 1 で述べたように、古典的と耐量子ハイブリッド方式は、安全な暗号化のための中短期的な選択肢として多くの政府機関や標準団体から推奨されている。これは、従来のアルゴリズムと耐量子アルゴリズムの両方で並行して暗号処理を行い、その結果を何らかの方法で組み合わせることを意味する。 鍵確立において「ハイブリッド」とは、楕円曲線ディフィー・ヘルマン（ECDH）とカイバーカプセル化といった二つの鍵交換を行い、両出力から実際のセッション鍵を導出することを意味することが多い。単純な方法は共有秘密を連結することである：秘密 = 鍵導出機能（KDF）(古典鍵 || ポスト量子鍵)（他の文脈情報を含む場合あり）。ETSI TS 103 744 標準はこの手法を採用している。具体的には、ディフィー・ヘルマン共有点と PQC KEM 共有秘密（例：Kyber 由来）、およびオプションの事前共有秘密を連結する。この連結された入力を鍵導出関数に入力し、最終的な鍵を生成する。結果として、攻撃者が鍵を復元するには古典的問題と耐量子問題の両方を解く必要がある。たとえ後々一方の構成要素が脆弱だと判明しても、もう一方がセキュリティを維持することが期待される。古典的＋PQC ハイブリッドはアップグレードも円滑にする。例えば二つのシステムがハイブリッドハンドシェイクをネゴシエートできる。量子対応クライアントは両方を使用するため互換性が保たれる。この手法はインターネット技術タスクフォース（IETF）において「耐量子従来型ハイブリッド方式（PQ/T ハイブリッド）」と呼ばれることがある。 IETF は複数のワーキンググループで「鍵交換と署名双方のハイブリッド型耐量子/従来型（PQ/T）方式を推進中」だ。例えば TLS 1.3 では、2 つの鍵共有拡張（ECDH 用と Kyber 交換用）を送信し結合する方法を規定するアクティブな標準が存在する。同様に、インターネット鍵交換プロトコルバージョン 2（IKEv2）における多重鍵交換は、既にデュアルな Diffie-Hellman＋Kyber 交換を実行し両者から鍵を導出するメカニズムを定義している。 ハイブリッドデジタル署名も検討されている（つまり、 メッセージを ECDSA と Dilithium の両方で署名し、両方の署名が有効であることが要求される）。複合証明書（2 つの公開鍵と 2 つの署名を含む）はその実装方法の一つだ。 ハイブリッド方式の主な欠点は、計算負荷の増加とメッセージサイズの拡大（基本的に単一方式の 2 倍）である。多くの場合、こ

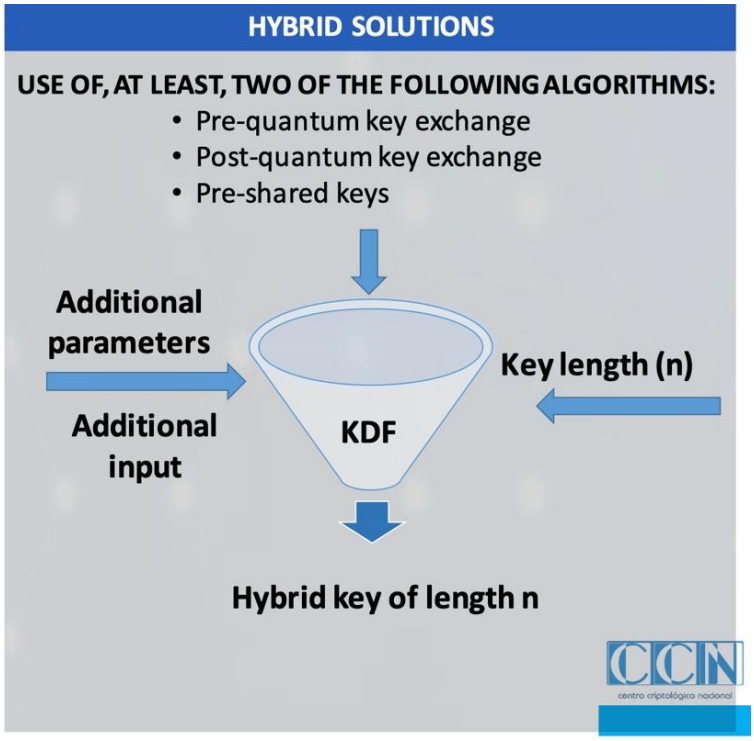
[13] Petcher and Campagna, 'Security of Hybrid Key Establishment using Concatenation', (出典)。

[14] IND-CPA（選択平文攻撃下での識別不能性）とは、攻撃者が 2 つのメッセージを選択し、そのうちの 1 つの暗号化を見ることができたとしても、どちらが暗号化されたものか判別できないことを意味する。

れは許容範囲内だ。例えば、TLS ハンドシェイクで 1～2 キロバイト増加しても負担にはならず、ECDH と Kyber KEM を併用する処理も現代の中央処理装置で容易に実行可能だ。したがって、古典暗号＋PQC のハイブリッド方式は、PQC 導入を加速する低リスクの中間段階と見なされている。

2) QKD と PQC、あるいは多層ハイブリッド。別のハイブリッド方式では、異なる層で根本的に異なるメカニズムを用いる。特に QKD と暗号技術（従来型または耐量子）を組み合わせる手法がある。提案の一つは、下位層のリンク（例えばネットワークルーター間やデータセンター間）を QKD で保護しつつ、エンドポイント間ではエンドツーエンドの耐量子暗号を併用する方式だ。これは層状ハイブリッドと見なせる（図 3）。リンクは量子鍵で防御されるため（攻撃者が検知されずに光ファイバーを傍受できない）、同時に、たとえ 1 つのリンクが侵害されても、データは送信者から受信者までエンドツーエンドの PQC アルゴリズムで暗号化される。このような構成は、単一障害点のリスクを大幅に低減できる。

図 3. ハイブリッド暗号化メカニズムの展開に関するスペイン国家暗号センターによる図解[15]



出典：タスクフォース資料、スペイン国家暗号センター

ボックス 2. ハイブリッド暗号化手法：タスクフォースの見解

ハイブリッドという用語は、耐量子移行の文脈で、古典的暗号と量子耐性のある暗号プリミティブを同時に使用することを指す場合によく使われる。ほとんどの場合、ECC や PQC（すなわち Kyber）などの公開鍵アルゴリズムの組み合わせを指す。欧州連合の公式政策の枠組み、特に NIS 協力グループの専門作業部会によって策定された

[15] この図では、鍵導出機能（KDF）が量子前鍵と量子後鍵を含む複数の入力を組み合わせてハイブリッド鍵を生成する。実際には、ほとんどのシステムが 3 つの暗号化方式を使用することはない。要するに、複数の独立した鍵が 1 つの暗号化組み合わせに投入されるのだ。

PQC ロードマップでは、ハイブリッド暗号の概念は狭義かつ特定の意味で使用されており、PQC アルゴリズムと従来の公開鍵暗号（すなわち RSA または ECC）の組み合わせを指している。 NIS ロードマップは、QKD や事前共有鍵（PSK）など、他の形態のハイブリッド化については言及も包含もしていない。しかし、欧州委員会の「耐量子暗号ロードマップに関する勧告」（2024 年 4 月 11 日、前文 6）および「欧州のデジタルインフラのニーズをどのように掌握するかに関する 2024 年白書」は、いずれも、階層化された量子安全アプローチの一部として、PQC/QKD のハイブリッド化について言及している。

一方、スペイン国立暗号センターは、ハイブリッド鍵を「従来の量子以前のアルゴリズム、耐量子アルゴリズム、事前共有鍵のうち少なくとも 2 つを使用するもの」と定義している。 PSK（長期的な秘密鍵をアウトオブバンドで事前共有）の組み込みは追加の安全策となる。たとえ両方の公開鍵方式が破られた場合でも、攻撃者は事前共有された秘密鍵を依然として必要とする。軍事コミュニケーションなどの特殊な状況では、三重ハイブリッド方式が採用される可能性がある。

この文脈において留意すべきは、従来の PQC ハイブリッドモデルが古典的攻撃に対する既存の暗号保証を維持しつつ、段階的に量子耐性を導入することに焦点を当てている点だ。しかしハイブリッド化は、信頼アンカーの多様化やシステム的レジリエンスの強化といった、より広範な目的にも寄与し得る。 例えば、ハイブリッド鍵交換は、後方互換性を維持するだけでなく、多層防御アーキテクチャを構築するために、PQC と古典的な公開鍵アルゴリズム、PSK、あるいは QKD ベースのメカニズムを組み合わせることがある。このようなアーキテクチャでは、QKD が下位レベルの通信リンク（ルーター間やデータセンター間など）を保護し、PQC がアプリケーション層でエンドツーエンド暗号化を提供する可能性がある。

これらの構成は相互運用性と調整上の課題を提起するため、ETSI、IETF、ISO などの標準化団体はハイブリッド利用のためのプロトコル形式とネゴシエーション方式を積極的に定義している。例えば ETSI TS 103 744 は、PSK や追加アルゴリズムに対応する柔軟な拡張フィールドを含む、ハイブリッド鍵確立のための具体的なメッセージ形式と暗号構成を定義している。 ETSI はまた、認証付き量子耐性ハイブリッド鍵確立（AQHKE）仕様の開発を進めている。

こうした背景を踏まえ、複数の暗号入力要素を組み合わせるあらゆる戦略を包括する、文脈認識型かつ技術的に包括的なアプローチを指す広義の用語として、「ハイブリッドソリューション」の使用を推奨する。

4. 量子耐性 への移行における課題

世界の技術市場では、量子安全暗号の実装がすでに始まっており、そのスピードは政策の策定よりも速い場合が多い。一部の組織は、将来の標準を見越して、暗号対応が柔軟なソリューションを展開している。これは、確固たる規制の推進がなくても、市場の力やベンダーの取り組みが早期導入を推進していることを意味する。NIS 協力グループが策定したタイムラインでは、2026 年から 2030 年の間に大きな動きが見込まれるが、業界の現実によって追い越されるリスクがある。

管轄区域によって移行のスピードが異なることは、業界にとって大きな課題となっている。グローバルエンタープライズやテクノロジーベンダーは、一部の市場では PQC の迅速な採用が求められている一方で、他の市場では待機態勢が続いているという、2 つのスピードが混在する環境に対応しなければならない。この不整合は、難しい選択

を迫る。断片的なアプローチは、開発の重複、コストの増加、潜在的なセキュリティの脆弱性につながる可能性がある。

以下では、調整の取れていない PQC 移行から生じる主なリスクと制約について概説する。

- **二極化した移行リスク**：暗号製品を開発するベンダーは、各国が量子耐性標準を異なるペースで採用する際に互換性のない要件に直面する。市場ごとに異なる暗号基盤をサポートすることは技術的に非効率であり、実装エラーのリスクを高め、テスト・更新・認証における大幅なオーバーヘッドを生む。別々の製品バージョン（例：A 地域向け PQC 対応版と B 地域向け非対応版）を維持することは持続可能ではない。結果として、多くのグローバル企業は世界的な最低要件が確立されるまで PQC を普遍的に採用しない可能性が高い。この状況は組織に調和が達成されるまで実装を遅らせるよう促し、実質的に動きの遅い管轄区域を迂回させる。それらの市場に展開される製品はポスト量子機能を含み得るが、現地の規制期待との整合性はない。EU にとって、比較的慎重な移行スケジュールは戦略的自律性を損なうリスクがある。なぜなら、重要なインフラが迅速な外国標準によって形作られた暗号システムに依存する可能性があるからだ。

- **標準化とコンプライアンスのギャップ**：インターネットの核心的なセキュリティ標準（TLS、IPsec など）は PQC オプションで更新されているが、規制のタイムラインは異なる。コンプライアンス対応に迫られる組織は難題に直面する。一部の規制当局は自主的ガイドラインのみを発行する一方、他は特定期日までに旧式アルゴリズムの使用禁止を計画している。この不一致はコンプライアンスに懸念すべき曖昧さを生み、明確性と説明責任を損なう。ある国で「量子耐性」と認められる製品が、別の国では未承認である可能性（あるいはその逆）がある。調達プロセスは複雑化する。例えば EU の顧客は現時点で PQC 機能を明示的に要求しない一方、米国政府機関はこれを欠く製品を拒否する可能性がある。ベンダーは最も厳しい共通基準を満たす（早期に追加コストと複雑性を生むリスクを伴う）か、暗号技術の柔軟性不足により後々異なる市場向けにソリューションを改修するリスクを負うかの選択を迫られる。さらに企業は、どの量子耐性アルゴリズムをいつ採用すべきか、明確な世界的合意がない中で誤った技術標準に賭けることを懸念している。先行企業が導入したスキームが後になって特定の国家当局に拒否され、技術の再設計と追加コストが発生する可能性がある。例えば、NIST 準拠でないロードマップを採用した組織は、後に EU 規制団体に拒否される恐れがある。一方で、欧州の一部当局はより多様なアプローチを採用し、NIST 選定セット外のアルゴリズム（FrodoKEM や Classic McEliece など）を推奨している。FrodoKEM は既に ENISA の暗号推奨リストに含まれており、世界的な合意形成が進む中、欧州規制当局が量子セキュリティに向けた代替経路を模索していることを示している。

- **運用上のボトルネック**：政策が整合されていても、PQC の実践的導入には資源と供給の課題が存在する。耐量子暗号に精通した熟練人材の不足は、新規アルゴリズムの大規模展開と監査を困難にする。この人材不足が政策対応の遅延要因となり得る。加えて、PQC ソリューションのサプライチェーンセキュリティも懸念事項だ。多くの企業は PQC を実現するため、サードパーティ製ライブラリ（オープンソースまたは商用）やハードウェア（例：ハードウェアセキュリティモジュール（HSM）、セキュアチップ）に依存している。これらのコンポーネントの信頼性を確保し、脆弱性を導入せずに統合することが不可欠だ。早期導入には厳格なテストが不可欠だ。広く使われる PQC ライブラリの欠陥は世界的な影響を及ぼす可能性がある。急いで進めれば、サプライチェーンの審査や認証済み・規格準拠コンポーネントの開発がボトルネックとなる恐れがある。移行は政策のタイムライン問題であると同時に運用上の課題だ。十分な専門家、堅牢なツール、量子耐性技術の安全な流通が必要となる。これらの要因は、国ごとの断片的な移行が問題である理由をさらに浮き彫りにしている。

第 VI 部 耐量子技術インベントリ

1. アプローチ

耐量子暗号への移行に備え、組織は暗号技術と製品のインベントリ構築・維持方法に注力しつつある。そこから生まれるのは硬直した青写真ではなく、早期計画、技術チームとガバナンスチーム間の連携、そしてインベントリが何を捕捉すべきか・その理由を明確に理解した上で形成される一連の指針となる実践手法である。 目標は、異なる関係者が暗号資産を孤立したチェックリストではなく、より広範な移行戦略を支える進化するツールとして扱える共通言語と運用マップを開発することだ。この枠組みには、早期計画、部門横断的な調整、そして暗号資産への体系的・構造的なアプローチ方法を理解するという主要目標が組み込まれる。暗号資産と製品資産の評価は別物である。

暗号インベントリは、組織のシステム全体で暗号技術がどこでどのように使用されているかを詳細にマッピングするものである。その目的は、使用中の暗号アルゴリズム、実装コンテキスト（コード署名、コミュニケーション用 TLS など）、量子耐性ステータス（レガシーか PQC か）、暗号モジュールや標準（Open Secure Sockets Layer（OpenSSL）や HSM など）の依存関係を識別することにある。 暗号在庫をマッピングすることで、システム内部の暗号ロジックと基本要素を理解できる。

製品インベントリは、組織が使用する外部製品、サービス、ハードウェア（つまりサードパーティプロバイダ）に焦点を当て、これらの製品の暗号特性をマッピングする。 これにより、ベンダーの暗号化ロードマップを特定できる。具体的には、PQC をサポートしているか、移行スケジュールと移行先技術、ファイアウォールやクラウドプラットフォームなどの調達技術に組み込まれた具体的な暗号技術、システム間の相互運用性の可能性、暗号化および認証に関する標準への準拠状況などである。全体として、前者は組織環境内での暗号化の運用方法に焦点を当て、後者は設計上組み込まれた組織が依存する製品に関わる。

暗号資産管理の重要なテーマは、リスクベースのアプローチを採用し、PQC を最優先で必要とする重要システムを特定することだ。全てのシステムやデータが同等のリスクを抱えているわけではない。したがって効率的な資産マッピングは階層的であるべきで、最も脆弱な資産にまず焦点を当てる。既存の資産リストに、各アイテムの重要性や機密性に関する文脈情報を付加することを検討することが推奨される。 機密アーカイブ、特許、企業固有システム（アプリケーションや内部ソフトウェアなど）といった、機微かつ長期保存が必要なデータを防御する暗号化用途は、優先順位リストの最上位に位置づけられる。

IT 環境をスキャンして暗号技術の使用箇所を特定し、保護対象データの分類メタデータを付加することで、優先順位付けされたインベントリが作成される。このリスク中心の階層構造は、組織がインベントリ項目をリスクレベル（高・中・低）で分類し、修復リソースを効果的に配分する指針となる。

暗号資産をカタログ化する際には、マッピングされたシステムの相互に絡み合ったインフラ構造を認識することが不可欠である。これは特に電気通信などの分野で重要だ。大規模ネットワークや重要インフラでは、暗号技術は相互依存する構成要素に組み込まれている。 したがって、組織の製品インベントリは、こうした外部依存関係や制約（例：通信事業者のインベントリが、自社が制御できないルーターやプロバイダ間通信プロトコルを使用していること）を考慮しなければならない。この問題は、第 III 部（量子耐性への移行課題）で述べた「二段階移行」のリスクに帰着する。つまり、各国が量子耐性標準を異なるペースで採用する場合、暗号製品を開発するベ

ンダーは互換性のない要件に直面するのだ。この状況は、調和が達成されるまで実装を遅らせるよう組織を促す。今回は管轄区域間ではなく（認証や標準ではこの問題も含まれるが）、エコシステム全体での調和が求められる。たとえある組織が PQ アルゴリズムの展開準備が整っていても、機器ベンダーやパートナー、顧客が同様にサポートする調整を待つ必要があるかもしれない。したがって、あらゆる資産管理枠組みは、内部システムだけでなく、依存する外部インフラストラクチャ内の暗号要素も把握すべきだ。ベンダーのロードマップや標準のタイムラインに関する注記も必要である。これにより、量子耐性移行計画が、国境を越えたネットワーク環境の広範なサプライチェーン内で現実的かつ調整された状態を維持でき、一部のコンポーネントが量子耐性へアップグレードする一方で、他のコンポーネントが従来の暗号化ベースのまま残る状況を回避できる。

2. 製品インベントリ

組織は製品在庫の暗号アセスメントに実用的なツールとプロセスを活用できる。調達ガイドラインに暗号要件を追加し、問い合わせに対応する方法が選択肢となる。つまり、新規ソフトウェア・ハードウェア・クラウドサービス購入時、組織はベンダーに対し製品で使用される暗号アルゴリズムとプロトコルの開示を要求し、必要に応じて耐量子アップグレードのロードマップも求める。

これは構造化されたベンダー質問票を通じて促進できる。製品で使用されている暗号化アルゴリズムの種類、それらの量子耐性有無、組織の PQC 準拠プロセスを把握することを目的とする。調達およびベンダー管理プロセスに質問項目を組み込むことで、組織は在庫マッピングに必要な情報を得られる。これによりサプライヤーからの透明性が確保され、レガシー暗号技術を使用するサードパーティ製コンポーネントの識別が可能となる。量子移行時に外部依存関係を見落とさないことを意味する。 具体的には、使用中の主要なサードパーティ製品・サービスごとに、依存する暗号化メカニズムを在庫記録に明記する。例えば「製品 X は安全通信に RSA-2048 を使用」「クラウドサービス Y は ECC 付き TLS 1.2 を使用、2025 年までに耐量子 TLS へアップグレード予定」といった形式だ。 これにより、すべての暗号依存関係を 1 か所に集約できる。製品暗号インベントリを暗号インベントリと併せて管理することでリスク分析の盲点に注意を払い、量子脅威に先んじてサプライヤーと積極的に連携することを可能にする。

3. 暗号インベントリ

暗号インベントリは暗号使用の識別・分類・監視を必要とするが、これは時間とリソースを要する作業だ。社内資産に焦点を当てた暗号インベントリの要素には、コードに組み込まれたアルゴリズム、使用プロトコル、暗号ライブラリの構成、暗号化プロセスを支えるハードウェアなどが含まれる。

こうしたインベントリに記録されるデータは、細分化され詳細である必要があり、以下を含む：

- 使用されているアルゴリズムの種類（RSA-2048、ECC、AES-128、Secure Hash Algorithm (SHA)-2 など）

- 当該暗号技術の機能目的（認証、機密性、完全性など）

- プロトコルのコンテキスト（例：TLS 1.2、IPsec、Secure/Multipurpose Internet Mail Extensions（S/MIME））

- 使用される資産（例：ルーターのファームウェア更新署名、アプリケーションの内部 API、VPN コンセントレータ）

- 暗号機能の起源（自社開発、サードパーティライブラリ、OS カーネルモジュールなど）

- PQC 標準との互換性、あるいはハイブリッド方式の一部であるかどうか

- 防御対象データの保存期間（短期保存データか長期保存データか）

- 防御対象データの機密性（専有情報、機密情報）。

CodeQL などのツールは暗号プリミティブを識別し、安全でない使用法や古い使用法をフラグ付けできる。開発者やセキュリティ研究者がセキュリティチェックの自動化やバリアント分析に利用し、組織内の言語、ライブラリ、フレームワークを可視化できる。 これにより、ソースコードの直接分析が可能となり、機械可読なインベントリ出力を生成し、非推奨のハッシュ関数などの安全でないインスタンス化を識別できる。これは暗号部品表（Cryptographic Bills of Materials）の新興標準に合致する。これにより暗号環境内のコンポーネントの品質、起源、有効期限リスクを判断する暗号インベントリの自動アセスメントが可能となる。

IBM の暗号発見・インベントリツール（ zCDI ）は、エンタープライズグレードのインフラがシステムレベルのテレメトリに暗号可視性を直接組み込む方法の一例を示す。このツールは IBM Z 環境全体で暗号の使用状況を継続的にスキャン・集約し、ライブラリ、鍵長、暗号モード、使用コンテキストをマッピングする。 重要なのは、暗号要素をアプリケーションのメタデータや業務プロセスと関連付けることで、組織がアルゴリズムのリスクだけでなく、業務上の重要性やコンプライアンス要件に基づいて移行の優先順位付けを行える点だ。このシステムレベルの統合は、受動的な暗号インベントリから実用的なインテリジェンスへの移行を反映している。

自動化によりツールの効果は高まるが、暗号資産の棚卸しは単なる列挙作業ではない。包括的なスキャンは誤解を招きやすく、優先順位付けが欠如していることが多い。さらに、完全な暗号マッピングはサイバーセキュリティ予算の限られたリソースを分散させる恐れがある。ビジネス優先度の観点から変更が必要な資産を特定することが必要だ（第 1 部で述べたように、階層的なリスクベース評価が推奨される）。

ロングテールソフトウェアコンポーネント、オープンソースモジュール、組み込みファームウェアは更新サイクルが遅いため課題となる。スタックの一部で PQ 耐性アルゴリズムを採用していても、量子耐性のないファームウェアやブートローダーによって無効化される可能性がある。インベントリには老朽化製品を含め、 の後方互換性を維持しつつ PQC 導入を準備するハイブリッドソリューションを計画すべきだ。これにより内部ネットワーク内の相互依存関係への認識が保証される。

したがって、リスクベースの分類システムでは、暗号化アイテムをデータ機密性、アルゴリズム脆弱性、暴露期間、保護データの寿命、更新能力、依存関係（製品インベントリ入力に基づく）に基づいてスコアまたはタグを割り当て、マッピングすることを意味する。 この枠組みでは、ベンダーのロードマップがなく、長期アーカイブデータを防御し、製造事業者のセキュアブートに依存する RSA-1024 を使用するレガシーVPN は、高リスクとフラグ付けされる可能性が高い。逆に、ストリーム暗号 AES-256 を使用するマイクロサービス間の短命な内部セッションは低リスクとなる。

この意味で、暗号技術インベントリは量子移行を導く技術的羅針盤として機能する。インベントリ内に潜む価値を理解し、優先順位を付けるには、技術的リソースと戦略的思考の両方が必要となる。

第 V 部 量子耐性への移行状況：欧州連合（EU、フランス、ドイツ、オランダ）

1. 序論

本節では、欧州連合（EU）及びその加盟国であるドイツ、フランス、オランダの 3 カ国が、耐量子暗号への移行にどのように取り組んでいるかを検証する。まず、EU の包括的戦略から始める。この戦略は、PQC（耐量子暗号）と QKD（量子鍵配送）を、デジタル主権とデジタル単一市場というより広範なアジェンダの中に位置づけている。次に、選定した各国の事例に移る。ドイツ、フランス、オランダを選んだのは、分析的及び実践的な考慮によるものである。これらの国々は量子耐性移行における先行者であり、欧州レベルで主導的役割を担っている。ドイツは連邦情報セキュリティ庁（BSI）の指針策定や EU ロードマップ策定プロセスの共同議長国としての活動を通じ、政策面での先駆者となっている。フランスは量子暗号を包括的な国家量子戦略に組み込み、多額の投資と政府主導のパイロットプロジェクトでこれを支えている。オランダは規模こそ小さいが、エコシステム主導のイノベーションと暗号技術における機敏性を特徴とする独自のモデルを提供しており、ドイツ・フランスと共に EU の PQC ワーキンググループ共同議長国を務めている。これら 3 つの事例は、耐量子暗号に対する欧州の戦略的・機構的・技術的アプローチの代表者を示すと同時に、重点の置き方、実施スタイル、国家主導と多主体協調への依存度の違いも浮き彫りにしている。

2. 欧州連合

2.1. 戦略とビジョン

欧州連合の耐量子暗号へのアプローチは、加盟国間の調整とデジタル主権の追求を中核としている。EU レベルでは、PQC は全加盟国で同期したタイムラインを必要とする緊急の戦略的移行と位置付けられている。2024 年 4 月、欧州委員会は「調整された実施ロードマップ」を求める勧告を発表し、欧州が足並みを揃えて前進できるよう、各加盟国が包括的な国家 PQC 移行戦略を策定するよう促した。安全保障と防衛は主に国家の管轄権に属するが、EU 当局者は PQC 対応を欧州のデジタル単一市場に不可欠な要素と位置付け、サイバーセキュリティ規制に依存するものと見なしている。

並行して EU は、特に政府機関や重要インフラ向けに、将来にわたり安全なコミュニケーションを実現する補完的基盤として量子鍵配送（QKD）を構想している。

欧州量子通信インフラ（EuroQCI）プログラムでは、地上光ファイバーと衛星を介して全 27 加盟国を網羅する汎欧州 QKD ネットワークの構築を目指す。

2.2. 分析

2.2.1. EU の整合性の欠如

欧州には強力な暗号研究コミュニティと野心的な戦略があるにもかかわらず、政策ビジョンと実践的な実行の間に顕著な不整合が存在する。

一つの問題は、資金と注目の偏りだ。EU の量子通信（QKD 及び関連インフラ）への投資は、耐量子暗号（PQC）の実装に充てられる額を大幅に上回っている。この不均衡により、QKD 用の大規模試験ネットワークが構築される一方で、産業界や政府が日常的な暗号化を PQC に移行するための支援資源は相対的に少ない状況が生じている。 この格差は実用的な影響の速度と規模を制限する可能性がある。なぜなら、大半のデジタルシステムにとってより差し迫った重要性を持つ PQC へのアップグレードは、十分な資金、ツール、人材育成がなければ遅れを取る恐れがあるからだ。現在の投資格差は潜在的な機会費用を伴う。量子通信ネットワークの開発は長期的な戦略的取り組みとして価値があるが、現時点では専門的なユースケースに限定されている。一方、PQC への移行は公開鍵システムに依存するほぼ全ての分野に恩恵をもたらす、より即時的かつ広範なデジタルセキュリティの向上策である。したがって、重要な移行期においてセキュリティ効果を最大化するには、探求的な量子インフラと展開可能な量子耐性対策の間で資源配分を均衡させることが不可欠だ[16] 。

量子耐性技術群の技術成熟度にもばらつきがある。対称暗号（例：より長い AES 鍵の使用）や鍵交換プロトコルは量子耐性化が可能であり、パイロット実装が進められている。しかし PQC 代替技術はより初期段階にある：主要アルゴリズムの標準化はごく最近行われたばかりで、実運用プロトコル（TLS、セキュアメール、認証システムなど）への統合は依然として実験段階が主流だ。 これらの新アルゴリズムには標準化と認証のギャップも存在する。欧州には PQC 実装の妥当性確認や、製品（スマートカード、HSM、VPN など）の量子耐性としての認証を行うための、透明性があり拡張可能なプロセスが不足している。対照的に、QKD 分野では認証スキームや標準の策定に多大な努力が注がれており、PQC の「ソフト面」（標準、コンプライアンス、トレーニング）にも同様の推進が必要であることを示している。

さらに、EU プログラム間の資金継続性と整合性も完全には達成されていない。ホライズン・ヨーロッパは数多くの有望な PQC 研究プロトタイプや手法に資金を提供している（前述の通り、多くのアルゴリズム候補は EU 資金チームから生まれた）。しかしながら、Digital Europe や国家プロジェクトを通じた展開への移行は遅く、中央集権的な調整もなされていない。欧州委員会自体がこのリスクを認識している。調整が改善されなければ、研究が重要課題を解決する前に展開プログラムが「始動」し、遅延や後々最適でない解決策への投資を招く恐れがある。要するに、欧州は耐量子暗号技術に対して強力な戦略的ビジョンを有している。 しかし、実施メカニズムは未だ完全に同期していない（PQC と QKD への適切な資金配分から、一貫した標準化努力、研究から導入への同期化されたパイプラインに至るまで）。この不整合は断片化した取り組みを招き、一部の加盟国や産業が先行する一方で他が後れを取る結果となり、EU が目指す結束そのものを損なう恐れがある。

もう一つの不整合は、EU の政策アプローチにある。安全保障分野における補完性の原則に基づき、拘束力のある法律ではなく勧告や間接的な立法手段を用いるためだ。2024 年 4 月の PQC に関する勧告は指針とタイムラインを示すが法的拘束力を持たない。加盟国がこれに基づいて行動するかは各国の裁量に委ねられている。ただし同文書は、国家レベルで十分な進展が見られない場合、拘束力のある措置が追随する可能性があると警告している。 一方、サイバーレジリエンス法（CRA）のような今後の規制は、「最先端」のセキュリティ慣

[16] タスクフォース参加者の中には、この解釈が現行の資金配分優先順位に込められた戦略的意図を見落とす恐れがあると指摘する者もいた。量子鍵配送（QKD）や量子ネットワークへの投資は、単にショアのアルゴリズムに対抗するためではなく、量子技術アジェンダ全体を推進することを目的としている。これには実用的な量子ネットワークの開発や、光通信・通信グレード部品のサプライチェーン確保も含まれる。この観点から、量子通信プログラムと PQC（ポスト量子暗号）の取り組みは、統一された暗号化近代化プロセスの補完的な段階と捉えるべきだ。 PQC と暗号の俊敏性は既存インフラの保護に向けた即時的な手段である一方、QKD と対称鍵インフラはハードウェアベースの信頼性と長期的なレジリエンスを通じて、後期段階における多様化と多重防御を提供し得る。したがって「PQC 対 QKD」という固定観念は逆効果だ。両コミュニティは最終的に、暗号レジリエンシーを強化する認証可能で標準化され相互運用性のある解決策を追求している。 緊密な連携により、量子セキュリティ資金が研究やネットワーク実証実験を支援するだけでなく、展開・認証可能な暗号技術への橋渡しとなり、この移行を担う資源不足のサイバーセキュリティ機関への負担軽減が可能となる。この観点では、PQC と QKD は対立関係ではなく、欧州のデジタル自律性を強化する相互補完的な手段である。

行を要求することで、関係者を量子対応へ暗に促している。欧州委員会の 2024 年白書『欧州のデジタルインフラ需要をどう掌握するか』はこの関連性を明確にし、CRA への準拠は「適切な場合には耐量子暗号の使用を伴う可能性がある」と述べている。 実際には、CRA が完全に施行される時期（2027 年 12 月）までに、量子耐性のない暗号技術の使用は時代遅れと見なされる可能性がある。しかし、PQC（耐量子暗号）が明示的に義務付けられていないため、企業は具体的な要件の欠如を理由に、対応を先延ばしにするかもしれない。その結果、政策のギャップが生じている。EU が PQC への移行を可能にするという戦略的目標（ ）は明確だが、その実施は慎重な姿勢を保ち、自主的な調整と各国のイニシアチブに依存している。 加盟国によって対応能力や緊急度は様々だ。フランスやドイツなど先行する国がある一方、ほとんど着手していない国もある。EU 全体で拘束力のある義務がないため、移行の速度は地域の政治的意思や認識に依存する可能性があり、これはまさに調整されたロードマップが克服しようとした課題である。

最後に、研究・イノベーション分野では、現行の枠組みでは十分達成されていない広範な学際的取り組みの必要性が認識されている。PQC と QKD はしばしば別々の分野（前者は数学／コンピュータサイエンス研究所、後者は物理学／工学研究所）で進められているが、現実世界ではこれらを組み合わせた形（例：ハイブリッドネットワーク）で利用される可能性がある。 欧州のプログラムは、新たな PQC アルゴリズムがハードウェアに脆弱性を導入しないよう、暗号アルゴリズム設計とサイドチャンネル耐性を組み合わせることや、古典的・量子暗号システム双方を強化するために QRNG を統合することなど、専門知識の統合の重要性を強調している。

2.2.2. 整合性の欠如から生じる可能性のあるリスク

こうした不整合は EU に複数のリスクをもたらす。一つは欧州の技術主権という目標が損なわれる可能性だ。欧州の耐量子暗号への移行が他国より遅れる場合、欧州の産業や政府は外部ソリューションに依存せざるを得なくなる。 例えば、米国規制が 2025～2026 年までに特定の PQC アルゴリズム群を義務付けた場合、米国企業は技術開発に迅速に投資し、EU 企業が着手する前に市場を支配する可能性がある。そうなれば欧州企業や公共サービスは、非欧州ベンダーからソフトウェアライブラリやハードウェアを調達せざるを得ず、欧州の情報セキュリティに対する支配力が低下する恐れがある[17] 。

しかし欧州が世界的な調整なしに独自路線を進むリスクもある。EU が他地域で認知されない独自の暗号標準を推進した場合、欧州のテクノロジー製品は相互運用性の問題に直面したり、国際市場から締め出されたりする可能性がある。 EU 域内の企業は、EU 固有のアルゴリズムに対応したシステム開発に投資したにもかかわらず、米国やアジアの顧客が NIST 標準アルゴリズムを要求する（あるいはその逆）事態に直面し、複数バージョンの維持を余儀なくされるか、ビジネス機会を失う可能性がある。このような分断は、異なる規格に対応するリソースが少ない中小の欧州企業やスタートアップに特に打撃を与えるだろう。

もう一つのリスクは、EU の指針が拘束力を持たない点にある。強制力がないため、一部の加盟国がシステム更新を先延ばしにするシナリオも考えられる。

---

[17] タスクフォース参加者の中には、イノベーションのペースが遅くなれば欧州企業に不利になるものの、EU が自らの安全保障を確保する能力を必ずしも損なうわけではないと指摘する者もいた。実際、NIST アルゴリズムは公開・透明性が高く、欧州の重要な貢献によって形作られているため、欧州は自国の規制枠組み内でそれらを採用・認証できる。この観点では、主権は新たなアルゴリズムの創出ではなく、信頼できる実装、ガバナンス、そしてレジリエントな展開を確保することにある。

量子コンピューターが普及する頃には、EU 域内で準備状況に格差が生じている可能性が考えられる。強固な PQC（ポスト量子暗号）や QKD（量子鍵配送）インフラを整備した国がある一方で、脆弱性を持つ旧式暗号技術を継続する国も存在するかもしれない。このパッチワーク状態は、遅れた国々を脅かすだけでなく、データが国境を越えて流れる以上、集団的な安全保障をも脅かす。 弱点リンク問題が発生する。ある国のネットワーク内の脆弱なノードが、他国への攻撃の侵入経路となり得るのだ。また、長年にわたる警告にもかかわらず、欧州の片隅で PQC 導入が遅れたために重大な侵害が発生した場合、EU のサイバーセキュリティ政策の信頼性が政治的に損なわれるだろう。

さらに、調整されたリスク認識戦略なしに EU の量子耐性ロードマップを推進することには重大なリスクが伴う。ロードマップは必要なマイルストーンとその期限を明示しなければならないが、加盟国、ベンダー、機構がそれらを達成する方法を定義できるのは支援戦略のみである。標準、認証スキーム、相互運用性枠組み、試験インフラが同期されなければ、規制が準備態勢を追い越す可能性がある。 したがって、このロードマップは、国家計画、産業の取り組み、規制ツールを整合させるより広範な EU 枠組みに組み込まれるべきである。これにより、CRA（サイバーリスク管理指令）、DORA（デジタル業務レジリエンス法）、NIS2（ネットワーク情報セキュリティ指令）間の調整が確保され、ENISA（欧州ネットワーク情報セキュリティ機関）、欧州委員会、ETSI（欧州電気標準化機構）、CEN/CENELEC（欧州電気標準化委員会）などの標準化団体といった機構主体によって導かれ、一貫性のある実行可能な移行が実現される。

3. ドイツ

3.1. 戦略とビジョン

ドイツの量子戦略は、量子脅威を早期に認識し、国内および欧州レベルで耐量子セキュリティを実現する体系的な計画を特徴とする。BSI は 2020 年以降、組織に対し「耐量子暗号への移行」を警告し、耐量子暗号に関する詳細な推奨事項を発行している。ドイツのビジョンは「量子脅威に今すぐ対応せよ」という原則に沿っている。 具体的には、暗号学的に実用的な量子コンピューター（ ）が登場するよりはるか前に、政府および重要インフラシステムを PQC へ移行させることを目指している。BSI は米国と歩調を合わせた暫定指針（2030-2035 年までに PQC へ置き換えない限り、128 ビット以上の古典的セキュリティアルゴリズムのみを使用するよう推奨）を設定している。 戦略的には、ドイツは欧州の PQC 取り組みを調整するリーダーとしての役割も想定している。EU の PQC ロードマップ構想の共同議長を務め、2024 年の EU 共同声明にも貢献した。主権の観点もある。ドイツは堅牢な暗号技術をデジタル主権（EU 文脈でドイツ当局者が強調する用語）に不可欠と位置付け、外国技術の優位性にかかわらずドイツ・欧州のデータを安全に保つことを重視している。

量子鍵配送（QKD）に関しては、ドイツの戦略はより慎重だが、特定分野では確固たる姿勢を示している。政府は 2019 年に「QuNET」イニシアチブを開始した。これは公共機関向けの安全な量子通信ネットワークを開発するための複数年計画である。2020 年代半ばまでに、主要な連邦機関間で盗聴不可能な通信を可能にする量子ネットワークのパイロット版を構築するという構想だ。

3.2. 分析

量子暗号に対するドイツの政策姿勢は、政府・産業界・研究機関を橋渡しする多主体エコシステム構築を目指す。BSI（連邦情報セキュリティ庁）が中核機関として技術要件や認証基準を共有し、内務省や研究・技術・宇宙省などの他省庁が研究開発の実施と資金調達を支援する。QuNET や PARFAIT といったイニシアチ

ブは連邦政府の優先課題をパイロットプロジェクトに結び付け、PQC（ポスト量子暗号）と QKD を具体的なシナリオに組み込んでいる。国際的には、ドイツは標準化のリーダーとして自らを位置付け、量子安全な移行における相互運用性と欧州の主権を確保している。

4. フランス

4.1. 戦略とビジョン

フランスの量子暗号戦略は、同国の総合的な量子戦略に組み込まれている。フランスは 2021 年、「フランス 2030」投資計画の下で国家量子戦略を開始し、18 億ユーロ（うち 10 億ユーロは公的資金）の資金拠出を約束した。この戦略は、国家資金、民間投資、学術的卓越性を組み合わせ、2030 年までにフランスを量子技術のリーダーとして位置付けることを目指している。量子コンピューティング、コミュニケーション、センシング、暗号技術を包括し、量子攻撃に耐性のある暗号手法の開発に特に 1 億 5000 万ユーロが割り当てられている。戦略的優先事項として「耐量子 量子暗号技術の開発と普及」を含む 5 つの柱から構成される。これまでに 80 以上のプロジェクトが資金提供を受け、PROQCIMA（2032 年までに国産量子コンピュータを実現する計画）などの新プログラムが開始された。2022 年 11 月には、フランスがワシントン大使館とパリ間で耐量子暗号（フランス企業 CryptoNext Security の FrodoKEM を使用）で暗号化された初の外交文書を送受信に成功し、政府高官レベルでの PQC 導入に向けた重要な一歩となった。

4.2. 分析

量子耐性システムへの移行に関するフランスの政治的立場は、国家主導であり、主要機関としてフランス国家情報システム保安庁（*Agence nationale de la sécurité des systèmes d'information*, ANSSI）が中心となっている。この機構は、移行の当面の解決策として、従来の暗号と PQC アルゴリズムを組み合わせたハイブリッド暗号を推進している。フランスはまた、ドイツ、オランダと共に EU の PQC ワーキンググループの共同議長国を務め、欧州標準、研究開発努力、そしてより実践的には暗号の適応性（クリプトアジリティ）とハイブリッド方式を推進している。国家政策は、軍事・防衛目的の量子技術開発という広範な計画の一環として、PQC と量子通信手法の促進を含む、より広範な防衛セクターにおける量子プログラムによって強化されている。パイロットプロジェクトへの民間企業の参画は優先されており、PQC-QKD リンクで保護された量子ネットワークに関する RESQUE コンソーシアムがその例だ。主要通信事業者であるオレンジ社も参加しており、産業準備と試験を通じた戦略的自律性の目標を体現している。

5. オランダ

5.1. 戦略とビジョン

オランダは量子技術を国家優先課題と位置付け、セキュリティ配慮を統合しつつイノベーションとインフラ整備に注力している。2021 年、オランダ政府は国家成長基金から Quantum Delta NL（QDNL）に 6 億 1500 万ユーロを交付した。これはフルスタック量子エコシステム構築を目指す包括的国家イニシアチブである。この資金は、デルフト、アイントホーフェン、アムステルダム、ライデン、トゥウェンテの 5 つのイノベーションハブと、量子ハードウェア、ソフトウェア、量子インターネット、人材育成プロジェクトを支援する。主に研究開発と経済発展に焦点を

当てているが、QDNL は量子通信ネットワークの推進（大都市圏 QKD リンクの試験運用や欧州量子セキュアネットワークへの準備など）を通じて、間接的にセキュリティ強化にも寄与している。

並行して、オランダは国家安全保障機関[18] を暗号政策の指針としている。オランダ国家コミュニケーション安全保障局は、国内組織に対し、耐量子暗号への移行準備を今すぐ開始し、PQC 計画を遅延させるべきではないと明示的に助言している。 2024 年、国家安全保障局（CWI 及び TNO と共同で）は『*PQC 移行ハンドブック*』第 2 版を発行し、組織がポスト量子暗号へ移行するための段階的ガイドラインを提供した。同書は三段階のアプローチを提示している：(1) 量子脆弱性診断：暗号資産の識別と量子リスクの評価、(2) 計画策定：システムの優先順位付けと移行ロードマップの策定；(3) 実行：PQC ソリューションの展開と統合テスト。同ハンドブックは、この移行及び将来の移行を円滑化するため、暗号アルゴリズムを容易に交換できる「暗号アジリティ」の確立を強く推奨している。オランダ政府機関はまた、暗号技術の棚卸しとハイブリッド（PQC＋従来型）実装の実証実験を目的としたパイロットプロジェクト（省庁及び重要インフラ分野）を実施している。

政策は官民連携を基盤に、省庁・銀行・通信事業者でのパイロット事業を通じて実施される。国際的には、オランダはフランス・ドイツと共同で EU の PQC ワーキンググループを主宰し、NIST や EuroQCI へ積極的に貢献。先端研究・標準化・責任ある展開の架け橋として、ハイブリッドソリューションと倫理的ガバナンスを重視する立場を確立している。

5.2. 分析

オランダは量子移行に対し実践的なアプローチを取り、PQC への移行をより広範な暗号技術適応文化に組み込んでいる。企業は公共セクターのガイダンスを評価できる。オランダが特に優れているのは、この応用実験を幅広いステークホルダーの参加と組み合わせている点だ。QuSoft や QBird のようなスタートアップ、主要通信事業者や銀行が早期に参画し、移行を共有責任としている。 EU の PQC ワーキンググループ共同議長を務めると同時に、NIST や EuroQCI への貢献を通じて、国内の実践が国際規範を形成するよう確保している。要するに、オランダは技術的信頼性とエコシステム協力を活用して集団的リーダーシップを育むことに優れており、量子耐性セキュリティの推進において政策・研究・産業を橋渡しする方法を示している。

[18] https://www.aivd.nl/ を参照。

第 VI 部 量子耐性への移行状況：EU 域外（英国、米国、中国）

1. 序論

本節では、EU 以外の 3 つの主体、すなわち英国（UK）、米国（US）、中国に焦点を当てる。これらの戦略は、耐量子暗号への世界的移行を形作る上で特に影響力を持つ。事例選定は、これらの主体が持つ世界的意義を反映している。米国と中国は量子技術分野における技術競争の二大極であり、膨大な資源、地政学的野心、そして事実上の世界的標準を設定する能力を有する。 英国は実用的な移行ロードマップの先駆者であり、大西洋横断の標準化フォーラムに積極的に参加し、産業界の実務と同盟国間の調整の両方に影響を与えている。これら 3 つの事例を総合することで、異なるガバナンスモデルが量子耐性移行をどのように運用しているか、そしてそれが国際的な連携、主権、相互運用性に何を意味するかを比較検討する視点が得られる。

2. 英国

2.1. 戦略とビジョン

英国の PQC 移行戦略は、サイバーセキュリティの国家技術機関である国家サイバーセキュリティセンター（NCSC）の指針に基づいて策定されている。NCSC は、目標時期を示す 3 段階の移行ロードマップを提示している。 フェーズ 1（2028 年までに）では、組織が発見と計画を完了することが求められる。これには、詳細な鍵やアルゴリズムの監査ではなく、システム、サービス、製品全体に公開鍵暗号が組み込まれている場所を示す組織的なマップ、つまり高レベルの暗号資産インベントリの作成が含まれる。このようなマッピングにより、サプライヤーとの連携や、早期の保護が必要な長寿命の機密データの特定が可能となる。 重点は初期移行計画の策定にあり、標準の進化、アルゴリズムの脆弱性発見、ベンダー製品の変更が想定される。フェーズ 2（2031 年までに）では、10 年以上安全性を維持すべきデータを優先的に移行する。機密性の高い長期保存情報を収集・復号リスクから保護しつつ、業務上重要なプロセスへの早期混乱を回避する論理だ。 重要なのは、初期移行はエラーが発生しやすいことから、組織は最も重要なシステムから着手すべきではないと警告されている点だ。したがってパイロットプロジェクトと反復的な計画策定が不可欠である。フェーズ 3（2035 年までに）は完全移行を目指し、全てのシステム・サービス・製品が PQC へ移行することを保証すると同時に、デジタルインフラの包括的見直しが既に進行中であることを踏まえ、 全体的なサイバーレジリエンス強化の機会を捉える。

技術的アプローチでは、暗号の俊敏性と段階的なハイブリッド展開を重視する。組織は、アルゴリズムを最小限の再設計で交換可能なシステムを構築するよう奨励される。これにより、新たな脆弱性が発見された場合や標準が進化した場合の柔軟性が確保される。アルゴリズムの選択は主に NIST プロセスを反映し、モジュール格子鍵カプセル化

メカニズム（ML-KEM）が鍵確立に推奨され、モジュール格子ベースデジタル署名アルゴリズム（ML-DSA）が署名に、ステートレスハッシュベースデジタル署名アルゴリズム（SLH-DSA）が長期アンカーとファームウェア用に確保されている。 NIST のハミング準循環符号（HQC）は ML-KEM の代替候補として挙げられていたが、NCSC の公開ガイダンスには含まれていない。

より広範な文脈では、PQC は英国の国家量子戦略に位置づけられており、10 年間で 25 億ポンドが投入される。PQC はこの構想の中核的要素として認識されており、防御上の必要性だけでなく戦略的技術能力の一部として位置づけられている。NCSC は既にパイロットプログラムを開始しており、8 社が PQC 移行支援を提供し、エコシステム全体の能力構築を進めている。 実施アプローチは、厳格な義務付けよりも調達要件と市場誘導に依存している。例えば政府契約や防衛調達では、基準となるサイバーセキュリティ枠組みへの準拠が求められており、標準が成熟するにつれて自然に PQC にも拡大される。このアプローチは、多くの組織が暗号技術そのものではなく調達する製品・サービスに動機づけられていることを認識している。ベンダーが PQC を製品に組み込むにつれて、採用は連鎖的に広がるだろう。

3. 米国

3.1. 戦略とビジョン

米国は耐量子暗号を、近い将来のサイバーセキュリティ上の必須要件と位置付けている。 2022 年のホワイトハウス国家安全保障覚書 10 号（NSM-10）は「米国は 2035 年までに暗号システムの耐量子暗号への移行を優先すべきだ」と宣言した。この緊急性は、現行の公開鍵アルゴリズム（RSA、ECC など）が量子攻撃に対して脆弱であり、システム移行には数年を要するという認識に基づく。

米国の戦略は NIST の PQC プログラムに集約されており、2016 年以降、新アルゴリズム標準化のための公開競争を主導してきた。2024 年、NIST は初の PQC 標準標準セットを発表した：鍵カプセル化用 CRYSTALS-Kyber（連邦情報処理規格 FIPS 203、別名 ML-KEM）とデジタル署名用 CRYSTALS-Dilithium（FIPS 204、別名 ML-DSA）、さらに 2 つの代替署名方式（FIPS 205 SPHINX）である。ML-KEM とも呼ばれる）、デジタル署名用 CRYSTALS-Dilithium（FIPS 204、ML-DSA とも呼ばれる）、および代替署名方式 2 種（FIPS 205 SPHINCS+SLH-DSA と FIPS 206 Falcon Fast-Fourier transform over NTRU-Lattice-Based Digital Signature Algorithm（FN-DSA））である。 これらは現在広く使われているアルゴリズムの量子耐性代替手段となるプロバイダ。NIST は選択肢を多様化するため、追加の署名方式（オンランプ「ラウンド 2」候補）を引き続き募集している。 重要な点として、NIST と連邦機関は量子脆弱性のある暗号技術の段階的廃止スケジュールを策定している。例えば、112 ビットセキュリティの RSA/ECC は 2030 年までに非推奨となり、2035 年までに使用禁止となる見込みだ。 より強固な古典暗号（256 ビット ECC など）は 2035 年まで使用が許可される。この時点までに量子耐性ソリューションが整備される見込みだ。このタイムラインは、2035 年までに米国政府システムを移行させるという NSM-10 の目標と一致している。

3.2. 分析

米国は量子脅威を緊急の国家政策として扱っている。NIST のドラフト『PQC 移行報告書』は、そのタイムラインを NSM-10 に明確に結び付け、112 ビットのセキュリティ（例：3K ビット RSA）を 2030 年までに廃止し、全ての古典的公開鍵方式を 2035 年までに廃止することを推奨している。

NIST と米国研究所は実装上の課題にも取り組んでいる。NIST 主導の PQC 移行プロジェクトは産業界と連携し、性能・相互運用性・テストの問題に対処している。例えば、NIST の暗号アルゴリズム妥当性確認プログラムは既に連邦情報処理規格（FIPS）140 検証スイートで PQC 候補をテスト中だ。市場参入促進のため、国家サイバーセキュリティ卓越センター（NCCoE）は PQC 統合ガイドを開発中である。

プログラムは既に連邦情報処理標準（FIPS）140 妥当性確認スイートで PQC 候補のテストを実施している。市場参画促進のため、国立サイバーセキュリティ・センター・オブ・エクセレンス（NCCoE）は PQC 統合ガイドを開発中であり、サイバーセキュリティ・インフラセキュリティ庁（CISA）は重要分野のリスク評価を進めている。研究開発面では、量子ネットワーク試験床の構築が米国の取り組みに含まれる。シカゴ量子取引所の新設「Bloch Tech Hub」は、QKD 及び長距離量子通信技術開発専用の公開量子ネットワーク試験環境を構築予定だ。ただし米国当局は QKD に慎重姿勢を維持している。国家安全保障局（NSA）の指針は、耐量子アルゴリズムが QKD より「費用対効果が高く維持容易」と明記し、現時点で国家安全保障用途の QKD 機器認証を行っていない。実際には、米国での展開（通信、データセンターなど）はハイブリッドな PQC-古典モードから始まっている。これにより、政府やベンダーは、レガシー互換性を維持しつつ、TLS、VPN、パブリッククラウド暗号化への PQC の組み込みと妥当性確認を進められる。

米国は標準や政策フォーラムを通じて同盟国と連携している。NIST と商務省の代表者は、IETF 暗号フォーラム研究グループや関連作業部会（例：TLS 1.3）で積極的に活動し、グローバルプロトコルが PQC アルゴリズムを採用するよう確保している。同様に、米国代表団は ISO と国際電気標準会議（IEC）の合同技術委員会（JTC）1/SC 27 において、NIST 選定の鍵交換メカニズム（KEM）と署名方式を ISO 標準に組み込む作業を進めている。ETSI の新設セキュリティアルゴリズム専門家グループ（SAGE）作業部会（耐量子暗号）には米国参加者が関与し、5G/6G モバイル標準への PQC 統合に関する勧告を策定中だ。米国は輸出管理と研究開発保護で均衡を保つ「政府全体」の連携も重視している。

米国は QKD について、ハードウェア依存性（専用機器、信頼ノード）をもたらし、セキュリティ上のリスクとなりやすく、拡張性も低いと見なしている。そのため、米国は他国に実験を任せている。一方で、既存ネットワーク上で機能する解決策に注力している。ただし米国は QKD の動向を注視しており、敵対者が独占的な量子安全通信能力を獲得した場合、完全に無防備な状態に陥ることは避けたいと考えている。現時点では、PQC における主導権と世界的な移行の推進が、米国の量子暗号戦略の基盤となっているようだ。

4. 中国

4.1. 戦略とビジョン

中国は量子技術における世界的な主導権獲得という広範な野望の一環として、量子暗号技術と耐量子暗号技術の展開、およびこれらの技術の標準と中核的知的財産の支配を目指す、強力な国家戦略を推進している。

量子鍵配送の分野において、中国の構想は規模において他に類を見ない。政府および重要産業チャネル向けに特別に設計された全国規模（最終的には世界規模）の量子通信ネットワークを構想している。これは最高指導部によって承認されており、習近平国家主席は量子通信を中国の五カ年計画に組み込むことを強調し、長期的な戦略目標にとって極めて重要であると述べた。その結果、中国は 2016 年に世界初の量子衛星「米子」（HYPERLINK "https://www.cnsa.gov.cn/english/n6465652/n6465653/c6799624/content.html" ¥h ）を打ち上げ（ ）、衛星と地上局の量子鍵配送を統合した数千キロに及ぶ安全な通信ネットワークを構築した。

これと並行して、中国は PQC（耐量子暗号）の到来にも備えている。政府の暗号当局は量子脅威を見据え、新たな暗号アルゴリズムの評価と標準化を積極的に進めている。中国の暗号法は「商用暗号」（市民・企業・非機密政府情報が使用する）が法的にサイバー・情報セキュリティを防御すべき枠組みを定めており、この法律は将来の暗号手段として PQC と QKD を暗黙的に包含している。これに沿い、中国は 2025 年 2 月に「次世代商用暗号アルゴリズム」（NGCC）イニシアチブを開始した。量子攻撃に耐性を持つ新たな公開鍵、ハッシュ、ブロック暗号アルゴリズムを世界的に募集する取り組みである。これは自立のビジョンを反映している。NIST の選択を単純に採用するのではなく、中国は自国で評価し、国内で標準化できる可能性のある、国内または世界中から提出されたアルゴリズムを求めているのだ。重点は数学的問題の多様性（単一障害点へのヘッジ）と、中核暗号技術に対する主権の保持にある。

4.2. 分析

中国の耐量子暗号へのアプローチは、国家主導で拡張的、かつ戦略的に二つの軌道を進む。量子鍵配送（QKD）においては、その展開を地政学的資産と位置付け、他国が追随できない大規模なパイロット事業（北京-上海幹線、ミチウスなどの衛星リンク）を既に運用し、研究開発を全国的なインフラへと転換している。PQC（耐量子暗号）に関しては、NGCC イニシアチブが示すように、北京は NIST への依存を回避し、技術的多様性と主権を両立させた独自の標準ポートフォリオを構築する意図を持っている。本質的に、中国の戦略は中国の主導または管理下にある包括的な量子セキュリティエコシステムの構築を目指すものである。地政学的には、量子暗号は中国が飛躍的に進歩しルールを設定できる領域と見なされており、それによって西側の暗号標準への依存を減らし、自国の機密を確実に保護できるとされている。

第 VII 部 NIS 協力グループロードマップに関するタスクフォースのコメント

1. NIS 協力グループロードマップ

NIS 協力グループが詳述している PQC への移行は、3 つの主要なマイルストーン（2026 年、2030 年、2035 年）で構成されるロードマップと、すべての加盟国が予定通りに量子セキュリティを確保するための具体的なステップからなるプロセスである。

- **フェーズ 1：2026 年 12 月 31 日**までに、加盟国は PQC 移行の基礎を整備することが期待されている。この「最初のステップ」では、PQC 製品を推進するベンダーやプロバイダを含むサプライチェーン内で、初期の戦略と調整を指導する重要なステークホルダーを識別することが含まれる。企業は、自社の暗号在庫を開発・維持しなければならない。これに基づき、暗号素材の供給者と採用者は協力し、企業の暗号資産インベントリにおける依存関係をマッピングすべきである。規制団体は量子リスク分析を実施し、高リスクのシステム／データを識別するとともに、EU のタイムラインに沿った明確な優先順位（準備・計画・実行フェーズ）を定めた実施計画とスケジュールを策定する必要がある。さらに、多様な関係者が連携し、経営幹部から IT スタッフに至る全レベルで量子脅威に関する国内意識を高め、EU の作業プロセスに参加すべきである。いかなる加盟国も単独でこの移行を進めるべきではない。

フェーズ 1 終了時までに、長期的なデータ機密性ニーズや長寿命システムを有する重要分野では、既に PQC ソリューションの実験が開始され、EU 全体で最低限の準備態勢が確保される。

- **フェーズ 2：2030 年 12 月 31 日まで**に、全ての加盟国は以下の「次の段階」を実施すべきである。移行における資源配分は、耐量子暗号を義務付ける特定の規制枠組み内で、民間・公共双方の主体によって必要となる。標準やガイドライン（例：EU サイバーセキュリティ法）における認証スキームの更新が求められる。さらに、公的機関・民間・学術界の国内・国際連携を強化し、移行加速の機会（例：専門研修プログラム、移行支援研究イニシアチブ）をエコシステム内で模索すべきだ。最後に、欧州の試験インフラとの連携により、国境を越えたシステムの相互運用性を確保する必要がある。

この第二段階では、重要システムは量子耐性を備え、この時点以降に販売されるソフトウェアはデフォルトでそのような暗号化をサポートすべきである。

- **フェース 3：2035 年 12 月 31 日まで**に移行を完了またはほぼ完了させ、中～高使用ケースを全て PQC に移行させる。このマイルストーンは調整されたロードマップの集大成であり、欧州のデータとコミュニケーションが量子コンピューターの進化する能力から保護される時点を示す。

この調整されたタイムラインにより、欧州は緊急性を持ちつつも十分な注意を払って行動し、慌ただしいあるいは混乱した移行を回避できる。これらのマイルストーンと手順に従うことで、政策立案者は量子コンピューティング時代における安全性と機密性を守ることができる。

2. NIS 協力グループロードマップに関するタスクフォースのコメント

2.1. 序論

本タスクフォースは、2025 年 6 月 11 日に NIS 協力グループが発表した「耐量子暗号への移行に関する調整実施ロードマップ」（以下「本ロードマップ」）をアセスメントし、以下のコメントを提出する。

2.2. ロードマップに関する全体的なコメント

- 本ロードマップは非常によく書かれ、有用である。特に、マイルストーンが国際的なエコシステムとよく整合していること、量子安全なソフトウェアおよびファームウェアへの早期移行の重要性が強調されていること、公開鍵基盤（PKI）や長寿命デバイスなどが直面する長い移行期間の課題が、これらのシステムについてできるだけ早く移行計画を開始する必要性とともに明確に記述されていることを高く評価する。

- 我々は、PQC への移行を促進する EU の包括的アプローチを支持する。特に欧州委員会が加盟国だけでなく産業界や学術界とも連携する姿勢を歓迎する。これらの利害関係者は全て、委員会が PQC のための効果的な支援策を設計する上で重要な役割を果たすだろう。

- 本ロードマップは、脆弱性の識別と移行計画策定に不可欠な暗号技術インベントリと依存関係マップの必要性を強調している。

- 量子脅威と PQC 移行の重要性について関係者を教育するため、個別対応型のキャンペーンを推奨している。

さらに、自らを「ハイレベルな概念文書」と定義しつつも、非常に実践的であり、迅速な実施を強調し、かなり具体的である。 例えば、加盟国に対し、この作業ストリームの最終成果物を待たずに、移行計画の作成または更新を直ちに開始し、最初のステップと並行して次のステップの実施を開始するよう促している。これにより、「2026 年末までに全ての加盟国で最低限の準備態勢を確保する」ことを具体的に目指している。

- 優れた実践例を具体的に示している。例えば 11 ページでは、フランスで実施された調査について言及している。その目的は「市場の準備状況を判断し、PQC 移行の障壁を識別し、3 種類の利害関係者（プロバイダ、ユーザー、コンサルティング会社）のニーズを把握すること」である。

- また、国家レベルで規定されている関連規制や技術要件、ガイダンスは、PQC に関する最新の推奨事項とともに、体系的に更新されるべきであると述べている。そのような規制や暗号政策が存在しない場合、加盟国は、例えば他国や NIS 協力グループに相談して、それらを作成することを検討すべきである。 PQC の普及には、製品の入手可能性と、機構による模範的な事例の両方が必要である。加盟国は、将来の国家調達プロセスに PQC 要件を組み込むことを検討すべきであり、現在の IT サプライヤーに連絡して PQC に関する成熟度を評価することが推奨される（14 ページ）。

- このロードマップは、データの機密性と完全性を保護することの重要性を強調している点で優れている（4 ページ）。しかし、クラウド上で機密情報を処理することがますます一般的になっているため、処理中のデー

タを防御する必要性についても明確に言及すべきである。 さらに、「保存中」「伝送中」「通信中」といった用語を使用する代わりに、「伝送中、保存中、処理中のデータの機密性と完全性を防御する」という広く受け入れられている表現を一貫して使用することを提案する。

- また、ロードマップでは可用性防御の必要性も明示的に強調すべきだ。可用性は完全性保護の結果として部分的に実現されるが、PQC 移行が重要インフラの可用性確保にも寄与することを読者に理解させる必要がある。ほとんどの重要システムにおいて、可用性は機密性・完全性と同等かそれ以上に重要であり（ ）、これを明示することで PQC の早期導入が必要な理由の全容を伝えるのに役立つ。

2.3. タイムライン

- 本ロードマップは PQC 移行の明確なタイムラインとマイルストーンを示し、高リスクユースケースは 2030 年までに、中リスクユースケースは 2035 年までに移行すべき緊急性を強調している。

- 具体的には、2035 年というタイムラインの完了日と、優先順位付けのアプローチの両方が非常に適切である。セクター間の複雑さ、加盟国間の成熟度の違い、厳しすぎずに明確である必要性を考慮すると、この文書とそこに記載されたロードマップは適切なバランスを保っている。

- 我々は、「最初のステップ」と「次のステップ」を作成しながら「今すぐ開始する」というアプローチ、および NIS 協力グループによって提案されたタイムラインを支持する。

- また、タイムラインと行動（2026 年、2030 年、2035 年）が米国の政策とも概ね一致していることを高く評価する。

- しかし、ロードマップはイニシアチブを完全に個々の加盟国に委ねているため、各国のアプローチをどのように調和させるかについては触れていない。さらに、EU が調整役を果たすかどうかは依然として不明であり、ロードマップは違反の結果について具体的に述べていない。

- ロードマップは、このタイムラインが展開に適用されることをより明確に記述するよう更新すべきだと考える。展開システムにおける PQC の完全な採用には、標準の更新と、展開のマイルストーンよりかなり前に安定した実装が利用可能になることが不可欠である。標準開発機関、機器ベンダー、システムを展開する事業者など、エコシステムにおけるさまざまなステークホルダーのタイムラインは、本質的に異なる。 標準団体は仕様を早期に確定し、ベンダーはソリューションの実装・テスト・認証に十分なリードタイムを必要とする。これらを経て初めて大規模展開が可能となる。各段階の明確な区別は、関係者の期待値を調整し、各主体が効果的に貢献計画を立てられるようにする。

- 実地でのパイロット運用と学習に焦点を当てている点を歓迎する。これらのパイロットでは、セキュリティが PQC 対応インフラに根ざす必要があるため、完全なスタックを試験運用することが重要な側面である。

- 継続的改善を可能にする PQC 対応更新の推進というアプローチを支持する。この目的を完全に達成するためには、ハードウェアベンダーとのパイロット実施により最新技術を理解し、ギャップを識別することを提案する。更新不可能なシステム（ハードウェア制限などによる）の取り扱い方法を明確化する必要がある。

パイロットユースケースは次の要件を満たすべきだ：i) 基礎から構築されること、ii) ハードウェアを含めること、iii) アプリケーションレベルのパイロットが PQC 対応インフラとハードウェアによって支えられることを保証すること。

2.4. 暗号アルゴリズムに対する脅威

「量子コンピューティングは多くの暗号アルゴリズムに対する脅威となる」

「量子コンピュータの開発は、使用中の多くの暗号アルゴリズムを破るために利用可能な脅威を暗号学にもたらす。」

- CRQC によって脅威に晒されるのは公開鍵アルゴリズムのみであることを明記すれば、読者にとってはるかに有益である。大半の読者は、耐量子暗号や量子攻撃に関する深い知識を持つ暗号専門家ではない。128 ビット鍵の対称アルゴリズムが CRQC によって実質的に脅威に晒されるという考えは、現在では誤解と見なされている[2–6]。CHES 2024 基調講演で説明された通り、量子コンピューターが単一の AES-128 鍵を破るには、月の表面積に相当する量子ビットが必要となる。対称鍵の長さを増やすことに注力することは、緊急の優先事項である耐量子公開鍵アルゴリズムへの移行から注意と資源をそらす。このような注意散漫は、費用がかかるだけでなく危険でもある。欧州は PQC 導入において既に米国に後れを取っており、最も必要な分野に努力を集中させることは一層重要だ。したがって我々は以下の改善案を提案する：

「量子コンピューティングは多くの公開鍵暗号アルゴリズムに対する脅威となる」

「量子コンピュータの開発は、公開鍵暗号に対する脅威をもたらし、使用中の多くの公開鍵暗号アルゴリズムを破る可能性がある」

- この文脈において、ロードマップが 6 ページで「用途によっては、公開鍵暗号の代わりに対称鍵方式を検討する価値がある」と認めている点は重要である。

- ここで、これが実際に何を意味するのかを詳しく説明する機会が必要だ。具体的にはどのユースケースか？どのアプローチか？ハイブリッドか？PQC に焦点を当てた取り組みは、主に大規模なユースケースに集中している。しかし、単に PQC アルゴリズムに更新するだけでは済まない複雑なシステムを担当する者も、同様に指針を必要としている。

ユースケースは大きく以下の 2 つのカテゴリーに分類できると考えられる：

- オープンでアドホック、大規模な「上位」レベルのアプリケーションにおいては、PKI が依然として洗練された最適な解決策である。ただし、保護対象システムが重要である場合や長期的なセキュリティを必要とする場合、少なくとも選択肢として「対称鍵インフラ」を活用し、多層防御と高信頼性の長期セキュリティを提供することが有効である（TLS や IPsec などの PSK メカニズムを通じた形が考えられる）。

小規模、非公開、ハードウェアに近い（例：光伝送ネットワーク向け独自セキュリティプロトコル（OTNsec））、あるいはエンドポイントが静的なユースケースでは、対称鍵方式がより自然である。公開鍵アルゴリズムを含めることも可能だが、完全な PKI の複雑さは不要かもしれない。

2.5. ハイブリッドソリューション

「同一のメカニズムにおいて、耐量子アルゴリズムと脆弱性アルゴリズムを組み合わせたもので、その安全性は構成要素のうちより高い方の安全性に準ずるものとする」

- 「ハイブリッド」の定義はやや狭く、古典的攻撃に対する量子化以前公開鍵暗号のセキュリティへの信頼を維持しつつ、PQC が提供する最高のセキュリティを活用することに焦点を当てている。少なくともこれはハイブリッド鍵交換の特殊なケースであることを示唆している（ハイブリッド署名も存在するが、それはさらに複雑で目的も異なる）。例えば、PSK（あるいは帯域外対称鍵）と公開鍵暗号から導出された鍵を組み合わせる手法を指す場合もある。例えば BSI は、QKD 鍵を使用する場合、PQC および ECC ベースの鍵と組み合わせることを推奨している。

「耐量子暗号ソリューションへの移行時には、実現可能かつ適切な場合には、標準化され検証済みのハイブリッドソリューションの使用が推奨される」

- この点については、より詳しく説明し、明確化すべきだと考える。業界や政府によって国際的に広く採用されている標準化されたアルゴリズムのみを使用すべきであるという点には同意する。しかし、SLH-DSA などのハッシュベースの署名を用いたハイブリッドソリューションの使用を推奨している主要な団体は、現時点では存在しないことに留意することが重要である。また、自由に利用可能な仕様のみを使用すべきであることも明確化すべきである。 多くの組織は、暗号アルゴリズムの有料仕様をサイバーセキュリティ上のリスクとみなして、断固として反対の立場を取っている。IETF と NIST は、そのようなアルゴリズムへの言及を可能な限り削除するよう取り組んでいる。NIS 協力グループも同様に、有料の暗号技術への言及を避ける必要がある。

- ハイブリッド KEM は IETF によって標準化され、実際の展開でも採用されているが、ハイブリッド署名については、同レベルの標準化や実装の成熟度は達成されていない。その結果、ハイブリッド署名は EU ロードマップのスケジュールに間に合うよう準備が整う可能性は低い。 現在、OpenSSL 3.5 長期サポート (LTS) で TLS での使用がサポートされている唯一の署名アルゴリズムは、スタンドアロンの ML-DSA である。米国および英国の政府は、IETF や ETSI などのオープン標準化団体での進展を推進するだけでなく、主要な暗号ライブラリにおけるスタンドアロンの ML-KEM および ML-DSA の実装を支援する上でも、はるかに積極的な姿勢を見せている。 皮肉なことに、標準化されたハイブリッド KEM 仕様（ETSI CatKDF および CasKDF）は英国政府が主導したものだが、同政府は現在ではスタンドアロンの ML-KEM と ML-DSA のみを推奨している。

- 現実的な移行経路として、業界が現在採用可能なのはハイブリッド型 ML-KEM、スタンドアロン型 ML-KEM、スタンドアロン型 ML-DSA、そしてある程度スタンドアロン型 SLH-DSA に限られる。代替 PQC アルゴリズム（FN-DSA など）は、要求されるタイムラインに間に合う形で標準化され広く実装されることはないだろう。

- TLS においては、X25519ML-KEM は既に大規模な実装サポートを得ており、OpenSSL、Firefox、Chrome、Edge、Go などでデフォルトとなっている。Cloudflare の報告によれば、全 HTTPS クライアントリクエストの 40%以上が PQC を使用している。OpenSSL 3.5 LTS は ML-KEM、ML-DSA、SLH-DSA をサポートする。 OpenSSH は現在、デフォルトの鍵交換方式として ML-KEM を採用している。多く

の IKEv2 実装が ML-KEM をサポートしている。IKEv2 は常に楕円曲線ディフィー・ヘルマン一時鍵交換（ECDHE）とのハイブリッド方式で ML-KEM を使用する。十分にテストされ相互運用性のある実装の可用性は、コスト効率が高く信頼性のある相互運用可能な展開を可能にするため、業界での採用における重要な要素である。

我々は、ロードマップを更新し、ML-KEM、ML-DSA、SLH-DSA を完全に採用すべきだと考える。これらは世界的な標準であり、世界中の主要な暗号研究者による長年の共同研究の成果である。 重要なことに、Kyber、Dilithium、SPHINCS+ の著者のほとんどはヨーロッパの研究者であり、その多くはヨーロッパの大学、研究所、企業から支援を受けている。EU 加盟国および欧州委員会からの研究資金が、これを実現する上で大きな役割を果たしてきた。これらの投資により、ヨーロッパは、将来の脅威から世界のデジタル インフラストラクチャを保護する上で中心的な役割を果たすようになった。これは、NIS 協力グループがその報告書で明確に認め、称賛すべき成果である。

しかし、ハイブリッド暗号を義務化すると、過度のパフォーマンスのオーバーヘッドが発生したり、すべてのプラットフォームで有効化されないリスクがあると考えられる。この点については、詳細な調査とベンチマークを行うべきである。

また、EU のロードマップが、実現可能な場合はハイブリッド型の耐量子暗号を強く推奨しているのに対し、米国、より具体的には NSA は PQC のみの標準を推奨しているという点で、顕著な違いがあることも指摘しておきたい。 さまざまな顧客がさまざまなリスクを考慮することを認識し、可能な場合は顧客に暗号の選択肢を提供することが目的であるべきだ。ただし、インフラストラクチャレベルでの決定など、一部の暗号に関する決定は顧客が設定できない場合がある。

2.6. インベントリ

あらゆる事業体にとって最初の必須措置であり後悔のない行動は、暗号処理を行う資産の最新インベントリを作成し維持することだ。

- 包括的な暗号資産目録の作成と維持が不可欠である点には全面的に同意する。目録作成を今まさに開始する組織は、ML-KEM、ML-DSA、SLH-DSA の計画・試験・実装と並行して目録作成を行うべきだ。

  ただし、サプライチェーンを含む完全な暗号資産目録の作成は、一部の組織にとって負担が大きすぎる可能性がある。継続的なリスクアセスメントに基づき、トップダウン方式で目録を作成し、アプリケーションや使用状況に掘り下げていく方が効率的だと考える。なぜなら、一部のサプライヤーやシステムの非準拠は全体的なリスクが無視できるレベルである一方、他のものはエンタープライズにとって極めて重要だからだ。

  IT システムと資産の適切なインベントリを保有する組織は極めて少ない。理想としては望ましいが、過去数十年の実績から実践では極めて困難であることが示されている。量子耐性化への移行において、このロードマップの構成が組織のより重要な活動から注意をそらす可能性があるため、慎重な検討が必要だと考える。

  最近の経験から、 の取り組みをどう活用するかを明確に理解せずに を構築しようとすると、その努力が無駄だったという結論に至りかねないことが示されている。どのような種類の が必要で、それをどう活用できるかを明確にすることが極めて重要だ。

2.7. 標準

- 全体として、欧州委員会が秩序ある移行には国際標準が不可欠であると認識し、また EU 域内の高リスク・中リスクユースケースにおける PQC 移行をグローバルなエコシステムと整合させて完了させる決意を示したことを歓迎する。また、そのタイムラインと行動計画（2026 年、2030 年、2035 年）が米国の政策ともおおむね一致している点にも留意した。

- 我々は、世界トップクラスの PQC 科学者が参加した公開競争を通じて定義された NIST の PQC 標準を基盤とする、標準ベースのアプローチを支持する。

- 新暗号技術への更新が必要な標準の数が広く認識されていないと考える。数百に及ぶプロトコル標準や業界標準のうち、量子耐性に対応したものはごく一部に過ぎない。多くの産業がこれらの標準に依存しており、標準更新なしには移行が不可能だ。 我々は、更新が必要な影響を受ける全標準の一覧と、その更新予定時期を、可能な限り多くの標準団体に正式に要求すべきだと提案する。これにより現状把握が可能となり、関連標準団体の行動喚起につながるだろう。

- 認証への過度な依存は、最良のソリューションが市場で成功するのを妨げる恐れがある。リスクを意図的に管理しシステムを改善する「プロセス」認証（例：ISO 27000）の役割は認めつつも、サードパーティ認証だけが PQC 適合性を証明する唯一の手段であってはならない。より多くの業界主導の取り組みやツールを支援すべきである。

- EU の CRA プロセスとの連携強化を提案する。具体的には、製品プロバイダに対し自社製品に含まれる暗号技術を明記させる認証要件を設ける形が考えられる。これにより、量子耐性ソリューション提供に依存する組織にとって重要なサプライチェーンの大部分が即座に可視化される。

2.8. 認識、協力、ガバナンス

「サイバー空間では、すべての国家が国境を越えてつながっており、この移行においても相互に依存している。したがって、加盟国は組織、事業体、関係者が知識と経験を共有できる環境、すなわち コミュニティを構築すべきである。」

- 我々は、全ての国家がサイバー空間だけでなく、貿易や世界市場を通じて相互に接続されていることに同意する。国際的に活動する欧州産業にとって、既に公表されている世界的なタイムラインやアルゴリズムの推奨事項[1-15]との緊密な連携が不可欠である。 多くの欧州企業は既に、自社製品・サービスにおける ML-KEM、MLDSA、SLH-DSA の開発・実装に深く関与し、野心的な 2030-2035 年 PQC 展開スケジュール達成に向けて取り組んでいる。

- 各加盟国が単独で、IETF、第 3 世代パートナーシッププロジェクト（3GPP）、米国政府、あるいは米国の主要企業といったグローバル組織や事業体、利害関係者を惹きつけるコミュニティを構築できると期待するのは現実的ではない。EU レベルでの調整でさえ極めて困難である。 その代わりに、加盟国は IETF や 3GPP といったオープンなグローバル標準化組織や、オープンソース暗号コミュニティに積極的に参加し、国際レベルでの連携、影響力、知識共有を確保すべきだ。

- 加盟国は透明性のある移行計画で率先すべきだ。政府の移行ロードマップを公表し、タイムライン、マイルストーン、予算を含め定期的に更新することで、知識共有とベストプラクティスを促進する。

- ロードマップは「ステークホルダー」の定義を省庁、規制機関、技術専門家を超えて拡大すべきだ。市民社会、マイノリティネットワーク、草の根組織は単なる「相談相手」ではなく共同リーダーとして認識されるべきである。

- 調達、パートナーシップ、政策評価への社会条項とコミュニティ配当の統合は、「ベストプラクティス」としてだけでなく、測定可能な包摂のための要件として不可欠である。

- 啓発キャンペーンや研修モジュールは、汎用的あるいは画一的であってはならない。本 CEPS タスクフォースは、市民教育とデジタル教育の抜本的拡充を要請する。PQC（耐量子暗号）の認知、量子リスク、デジタル権利といったテーマを、技術チームだけでなく社会全体、学校、介護機構、コミュニティセンターに浸透させる必要がある。

- ロードマップは、市民が情報を受け取るだけでなく戦略を積極的に形成できる仕組み（市民議会、協議パネル、定期的な透明性のある更新）を確立すべきだ。

- ロードマップは、2030 年までに国境を越えたサービスにおける PQC の相互運用性を試験する EU レベルの共同パイロットプロジェクトを促進すべきだ。

- 我々は、進捗を監視し必要に応じてスケジュールの前倒しを推奨するため、ENISA 傘下に官民共同の PQC 移行監視機関を設置することを提案する。

- 政策立案者が実施を進めるにあたり、管轄区域内または区域間で技術的課題や相互運用性の問題を引き起こす可能性のある、規範的な規制や要件は避けるべきだ。我々は移行戦略と標準に関する国際的な対話の継続を提唱する。一つの可能性として、G7 が金融セクターにおける現行の量子安全イニシアチブの範囲を拡大し、全分野にわたるより広範な議論を含めることを歓迎する。

2.9. 相互運用性の課題

本ロードマップは、移行期間中の相互運用性維持の複雑性、特に国境を越えたサービスや相互依存的な暗号システムにおける課題に十分に対応していない。混乱を回避しシームレスな移行を確保するには、こうした（国境を越えた）組織間の緊密な連携が不可欠である。

2.10. 並列化の強化

ロードマップの現行構造は、段階的または直線的なアプローチを暗黙的に前提としており、特にある領域の進捗が別の領域の完了に依存する場合、意図せずボトルネックを生む可能性がある。EU 全域における暗号システムの複雑性と多様性を考慮し、進捗加速とシステミックリスク低減のため、ロードマップへの並行処理の強化を推奨する。 以下に、調整と整合性を維持しつつ並列性を高めるための具体的かつ実行可能な提案を示す。活動の一連の流れ（例：インベントリ→リスクアセスメント→パイロット→展開）を厳格に推奨する代わりに、ロードマッ

プをモジュール化され組み合わせ可能なマイルストーンパッケージとして構成することを提案する。これらのモジュールは条件が許せば独立して開始でき、加盟国、セクター、事業者が先行する全タスクの完了を待たずに前進することを可能にする。

例えば：

- プロトコル準備状況の評価と並行して、資産の棚卸しと暗号資産の分類を進めることができる。
- ベンダーとの協議や調達計画は、規制整合性の議論が進行中である間にも開始できる。

ロードマップを役割別トラックに分解することを提案する。各トラックは独自の活動、成果物、タイムラインを持つ。これらのトラックはエコシステム全体の自然な分業を反映し、異なるステークホルダーが並行して進められるようにする：

- 政策・規制トラック：義務付け事項、法的調和、公共セクターの資金調達手段に焦点を当てる。
- 標準化と相互運用性トラック：プロファイリング、適合規準、新興国際標準の統合に焦点を当てる。
- ベンダー支援トラック：PQC 対応製品の開発、認証、ベンチマークを促進することに焦点を当てる。
- 運用展開トラック：資産インベントリ、暗号部品表（Cryptography Bill of Materials）、公共サービスの移行、インシデント対応の更新に焦点を当てる。
- 監視と指標トラック：測定枠組み、監査、成熟度モデルに焦点を当てる。

この構造により、各ステークホルダーグループは他のグループの進捗に関係なく、関連するタスクに取り組むことができる。

2.11. コスト見積もりに関するガイダンス

本ロードマップは、ハードウェアの交換、ソフトウェアの更新、潜在的なダウンタイムを含む PQC 移行のコストを推定する方法論について言及または示唆していない。組織が効果的にリソースを配分し予算を計画するためには、包括的なコスト枠組みが不可欠である。

2.12. 法的枠組み

ロードマップは 3 ページで関連する法的枠組みについて言及しているが、一般データ保護規則（GDPR）が省略されているのは非常に奇妙だ。これはデジタル環境における中核的な法令であり、最先端のセキュリティ対策に関する規定や暗号化への具体的な言及を含んでいる。EU のサイバーセキュリティ関連法規では相互関連性から GDPR が頻繁に言及されており、で GDPR に触れることは PQC 採用の説得力を確実に高めるだろう。

同様に、本文書が NIS2、信用情報機関（CRA）、電子識別・認証・トラストサービス規則（eIDAS）の監督当局の関与の重要性を述べている箇所については、データ保護当局もこのプロセスに確実に参加すべきだと考える。DORA 監督団体についても同様だ。

同様に、一貫性と明確性を高めるため、eIDAS を他の法令と共に 3 ページで言及するのが妥当である。なぜなら、その監督団体は後段で関連ステークホルダーとして示されているからだ。

2.13. 編集上のコメント

定義のセクションは有用かつ正確である。しかし、文書内の位置がかなり遅い（技術的・政策的内容が既に様々な用語を使用した後）。定義を文書の早い段階に配置するか、主要用語（例：「ハイブリッド」、「量子耐性」）を要約する（例えば、エグゼクティブサマリーのボックス付き用語集で）ことで、読者が最初から方向性を把握しやすくなるだろう。

段階的なロードマップ（2026 年、2030 年、2035 年）は本稿の最も優れた部分の一つだ。緊急性と現実性のバランスが取れている。米国や英国の政策（NSA、NIST、NCSC など）への言及を含めることで、EU の推奨事項をグローバルな文脈に位置付ける助けにもなっている。タイムラインをガントチャートやインフォグラフィックで視覚的に要約すると、明確さと関与の促進に役立つかもしれない。

技術的なセクションは長いが理解できる。特定のリスクモデル（例：PQC 移行ハンドブック図 2.7）への言及は有用だが、一部の相互参照はリスクマネジメント手法（ISO 27001 など）への習熟を前提としており、技術的な読者全員が共有しているとは限らない。リスクスコアの算出方法を平易に説明した 1 段落の解説が有用だろう。

第 VIII 部 金融セクターにおける PQC への移行

1. 序論

本章では金融セクターにおける PQC への移行を検討する。量子コンピューティングが決済、メッセージング、本人確認といった中核システムを脅かすと結論づける。機構は暗号資産の棚卸しを開始し、長期保存される機密データへの防御を展開するよう促される。タイムラインの不確実性にもかかわらず、今すぐ着手すべきという点で業界全体で一致している。

EU、英国、米国では規制対応が異なるが、共通の方向性を共有している。EU の DORA は暗号技術の適応性と新興脅威への認識を義務付ける。英国は協力フォーラムと長期的なタイムラインを通じた業界主導の行動を支援する。米国は連邦システムに期限を設け、業界の移行を支援する。各管轄区域は 2028 年から 2030 年を目途に共通標準と実施目標に向けて取り組んでいる。

PQC 導入を遅らせる 3 つのボトルネックは、技術的課題、人材不足、ベンダー依存である。レガシーシステムは改修が必要で、人材が不足し、サプライヤーも完全な PQC 対応には至っていない。これらの要因がコスト増と対応遅延を招く。協調的な取り組みがなければ、組織は互換性の欠如や標準の分断化リスクに直面する。

- レガシーシステムは設計上、暗号技術への適応性に欠ける。
- 金融 IT チーム（および経営陣内）における暗号技術の専門知識は限られている。
- ベンダーや標準団体は業界のニーズに遅れを取っている。

2. 金融セクターにおける PQC への移行

量子暗号の出現は、決済・銀行間通信・デジタル ID を保護する公開鍵暗号を脅かし、金融システムにシステミックリスクをもたらす。十分な性能を持つ量子コンピュータが登場すれば、決済ネットワーク（例：SWIFT）や認証システムを防御する RSA・ECC 等のアルゴリズムを破り、取引の機密性・完全性を損なう可能性がある。金融情報の長期的な機密性を考慮すると、現在送信中または保存中のデータが遡及的に暴露される可能性があり、金融セクターの基盤となるセキュリティへの信頼が損なわれる。

金融システムが暗号技術に大きく依存している以上、量子技術による暗号解読は深刻な結果を招く。決済システムやデジタルバンキングは、取引や本人確認のために暗号化通信経路（VPN トンネルや TLS など）とデジタル署名に依存している。現状の暗号保護策が破られると、資金移動が改ざんされたり、身元がなりすまされたりする可能性がある。この点を認識し、規制当局や中央銀行関係者は警鐘を鳴らしている。 欧州中央銀行（ECB）のクリスティーヌ・ラガルド総裁は、次の金融危機はサイバー関連のものになる可能性を示唆している。重要なのは、金融事業体が耐量子暗号（PQC）への移行を緊急に行うべきだというコンセンサスだ。ECB、国際決済銀行（BIS）、オランダの PQC 移行ハンドブックは、銀行を「緊急導入者」に分類し、可能な限り早期に移行を開始すべきとしている。

重要なニュアンスとして、量子リスクは未知の期限（CRQC の到来時期は一部の専門家により 2030 年から 2035 年と推定される）と差し迫った脅威（「今すぐ収集し、後で復号する」）を併せ持つ。この特異な課題により、金融セクターは現在のサイバーセキュリティと将来を見据えた対策のバランスを取る必要がある。

要約すると、金融セクターにおける PQC 移行は安定性と信頼の維持が必要であることから推進されている。したがって金融システムに対する量子脅威は存亡に関わるものであり、データの機密性だけでなく中核的な金融機能の継続性を脅かす。この認識が、量子コンピューティングの進展時期が不確実であるにもかかわらず、今すぐ PQC 移行を開始すべきという世界的な要請の根拠となっている。金融機関は暗号資産を棚卸し、脆弱性（長期保存される秘密鍵、重要な取引リンクなど）を特定し、まずそれらの領域から量子耐性ソリューションの展開を開始すべきだ。

3. 現行の規制環境（EU、英国、米国）

欧州連合：EU は金融セクターに関する特定の規制を有しており、特に DORA（デジタルリスク管理指令）とその実施規則を通じて規定されている。幅広い金融事業体に適用される DORA は、暗号リスクを含む厳格な ICT リスクマネジメントを義務付けている。DORA 第 9 条は、事業者が ICT システムのセキュリティと機能を監視・管理し、データ機密性と完全性に関する高い標準を維持することを要求する。特に重要なのは、2024 年 3 月に DORA に基づく欧州委員会委任規則（EU 2024/1774）が制定されたことで、金融機関は技術進歩に対応した暗号化・暗号管理方針を策定することが義務付けられた。この方針には、確立されたベストプラクティスや標準に基づく暗号技術選定規準、ならびに の暗号解読技術進歩に応じて必要に応じて暗号技術を更新・変更する規定を含めなければならない。最先端の暗号標準に即時対応できない事業体は、サイバー脅威に対するレジリエンスを確保するため、補償的統制を実施しなければならない。暗号技術の種類や手法については、大半の機関関係者（BSI、ANSSI、欧州委員会）が暗号技術の俊敏性の重要性を強調している（[19]）。EU の立場は、事実上、量子技術への対応を業務継続性コンプライアンスの一部としている。金融監督当局は「最先端」セキュリティ原則（GDPR に組み込まれ、DORA 要件で再確認され、CRA で強調される）を根拠に、暗号技術を最新状態に保つ企業責任を追及できる。しかし規制当局の期待と業界の認識には依然として隔たりがあり、認識がある場合でも「最先端」があらゆる状況で何を要求するかは必ずしも明確ではない。

DORA は強力な規制上の推進力（20 以上の金融事業体カテゴリーをカバー）を提供するが、具体的な PQC 移行計画を促すためには、さらなるガイダンスや監督上の圧力が必要であるとの認識がある。一部の専門家は、量子耐性への移行を政策目標として「より明確化」するため、EU レベルでの追加文書やロードマップの策定を求めている。とはいえ、EU が暗号技術適応性要件を法的に組み込んだことは極めて重要な一歩だ。これにより EU の金融規制当局は、レジリエンスの一環として PQC 移行を強制できる。

英国：英国の PQC 移行への取り組みは積極的だが、現時点では具体的な新法ではなくガイダンスと業界連携に依存している。金融行動監視機構（FCA）は、サイバーセキュリティと業務継続性に関する広範な権限の下で量子セキュリティを扱い、企業が管理すべき新たなリスクの一つと位置付けている。PQC 専用の新法は存在せず、量子リスクは企業がサイバーインシデントや暗号解読の試みに耐えるよう求める既存の規制要件に含まれる。実際、英国規制当局は業界や国際団体と緊密に連携し、一貫性のある移行戦略を構築している。FCA

[19] 量子暗号に関する NIS グループ報告書で定義されているように、暗号の敏捷性とは、「暗号コンポーネントの交換を可能にする、モジュール化された暗号プロトコルおよびシステムの設計」を指す。

と世界経済フォーラムが共同で発表した 2024 年白書『金融セクターのための量子セキュリティ：グローバルな規制アプローチへの示唆』は、国際協調の必要性を強調している。この協力体制は、量子脅威への対応には業界と規制当局の緊密な連携、および管轄区域を超えた協調的アプローチが不可欠であるという英国の立場を浮き彫りにしている。

PQC の導入に関する英国のスケジュールは、国内および国際的な目標との整合性の観点から議論されている。量子安全計画の開発目標として、英国は 2028 年という目標を掲げており、EU の 2026 年という目標[20]と比べると野心的ではないように見えるが、2030/31 年頃の最終目標はほぼ同じである。 FCA と他の規制当局を統合する英国のデジタル規制協力フォーラムは、セクター間の暗号標準を調整する場を提供している。本質的に、英国は金融規制当局、国家安全保障局、業界団体が効果的に協力することを確保している。例えば、イングランド銀行は G7 ワーキンググループに参加しており、UK Finance はその議題に量子リスクを掲げている。

英国は、PQC に関する拘束力のある規則をまだ発行していないが、監督当局の姿勢は明確である。企業は、量子脆弱性をサイバーリスクマネジメントの一要素として扱い、暗号解読によって可能になったものを含むサイバーインシデントを克服すべきである。企業は、規制による強制を待つのではなく、今すぐ「後悔のない」措置（暗号監査、在庫管理、アップグレードなど）を講じることを期待されている。 したがって、英国の規制環境は早期関与、ガイダンス提供、国際協力が特徴だ。標準が成熟すればより明確なガイダンスが示され、金融セクター向けの具体的な助言は他国より「早期」に発表されると予想される。とはいえ、英国規制当局は既に PQC に関する国際的な原則策定に積極的に参加している。

米国：米国では、金融セクターにおける暗号の俊敏性と PQC 導入の推進は、連邦政府の指令と業界主導の取り組みの両方によって推進されている。NIST は 2024 年 8 月に最初の PQC アルゴリズム（FIPS 203、204、205）を確定し、これらは今後暗号標準の基盤となる。 これと並行して、NIST の NCCoE は NIST 特別刊行物 1800-38B を発行した。これは金融機関向けの実践的な移行ガイダンスを提供し、暗号資産の棚卸し方法や業界固有のユースケースを含む。この取り組みは金融関係者を直接関与させ、銀行や市場インフラに暗号資産適応のための運用上の青写真を提供する。 連邦レベルでは、2022 年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、NIST 標準の公開後速やかな採用を各機関に義務付け、ICT システム調達機関に対し耐量子移行の準備を強制している。 大統領令 14144 号及び 14306 号は政府システム全体での PQC 対応製品展開期限を設定し、さらなる強化を図る。主に公共セクター向けだが、ベンダー依存や重要インフラ連携を通じて金融業界にも影響を及ぼす。 通貨監督庁（p21）や連邦準備制度理事会などの金融規制当局は、既に業務継続性枠組み内で量子リスクに言及している。財務省は金融セクターサイバーセキュリティフレームワークを通じ、 の量子脅威をガイダンスに統合した。連邦金融機関検査協議会は、監督資料に量子レジリエンスの考慮事項を組み込み始めている。

業界側では、金融サービス - 情報共有・分析センター（FS-ISAC）などの組織が主導的役割を担っている。2024 年 10 月、FS-ISAC の PQC ワーキンググループは『金融セクターにおける暗号技術アジリティ構築』を発表した。これは企業が協調的に暗号アジリティを達成するための包括的な青写真である。米国金融規制当局もこの協調的かつアジリティ重視のアプローチを支持している。FFIEC はハンドブックに量子リスク考慮事項を追加し、財務省の金融セクターサイバーセキュリティ枠組みは暗号技術インベントリとアップグレード計画を強調してい

[20] このマイルストーンは、ドイツ連邦情報セキュリティ庁（BSI）が以前に提案した、量子暗号に関する NIS 協力グループによって提示されたものである。これは、政策に刻まれた公式のロードマップではない。

る。さらに、量子コンピューティング対策サイバーセキュリティ準備法の一部など、立法化が進められており、重要な金融インフラの量子耐性化に向けた官民連携が継続されることが保証されている。これらの取り組みは、2023 年 3 月の米国国家サイバーセキュリティ戦略と整合しており、同戦略では PQC を政府及び重要民間インフラ双方の優先課題としている。

全体として、米国の規制環境はトップダウン要件（連邦機関および間接的にその契約業者、一部の金融市場インフラを含む）とボトムアップの業界枠組みを組み合わせている。これにより、暗号資産の強制的な棚卸し、リスクアセスメント、移行プレイブックの開発といった準備段階が生まれている。証券取引委員会や FFIEC を通じた銀行監督機関などの金融セクター規制当局は、まだ PQC に特化した規則を発行していないが、既存の安全性・健全性に関する義務に依拠する可能性が高い。当局は、銀行が NIST 標準や FS-ISAC のベストプラクティスが利用可能になり次第、それらに従うことを期待している。要するに、米国当局はガイドラインを更新し、ポスト量子暗号のためのエコシステムを育成することで、政策と実践を整合させているのである。

4. 金融セクターにおける耐量子暗号への移行モデル

耐量子暗号への移行は、複雑で数年を要するプロセスとなる。この移行を管理するための主要な戦略には、暗号技術の俊敏性を高めること、徹底的なリスクアセスメントを実施して対応策の優先順位を決定すること、金融セクターにおける先行事例（パイロットプロジェクトや実験）から学び、より広範な展開に活かすことが含まれる。

専門家は、アルゴリズムの一括置換ではなく、暗号適応性アプローチを提唱している。これは、最小限の混乱で暗号アルゴリズムやプロトコルを迅速に変更する能力を構築する手法だ。これにより、旧式アルゴリズムのセキュリティ脆弱性を回避できる。例えば、アプリケーションはコードの大幅な変更ではなく設定変更でアルゴリズムを変更できる暗号化をサポートすべきであり、プロトコルは当事者間で利用可能な最強の標準アルゴリズムを使用するよう交渉されるべきだ。アジリティは移行期間中の相互運用性維持も意味し、これは必須とされる。BIS の Project Leap 報告書は、ハイブリッド方式（従来型と量子耐性アルゴリズムの併用）が「移行段階での相互運用性維持」に不可欠だと指摘。片側が完全移行していなくてもコミュニケーションの安全性を確保するためだ。

暗号の俊敏性を実現するには、組織はいくつかの実践的措置を講じるべきだ。ガバナンス体制が重要であり、企業は PQC 移行運営委員会またはタスクフォースを設置すべきである。この組織は暗号使用状況の棚卸し、標準追跡、事業優先度と規制要件に沿った移行スケジュール設定を監督する。多くの大手銀行は既にこの目的で内部の「量子リスク」または「暗号俊敏性」チームを編成している。次に、HSM（ハードウェアセキュリティモジュール）、暗号ライブラリ、VPN アプライアンスなどの基盤インフラをアップグレードし、新アルゴリズムに対応させる必要がある。重要な推奨事項として、広範な近代化計画の一環としてアルゴリズムの刷新が挙げられる。例えば、銀行がサービスをクラウド移行したり基幹銀行システムを刷新したりする場合、暗号アジリティの考慮事項を最初から組み込むべきだ。これと並行して、IT チームやセキュリティチーム向けのワークショップを通じ、量子コンピューティングと暗号技術の基礎知識に関する研修を従業員に提供する必要がある。このスキルアップにより、従業員が新たな暗号ソリューションを効果的に導入・維持できるようになる。最後に、ベンダーやパートナーとの連携が極めて重要だ。企業は早期にベンダーと協議し、ロードマップに PQC（ポスト量子暗号）対応が含まれるよう確保すべきである。つまり、新規調達において設計段階からの暗号アジリティを要求するのだ。

移行の規模を考慮すると、全てを一度に変更することは不可能だ。どのシステムとデータを優先的に保護すべきかを判断するには、リスクベースのアプローチが不可欠である。このプロセスは暗号資産の棚卸しから始まる。金融機関は、アルゴリズム、鍵長、証明書、それらの使用場所や方法を含む全ての暗号資産をカタログ化すべきだ。

棚卸しでは、長期にわたる機密保持要件を持つ資産（例えば 10 年以上秘密に保つ必要があるデータ）も識別しなければならない。 実際、こうした資産は「収集は今すぐ、復号は後で」という攻撃に対してより高いリスクに晒されている。このインベントリを活用し、各資産の量子脆弱性を推定できる。タスクフォースで提示された手法の一つは、 の量子コンピューティング進捗予測に基づき、特定期間内に資産の暗号化が破られる確率を算出する方法だ。このタイムラインを決定するには、モスカの定理を適用することが有用である[21] 。

重要なのは、リスクアセスメントにおいて暗号の強さと事業への影響の両方を考慮することだ。全てのシステムが同等のリスクを抱えているわけではない。優先的に PQC を導入すべき重要システムを特定する必要がある。決済システムや銀行間認証を支える PKI など、影響度が高くセキュリティ寿命が長い資産は早期に移行すべきだ。一方、機密性が低いデータやプロセス、短期的な機密性が必要なものは後回しにできる。 このプロセスを導くための複数の枠組みが登場している。オランダの PQC 移行ハンドブックやオランダ応用科学研究機構の研究では、アルゴリズムの量子脆弱性スコア、各種データの影響レベル、移行に必要な労力を組み合わせた構造化されたリスクモデルが導入されている。同様に、ECB は「*5* つの領域」からなるリスクと準備状況の枠組みを開発した：(1) 知識（脅威認識、技術的専門性）、(2) 計画（労力見積もりとロードマップ）、(3) 発見（暗号技術の使用事例の棚卸し、リスクに晒されるデータ）；(4) サードパーティ（ベンダーと法的考慮事項）；(5) リスクマネジメント（リスク登録簿の更新と緩和の優先順位付け） 各領域には成熟度レベルが設定され、機構の進捗を評価する。こうしたモデルを用いることで、企業は現状の位置付けを把握し、対処すべき課題を特定できる。例えば銀行が「発見」領域の脆弱性（包括的な暗号技術インベントリ未整備）を認識した場合、それは短期的な対応課題となる。

リスクマネジメントの別の側面は、緩和策の費用対効果分析である。解決策は全て同等ではない。ハードウェア変更を伴うもの（ハードウェアのハイブリッドソリューション採用、QRNG や QKD リンクの展開）もあれば、純粋にソフトウェアベースのもの（PQC アルゴリズムへの切り替え）もある。

大手銀行における暗号技術の完全移行には数億ドル規模の費用がかかるという報告がある。取締役会や経営陣にとって、リスク低減効果に対する支出を正当化するには、定量化されたリスクアセスメントが不可欠だ。何もしない場合のコスト（将来の侵害による罰金、損失、評判毀損の可能性）が移行コストを上回る場合、PQC 投資のビジネスケースは明らかになる。 規制当局もこうした分析に関心を持っている。世界経済フォーラム（WEF）と英国金融行動監視機構（FCA）のロードマップは、規制当局に対し「量子リスクへの異なるアプローチの費用便益分析を実施し、それに基づいて決定を下す」よう促している。

リスク主導の優先順位付けとは、どの暗号化エクスポージャーを最初に対処すべきかを識別し、アップグレードのタイムライン（多くの場合複数段階）を策定し、リソースが効率的に配分されることを保証することを意味する。このアプローチにより段階的な移行が可能となり、早期に迅速な成果（例：新標準をサポートするソフトウェアのアルゴリズム交換）を達成できる。 一方、より複雑な変更（例：新しい鍵サイズに対応できないレガシーシステムの置換やリファクタリング）は、十分なリードタイムを置いて計画される。

金融セクターは全体として、IT プロセスのアップグレードを目的とした広範な戦略の一環として、暗号素材のリスク主導型優先順位付けに注力すべきだ。移行コストは非常に高額になり得るため、経営幹部層の関与が不可欠

[21] モスカのアプローチは、機密データの残存寿命、量子コンピュータが現在の暗号を破るまでに予想される時間、PQC への移行に必要な時間を考慮している。データの必要な秘密保持期間と移行時間の合計が、推定される量子による「破られる」日付を超える場合、即座の行動が必要とされる。

である。具体的な移行チームやタスクフォースを設置し、何もしないことのリスク（将来の侵害による潜在的な罰金、損失、評判の毀損など）を提示する必要がある。

5. 金融セクターにおける取り組み

PQC 移行の抽象的な性質は、いくつかの先駆的なプロジェクトや協力関係によって具体化されつつある。これらの事例研究は、実践的な移行方法と進捗状況に関する知見を提供する：

- **中央銀行の実験**：複数の中央銀行が量子耐性技術の実証実験を実施している。BIS イノベーションハブがフランス銀行とドイツ連邦銀行と共同で主導するプロジェクト・リープは、銀行間接続向けの量子耐性 VPN を実証した。 2023 年、プロジェクト・リープの第 1 段階では、パリとフランクフルト間で ISO 20022 決済メッセージを伝送するため、ハイブリッド暗号（従来の RSA と NIST PQC アルゴリズムの組み合わせ）で保護されたサイト間 IPsec トンネルを確立した。本プロジェクトでは、暗号の俊敏性（VPN 内でのアルゴリズム交換能力）、性能への影響、統合上の課題を評価した。 本プロジェクトは、新プロトコルへの移行には暗号プロトコル一式を事前に変更する必要があることを実証した。また、耐量子暗号の専門家が不足しているといった運用上の課題も浮き彫りにした。BIS は当該分野の専門技能を持つ人材不足を指摘し、特別にチームを訓練する必要があった。プロジェクト第 2 段階では、より多くのネットワークアーキテクチャの検討と、決済バリューチェーンの追加層の組み込みが計画されている。 並行して、イスラエルやカナダなどの中央銀行はワークショップを開催し推奨事項を行った。2024 年 G7 議長国であるイタリア銀行は「量子耐性金融システムの構築：当局と民間セクターの役割は？」と題する会議を主催した。成果の一つとして、各国間で早期計画と量子レジリエンスに関する共通ロードマップを策定するよう求める G7 声明が発表された。 こうしたトップダウンの推進により、各国中央銀行はリアルタイムグロス決済ネットワーク（ECB の TARGET サービスなど）といった 重要システム向けの移行計画策定を迫られている。実際、ECB は既にユーロシステムインフラ向けの「内部移行ロードマップ」策定のため、自身と主要各国中央銀行で構成される専門タスクフォースを設置済みだ。

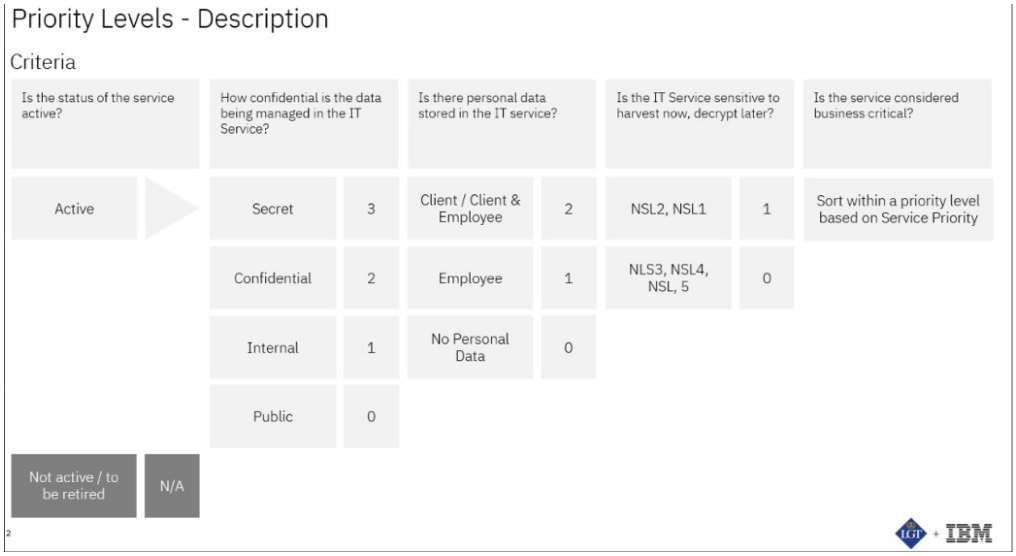
- 民間セクターでは、サンタンデール銀行や LGT などの銀行が先行している。サンタンデール銀行は量子セキュリティ専門チームを擁し、PQC と QKD を組み合わせた業界パイロットに参加している。2023 年には MadridQCI と共同で、安全なコミュニケーションのためのハイブリッド PQC-QKD ネットワークの試験を実施した。 この構成では、ソフトウェア定義ネットワーク（SD-WAN）が IPsec ルーターに鍵を配信し、従来の事前共有鍵と QKD で配信された鍵（ETSI TS 103 744 標準に準拠）を組み合わせて VPN トンネルを確立した。 この試験では、マルチベンダーの QKD ソース（Cisco、QoolNet、ID Quantique デバイス、Luxquanta）を使用しても、このようなハイブリッド IPsec が実現可能であることが確認された。 サンタンデールのパイロット試験から得られた結論は有望である：ソフトウェア定義ネットワークに基づく鍵管理アプローチは、大規模な IPsec ネットワークにおいて早期の量子耐性を実現し、異なる鍵交換メカニズム間の相互運用性を可能にする。これは暗号の俊敏性とハイブリッド暗号の実用的な実証であり、完全な PQC 標準が確定する前であっても、ネットワークを量子耐性化できる（つまり二重アルゴリズムや追加の QKD 層による）ことを示唆している。

  同様に、LGT プライベートバンク（リヒテンシュタイン）も量子安全コミュニケーションの実験を行っていると報じられている。例えばデータセンター間で QKD リンクを使用しているが、詳細は乏しい。プライベートバンキングや資産運用会社がこうした技術を模索している事実は、顧客の機密性への懸念がこれらの技術の早期導入を推進していることを示唆している。 量子暗号への彼らのアプローチにおける顕著な要素は、質問票

を用いた資料の階層的優先順位付けの精緻化であった（この手法は IBM と共同で開発された、図 4 参照）。

- 業界コンソーシアムとフォーラム：共同イニシアチブが移行の指針となっている。FS-ISAC の耐量子ワーキンググループはガイダンスを作成し、世界中の銀行間での情報共有を促進している。もう一つは欧州刑事警察機構の監督下で活動する量子安全金融フォーラムだ。業界主導で運営されるこのフォーラムは、セクター横断的な脅威情報の共有とベンダーへの共同圧力を推進している。同フォーラムは、コアバンキングソフトウェア、ATM ハードウェア、クラウドサービスなどのベンダーが、製品ロードマップで PQC を優先させるには金融業界からの明確な要求が必要だと認識している。標準の面では、ETSI や ISO などの組織が活動している。スタートアップ、学術機関、銀行業界を含む 9 組織のコンソーシアムは、CryptQ プロジェクトの下で、デンマークのダンスケ銀行の 2 データセンター間における量子通信二点間ネットワーク（ ）を開発した。デンマーク工科大学は、コンサルティング会社 KPMG の資金援助と技術支援を得て、標準化された通信用光ファイバー上で安全な暗号鍵を生成・共有した。これは、この技術が他の重要インフラにどのように実装できるかを示している。本プロジェクトは、Horizon 2020 イニシアチブに基づき、OPENQKD 公募（EU 資金）およびデンマークの CryptQ プロジェクト（デンマーク革新基金による 2250 万デンマーククローネの投資）の資金提供を受けて構築された。

図 4. LGT の暗号優先度レベル



出典：ETSI 会議スライド、2025 年

これらの取り組みは、多くの金融機関が PQC 移行において概念実証（PoC）または初期展開ステージにあることを示唆している。広く展開された量子耐性のある銀行間ネットワークはまだ存在しないが、構成要素（PQC アルゴリズム、ハイブリッドプロトコル、ハードウェアにおけるベンダーサポート）は急速に具体化しつつある。規制当局はこれらのパイロット事業を注視している。例えばシンガポール金融管理局は 2024 年、量子技術のサイバーセキュリティリスクに関する勧告を発表した。イングランド銀行などと共に国際的な量子リスク議論に参加し、プロジェクト・リープやサンタンデールの試験など個々のプロジェクトの知見がグローバルなアプローチに反映されるよう確保している。したがって、移行の「方法」はこれらの継続的取り組みを通じて洗練されている。具体的には、既存プロトコルへの PQC アルゴリズムの組み込み、長期移行期間中のリスク緩和のための古典的・量子ハイブリッド手法の採用、さらに次世代手法（例：サンタンデールの PQC・QKD ネットワーク）の開発、そして フォーラムを

通じた調整である。これにより、最終的に金融セクター全体が耐量子暗号への切り替え時期に足並みを揃えて移行できるようになるのだ。

6. 金融セクターにおける PQC 移行のボトルネック

勢いが増しているにもかかわらず、金融セクターの PQC 移行を遅らせている重大な障害が存在する。これらのボトルネックは技術的、組織的、インフラストラクチャ的なものであり、進展を加速させるためには対処が必要だ。

- 技術的課題：主要な技術的障壁は、新暗号アルゴリズムをレガシーシステムに統合することだ。金融 IT 環境にはレガシープロトコルやハードコード化された暗号技術が蔓延している。例えば多くの VPN やセキュアメッセージングシステムは鍵交換に RSA や ECC を前提としており、格子ベースの鍵交換メカニズム（KEM）へアップグレードするには新たなプロトコル拡張、メッセージフォーマット、エラー処理ロジックが必要となる。アップグレード済みと未アップグレードの事業体間の相互運用性を確保することも問題を複雑化させる。 性能も懸念事項だ：PQC アルゴリズムは一般的に鍵サイズや署名サイズが大きく、格子ベース方式など処理速度が遅いものもある。高スループット取引システムや低遅延決済スイッチでは、こうした性能低下を慎重にベンチマークする必要がある。初期テストでは、PQC ハンドシェイクがセッション設定に数秒の遅延を生むことが示されている。用途によっては許容範囲だが、他の用途では問題となる可能性がある。 PQC の性能と安定性のためにシステムを調整するのは容易ではない。 アルゴリズムの不確実性も問題だ。NIST が初期標準（CRYSTALS-Kyber、Dilithium など）を選定した一方で、追加アルゴリズム（署名用や FIPS 140-3 準拠などの特定ユースケース向け）は依然評価中である。標準が完全に確定する前（ステートフルハッシュ署名や将来のラウンドアルゴリズムを含む）に一組のアルゴリズムを展開することに、誤った選択を恐れて躊躇する企業もある。 イタリア銀行の報告書が指摘したように、標準とロードマップに関する普遍的な合意が欠如しているため、移行計画の設計は困難だ。この分断リスクにより、技術チームは複数の PQC オプションを実装するか、アルゴリズムが後に脆弱と判明した場合（NIST 第 3 ラウンド候補の一部で起きたように）に方向転換する準備が必要となる。これらの課題はすべて、移行の複雑さとコストを増大させる。

- 組織的・技術的ギャップ：金融機関は全レベルで暗号技術のスキルと認識が不足している。暗号技術は従来 IT 分野のニッチ領域だったが、今や主流の関心事とならねばならない。多くの金融機関では暗号技術を静的なユーティリティとして扱う文化が根付いている。この考え方を継続的な暗号技術の改善へと転換することが組織的課題だ。 が示す認識のギャップでは、取締役会や経営陣が差し迫った懸念事項の中で量子リスクを優先順位付けできていない可能性がある。 経営陣の認識がなければ、PQC プロジェクトの予算とリソースは限られる。一方で認識が高まると新たな課題が生じる：取り組みの過大評価や誤った配分だ。調整不足のイニシアチブが乱立すれば（各事業部門が独自に動く）、重複や不整合なアプローチを招く恐れがある。企業内での統一戦略の必要性は極めて重要だ（そのため運営委員会などの内部ガバナンスが求められる）。 暗号在庫管理プロセス自体が組織的な煩雑さを伴う。部門横断的な協力や外部組織（ソフトウェア・ハードウェアプロバイダなど、後述参照）との連携が必要となるためだ。大規模銀行における暗号技術の全用途発見は、数か月を要する監査に匹敵する。多くの銀行には数万のアプリケーションが存在し、これらを暗号依存関係でスキャンする作業は膨大な調整努力を要する。 限られた熟練人材、競合する優先事項、部門横断的な協力の必要性が、人的側面での移行を遅らせている。

- インフラとベンダー依存性：金融セクターの暗号インフラは単一機構の枠を超えている。ベンダー、サードパーティサービスプロバイダー、ハードウェア製造事業者を含む。主要なボトルネックは、技術プロバイダの PQC

対応準備状況だ。金融機関は、ベンダー（コアバンキングソフトウェア、HSM デバイス、ネットワーク機器、クラウドプラットフォームなど）が互換性のある認証済みソリューションを提供するまで、特定システムのアップグレードができないと報告している。IT 業界と金融業界のタイムラインが一致しない場合、業界は信頼性に欠ける技術を採用するか、移行を遅らせるかの選択を迫られるリスクに直面する。これがベンダーへの圧力となる理由だ。例えば米国政府機関は IT ベンダーに対し PQC 導入を期待しており、市場全体を前進させる効果的な後押しとなっている。しかし全てのベンダーが同等の速度で動いているわけではない。小規模ベンダーやニッチなソフトウェアプロバイダは、顧客が要求するまでリソースやインセンティブが不足している可能性がある。認証とコンプライアンスの問題もある。銀行はカード向けに FIPS 認証暗号や EMV 標準を要求するが、これらの標準化団体は PQC 対応仕様の更新を継続中であり、これがベンダーの実装遅延につながっている。もう一つのインフラ上のボトルネックはデバイスの制限だ。使用中の HSM やスマートカードチップの中には、固定アルゴリズムサポート（RSA/ECC のみなど）や、より大きな PQC 鍵に対応する処理能力・メモリが限られているものがある。こうしたセキュアエレメント（ATM ネットワーク、決済カード、モバイルセキュアエレメントなどに数百万台存在する）の交換やアップグレードは、膨大な物流作業を伴う。決済システムでは、EMV や ISO 8583 といったプロトコルさえも PQC 対応のため改訂が必要であり、これは世界的な調整を要する。標準とインフラが追いつくまで、多くの機構は互換性不足を恐れ、率先して移行することを躊躇している。これが、異なる市場間の規制の分断（管轄区域間の不整合リスク）が重大な懸念事項である理由だ。このボトルネックを解消するには、ISO や G7 などの組織で進行中の標準化作業が不可欠だ。遅いが、必要な作業である。

- 移行のコストと複雑性：上記すべてに共通するのは、移行そのものの膨大なコストと複雑性であり、これ自体がボトルネックとなり得る。移行には金銭的負担だけでなく業務への影響も伴う。義務付けられていないか、収益に明確に結びつかない限り、リスクが差し迫るまでは内部でこの支出を正当化するのは難しい。さらに、一部の IT プロジェクトとは異なり、暗号技術移行には即時のビジネス上のメリットがない（顧客は新機能を見ない。これは下振れリスクの低減が目的である）。そのため、しばしば先送りされる。複雑さは計画立案も困難にする。機構は下位互換性、現在暗号化されているデータ（アーカイブの再暗号化方法？）、取引相手との調整を考慮しなければならない。例えば、署名付きメッセージを定期的に交換する 2 行は、新たな署名アルゴリズムへ同期して移行する必要がある。実際、この業界では過去に暗号技術移行（3DES から AES、SHA-1 から SHA-256、RSA-1024 から RSA-2048 など）を経験しており、その都度前回より複雑で時間のかかる作業となっている。これは終わりのないサイクルであり、持続不可能になりつつある。だからこそ、今や異なるアプローチ（アジリティ）が必要だ。しかし、そのアジリティを実現すること自体が複雑である。大幅なリエンジニアリングを必要とする。ガートナーの「5 つの R」（Rehost、Refactor、Revise、Rebuild、Replace）は、新しい暗号化を容易に扱えないレガシーアプリケーションに対処する戦略としてよく引用される。これらの戦略をケースバイケースで選択・実行すること（古い決済プラットフォームを完全に置き換えるべきか、それとも暗号通貨対応の API を使用するためにリファクタリングできるか？）は詳細な作業であり、一部の組織では分析麻痺を引き起こしている。

第 IX 部：公共セクターにおける量子耐性への移行

1. 序論

本章では、公共セクターにおける PKI（公開鍵基盤）とデジタル ID システムの PQC（耐量子暗号）への移行を検討する。PKI はデジタル信頼の基盤を形成し、政府サービス全体での安全な認証とコミュニケーションを可能にする。しかし量子コンピューティングの出現は、これらのシステムが依存する古典暗号アルゴリズムを脅威に晒し、量子耐性のある代替手段への協調的な移行を必要としている。

公共セクターの PQC 移行には、広範な認証システムのアップグレードに伴う技術的複雑性、相互依存する関係者間の組織的適応、標準化とガバナンスにおける機構的分断といった、異なるボトルネックが存在する。 この特定分野における 移行は、単なる技術的問題ではない。アルゴリズム選択（ハッシュベース、格子ベース、ハイブリッド）にはそれぞれトレードオフが存在するが、より広範な課題は、認証局から失効システム、ハードウェアモジュールに至る信頼エコシステム全体の適応にある。EU デジタル ID ウォレットの事例は、その可能性とリスクの両方を示している。当初から PQC を統合しなければ、欧州は陳腐化した暗号技術に自らを閉じ込めるリスクがある。

こうした状況を踏まえ、本タスクフォースは以下の優先行動を推奨事項する：

- PKI およびデジタル ID システム向けの段階的移行計画を実施する
- 認証層を同期化し、分断化とサービス中断を防ぐこと
- 国境を越えたロードマップを調整し、各国の移民戦略を整合させる
- 量子安全性をデジタル ID に最初から統合する
- 量子移行を社会技術プログラムとして調整管理する。

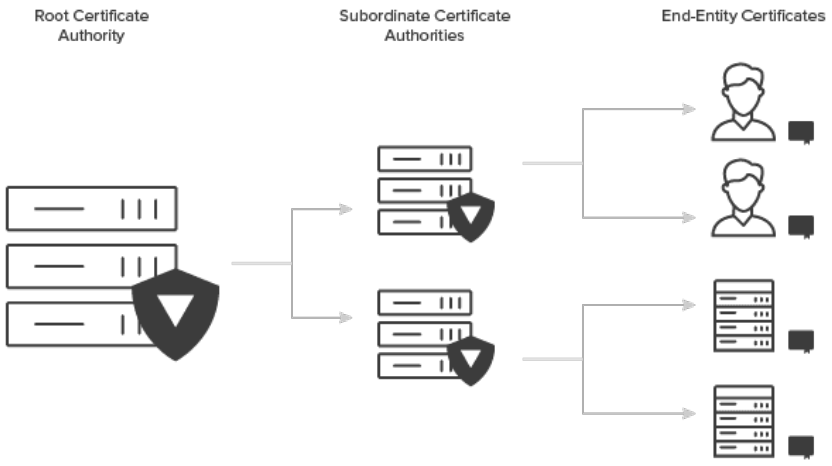
2. 公共セクターにおける PQC への移行

PKI は現代行政におけるデジタル信頼の基盤である。PKI は、個人・組織・サービス・デバイスがオンライン上で身元を証明できるよう、デジタル証明書を発行・管理するガバナンスおよび技術的枠組みだ。公開鍵と秘密鍵の発行・管理・妥当性確認を行う枠組みを提供し、デジタルコミュニケーション・サービス・身元の認証と検証を保証する。

PKI は通常階層構造を取る（図 5）。少数の防御された「ルート」認証局が信頼の基盤となる。これらのルートは特定の領域（省庁、部門、セクターなど）において、自身に代わって活動する「中間」認証局を認可する。これらの中間認証局は（通常）「エンド事業体」である個人、サーバー、アプリ、デバイスに対して実際の証明書を発行する。 したがって PKI は信頼の連鎖に依存している。ルート認証局が信頼の基盤となり、中間認証局が特定の領域や部門に信頼を分配し、エンドエンティティ証明書がユーザー、組織、デバイスに発行される。この階

層型アーキテクチャは、安全な電子メール、政府システムの認証、行政手続きで使用されるデジタル署名といった重要サービスを支えている。

図 5. PKI インフラストラクチャ



出典: https://www.keyfactor.com/education-center/what-is-pki/

証明書は、情報が正しい相手と交換され、傍受や改ざんから防御されることを保証することで、当事者間の安全なコミュニケーションを支える。証明書には定義されたライフサイクルがあり、ルート認証局では通常 10 年、中間認証局では数年、エンド事業体ではより短い期間が設定される。セキュリティと信頼性を維持するためには、継続的な更新、失効、監視が必要だ。

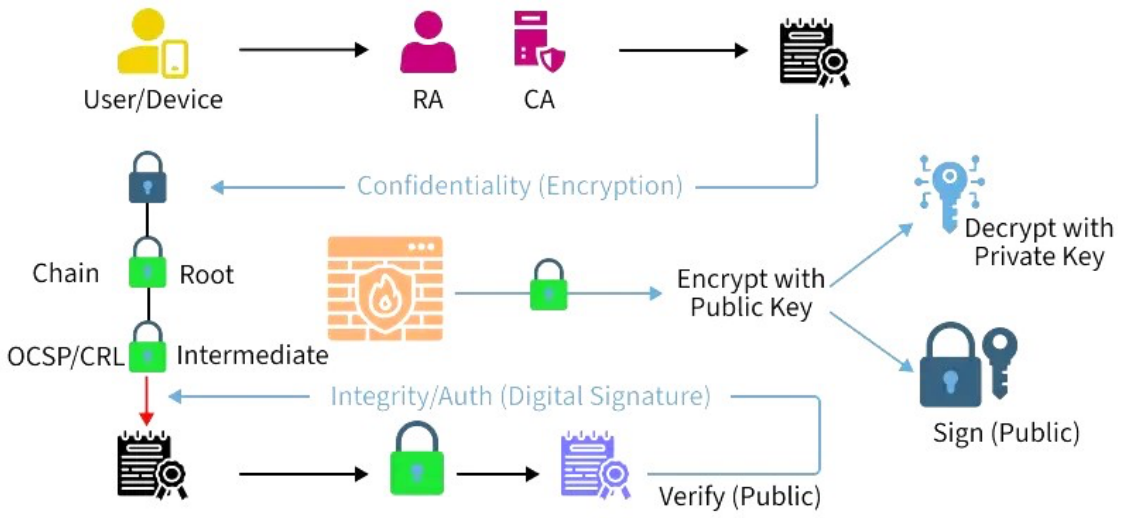
しかし量子コンピューティングの出現は、この信頼モデルの基盤そのものに挑戦を突きつけている。現行の PKI は、コミュニケーションの保護やデジタル署名による真正性の保証に、RSA や楕円曲線暗号といった古典的な公開鍵アルゴリズムに依存している。大規模な量子コンピューターが実用化されれば、これらのアルゴリズムは効率的に破られ、暗号化と認証の両メカニズムが損なわれる可能性がある。

これに対応するため、PQC（耐量子暗号）への移行に向けた取り組みは既に始まっているが、インターネットセキュリティの各層で進捗状況は異なる。コミュニケーションの秘密性を一時的で認証不要な鍵交換によって保護する機密性層が最も急速に進展している。2014 年から 2016 年にかけて、Google、Mozilla、Cloudflare、Fastly、Akamai といった主要プレイヤーが TLS におけるハイブリッド型耐量子鍵交換の試験運用を行い、現在では古典的アルゴリズムと量子耐性アルゴリズムを並行して動作させるハイブリッド方式を展開している。この進化は主に「今収集し、後で を復号する」という脅威によって推進されてきた。経験的証拠によれば、古いデバイスやミドルボックスでの若干の遅延を除けば、ほとんどのユーザーにとってパフォーマンスへの影響は最小限に留まっている。

一方、エンドポイントの真正性と証明書の有効性を保証する認証機能（図 6）は依然として主要なボトルネックである。この非対称性は、複数主体による PKI 信頼基盤全体を移行するよりも、二者間の（一時的で認証

されていない）鍵交換をアップグレードする方が比較的容易であるという相対的な簡便性を反映している。ここでは、PQC への移行が証明書の階層構造全体とライフサイクル管理に影響を及ぼす。

図 6. PKI における機密性と認証



出典: https://www.geeksforgeeks.org/computer-networks/public-key-infrastructure/

この複雑性により、適切な耐量子アルゴリズムの選択は PKI 設計・展開において特に重大な意味を持つ。各候補アルゴリズム群は、性能・運用複雑性・セキュリティ保証のバランスが異なる。現在評価中の主要選択肢はこれらの対比を示している。

- SLH-DSA（ステートレスハッシュベース署名）：これらは十分に理解されたセキュリティ特性に基づいて構築されており、最も保守的で堅牢な選択肢の一つである。欠点は署名サイズが非常に大きく、証明書やチェーンを肥大化させ、帯域幅やストレージに負荷をかけることだ。

- 拡張マークル署名方式（XMSS）とレイトン・ミカリ署名（LMS）（ステートフルハッシュベース署名）：これらも確立されたセキュリティ仮定に基づく。署名と公開鍵を非常に小さく生成できる点が 、証明書サイズにとって魅力的だ。ただし状態管理が必要となる。これにより運用手順、バックアップ、復旧が複雑化する。

- ML-DSA + ECDSA（ハイブリッド）：格子ベース署名と従来方式を組み合わせることで「安全網」を提供する。一方の構成要素が安全であれば信頼は維持される。ハイブリッド方式では ECDH 部分がわずかなオーバーヘッドしか加えないため、署名と公開鍵のサイズも適度なまま保たれる。ただしエコシステム全体での採用・サポートは依然不透明だ。

- ML-DSA（純粋）：格子のみの使用は 2 つのアルゴリズム管理の複雑さを回避し、ソフトウェア・ハードウェアプラットフォーム全体での広範な採用が見込まれる。署名と鍵のサイズは中程度で、多くの展開で実用的な規模だ。とはいえ、構造化された格子仮定への依存は、長期的な信頼性という点で未解決の問題として残る。IETF は RFC 9881 を公開し、X.509 PKI 環境における ML-DSA のアルゴリズム識別子を

規定した。この進展は、ML-DSA-44/ML-DSA-65/ML-DSA-87 パラメータセットが証明書構造にマッピングされる方法を形式化したものであり、純粋な ML-DSA 変種のエコシステム対応に向けた重要な一歩となる。 とはいえ、展開の成熟度、ベンダーサポート、構造化格子仮定への長期的な信頼性に関する疑問が自動的に解消されるわけではない。

全体として、欧州当局や BSI などの国家機関はハイブリッド証明書の積極的な推進を行っている。ステートフルな LMS/XMSS などのハッシュベース署名技術は、保守的なセキュリティ基盤とコンパクトなサイズから信頼アンカー候補として提案されている。これらの推奨事項は、より広範な政策指針の一環として欧州委員会のチャネルに反映されつつある。 同時に、XMSS や LMS といったステートフル方式の脆弱性への懸念も浮上している。各鍵は一度しか使用できないため、状態管理やバックアップ管理における運用ミスが致命的な障害を引き起こす可能性がある。各国当局はルートレベルでの管理には自信を示しつつも、ミスが発生しやすい中間証明書への適用義務化にはリスクを認めている。

しかし、この移行は信頼のエコシステム全体に影響を及ぼす。これには、証明書の妥当性確認に用いられる仕組み、新たな信頼アンカーを導入する手順、認証局の業務プロセス、そしてハードウェアセキュリティモジュールや証明書管理システムといった支援インフラが含まれる。 したがって、これはシステム的な取り組みであり、ルートおよび中間認証局、証明書透明性ログ運営者、失効およびオンライン証明書ステータスプロトコル（OCSP）対応、HSM ベンダー、 証明書ライフサイクル管理システム、アプリケーションレベルの検証者間の調整が必要だ。一貫した信頼の連鎖が機能するためには、これらの各関係者が同時に適応しなければならない。

国際電気通信連合電気通信標準化部門（ITU-T）X.509 などの標準規格により、耐量子証明書を処理可能な PKI ソフトウェアの利用が可能となった。しかしこの移行は、現時点では正式な法的義務ではなく、業界固有の調達要件として反映されているに過ぎない。 耐量子暗号は広く使われるソフトウェアライブラリ（例：Botan、BouncyCastle、OpenSSL）にも組み込まれつつある。相互運用性は IETF ハッカソンなどの国際イベントで検証され、実験的な PQ 証明書がシステム間で交換されている。

特筆すべきは、PQC 移行が PKI の潜在的な構造的弱点を再設計する機会でもある点だ。既にブラウザで大量にキャッシュされている中間証明書は、チェーン長とオーバーヘッド削減のために合理化または削除できる。 証明書ステータス確認におけるプライバシー上の欠点、例えばユーザーの閲覧パターンがサードパーティの CT や失効サービスに漏洩する問題は、プライバシー保護暗号を統合することで解決できる。具体的には、最近実用段階に達した非公開情報検索（PIR）、プライベート共通集合（PSI）、忘却 RAM（ORAM）の進歩を活用する。これらのプリミティブの多くは格子ベースであり、したがって PQC と互換性がある。これにより、ユーザーの行動を暴露せずに検証が可能となる。 このような強化策を移行プロセスに組み込むことで、PKI は現行形態よりもレジリエンス、効率性、ユーザー保護性に優れた形態へと進化し得る。

この移行の影響は、安全なコミュニケーションを超えて、PKI に依存する本人確認システムそのものにも及ぶ。デジタル ID インフラは、ユーザー認証、資格証明の妥当性確認、国境を越えた相互運用性を実現するため、PKI の信頼アーキテクチャを継承している。 したがって欧州のデジタル ID システムは、PKI ベースの信頼枠組み上に構築されている。資格情報は「誰が誰に何を発行したか」を証明する証明書チェーンを通じて発行・妥当性確認される。資格情報の範囲は、単純な身元主張（例：「保持者はジョン・ドウである」）から、より複雑な属性ベースの主張（例：「保持者は 18 歳以上である」または「加盟国 X の居住者である」）まで多岐にわたる。

デジタル ID システムの設計選択を左右する三つの特性がある：相互運用性（資格情報が異種システム・分野間で検証可能であること）、信頼性のある発行（暗号的健全性と適切な個人・組織への紐付け）、そして国境を越えた利用可能性だ。国境を越えた利用には、共有 API、調和された証明書プロファイル、信頼アンカーの相互承認が必要である。さもなければ、一国の脆弱または互換性のないスキームが他国で発行された資格情報への信頼を損なう。 したがって、調整されたタイムラインと相互に認められた耐量子ルーツは、国境を越えたアイデンティティの前提条件である。年齢や資格証明といったより高度なアイデンティティ応用（ ）は、プライバシー要件も導入する。ユーザーは必要な情報のみを開示すべきであり、これには選択的開示、非連結性、ゼロ知識証明といったプライバシー保護暗号ツールが求められる。これらの技術は PQC 形式で存在するが、従来のソリューションほど成熟しておらず効率的でもない。

デジタル身分証明システムにおいて、量子リスクは暗号機能によって異なる。暗号化では「即時収集・後解読」の脅威により、量子コンピュータが実用化されれば保存された暗号化データは全て侵害される可能性があるため、耐量子保護の緊急性が求められる。デジタル署名では、将来的な偽造による不正認証のリスクが存在するため、移行は依然として期日通りに行うべきである。

ボックス 3. EU デジタルウォレット事例

改正 eIDAS 枠組みの下では、全ての加盟国は少なくとも 1 つの欧州デジタル ID ウォレットを提供し、2026 年末までに認証と届出を完了しなければならない。ウォレットはオープンソースであること、欧州委員会が公表する共通アーキテクチャ参照とプロファイルを実装すること、認定適合性評価機関によるアセスメントを通過することが認められる条件だ。 欧州委員会は発行者向け信頼リストと依存者向け登録プロセスを維持し、市民が国境を越えて「発行元」と「要求元」の両方を検証できるようにする。このウォレットは検証可能クレデンシャル（個人識別データ、モバイル運転免許証、学歴記録、障害者手帳、社会保障受給資格、デジタル旅行証明書など）の汎用コンテナである。利点は、共通データとプロトコルプロファイルの簡素化・標準化、相互互換性に集約される。 複数の加盟国（イタリア、ポルトガル、ポーランド、フランス、オーストリア、ドイツなど）は、EU プロファイルとの完全な整合と認証待ちの状態ながら、ウォレット準拠に向けた国内アプリの開発を進めている。実証済みのユースケースには、決済時の強固な顧客認証、会場／空港チェックイン、ホテルチェックイン、近接型 ID 確認などが含まれる。

デジタル ID ウォレットの規定では、個人識別データと鍵の防御（保証レベル、HSM、セキュアエレメントによる）が義務付けられているが、重要な点として、ポスト量子暗号（PQ）の採用は義務化されていない。実際には、現行の展開では従来型アルゴリズムに依存し続けることを意味する。一方で、ハードウェアと保証枠組みは、標準と認証が成熟した段階で PQ またはハイブリッド方式を導入するための基盤を提供している。 こうした背景から、PQC 機能を持たないウォレットが導入され、2030 年代まで運用され続けるリスクがある。エコシステムの慣性と改修コストの高さから、欧州は事実上、時代遅れの暗号技術に縛られることになる。

このため、将来の「差し替え」として扱うのではなく、設計段階で PQC を考慮に入れる強い根拠がある。言い換えれば、欧州のデジタル ID ウォレットは PQ アルゴリズムを組み込むべきだ。先を見据えたアプローチには、暗号アルゴリズムとプロファイルの更新を円滑にする暗号対応インターフェース、PQ 対応のセキュアエレメントと HSM、エンドユーザー端末での検証性能を維持するフットプリントを意識した暗号選択が必要となる。 改訂された eIDAS 枠組みが欧州のデジタル ID とウォレットの法的基盤を提供する以上、その非連結性と越境信頼への重点は、耐量子要件に直接対応し得る。将来の量子攻撃者に対する非連結性の維持は、今日の設計段階での PQ 採用を正当化する。

この文脈において、欧州はアイデンティティ向けの共通 PQ デフォルト（例：伝送・認証署名用格子 KEM/署名ペア、信頼アンカー用ハッシュベース署名オプション）を定義し、共有 API・プロファイル仕様を公開し、調達と適合性試験を調整すべきだ。EU 団体による明確なガイダンス（例：市民向けサービス向けアルゴリズムスイートとプロファイル、

可能な限り統合して実装複雑性を低減）は断片化を最小化し実装リスクを低減する。より具体的かつ差し迫った行動としては、以下のことが挙げられる：ウォレットと認証情報のフォーマットを PQ ネイティブかつ暗号技術に柔軟に対応できる設計とする；ハイブリッド方式を採用する；KEM と署名の両方をカバーするアルゴリズムスイートを選択し、長寿命の信頼アンカーにはハッシュベースの署名を留保する；実機とネットワークでの性能測定を目的とした EU レベルのパイロットを実施する；プロファイル、API、保証に関する加盟国の整合を図るための規範的ガイダンスを公開する。これらの措置を今すぐ講じなければ、エコシステムの慣性により、2030 年の高リスク移行期限に間に合わないリスクがある。

3. 公共セクターにおける PQC 移行の技術的ボトルネック

本節では、公共セクターが PQC へ移行する際に直面する主な技術的ボトルネックを要約する。公共セクターの PQC 移行における最も差し迫った課題は、既存インフラの移行にある。主なリスクは、既存 PKI の規模と複雑さを考慮すると、複雑な認証システムを期限内に移行することが構造的に困難である点だ。行政機関にとってこのリスクは特に深刻である。何十万もの証明書と複数層の認証局を更新しなければならないからだ。

これに加え、機密性層は進歩したものの、認証層は重大なボトルネックである。認証はルート、中間、事業体からなる信頼構造全体に依存する。認証局が PQ 対応チェーンを発行しても、ブラウザに PQC 検証機能が欠ければ相互運用性は崩壊する。さらに、CT ログはより大きな証明書を処理する必要があり、失効システムはより高い計算負荷と帯域幅負荷を管理しなければならない。

前述の通り、もう一つの重要な技術的ボトルネックは、PQ アルゴリズムが重大な性能トレードオフをもたらす点だ。鍵サイズと署名サイズの拡大は、メッセージ長、検証時間、ストレージ要件の増加を招く。特に注目すべきは、これらの影響はエンドユーザーには軽微でも、大規模な ID システムでは累積する点だ。特に毎日数百万の認証情報や取引が処理される環境では顕著である。

Box 4. TLS 1.3 の事例

2018 年に IETF が発表した TLS 標準の最新バージョンである TLS 1.3 は、インターネット通信のプライバシーと完全性を保証する。同時に、耐量子時代における認証課題の深刻さを示している。鍵交換は単一のハイブリッドハンドシェイクで更新可能だが、認証はセッションごとに複数の署名と証明書妥当性確認に依存する。これにはハンドシェイク自体、チェーン内の各証明書、証明書透明性ログの妥当性確認が含まれる。 実際には、単一の TLS 接続で半ダースもの署名検証が行われることがある。

耐量子アルゴリズムは署名サイズと鍵サイズを大幅に増加させるため、特に制約のあるデバイスや脆弱なネットワークリンクにおいて、パケットの断片化、再送信、性能低下を引き起こす可能性がある。実証研究ではこうした影響が確認されているが、証明書チェーン全体にわたる包括的な測定は依然として限定的だ。

インターネット認証の大半は PKI 発行のデジタル証明書に依存しているが、他の手法も存在する。一部のプロトコルは PSK やパスワード認証を使用し、新興提案である KEM-TLS は暗号化と認証の両方に KEM を採用することで、大規模な耐量子署名の必要性を減らし効率を向上させる。 しかし、これらの代替手段を大規模に採用するには、インターネット基盤の再設計と、ブラウザ・サーバー・認証局間の相互運用性の確保が必要となる。結果として、これらの手法は代替ではなく補完と見なされており、耐量子セキュリティを実現するには既存 PKI の強化が依然として不可欠である。

重要なことに、IETF は鍵交換に関して既に具体的な措置を講じている。ワーキンググループは、古典的な ECDHE アルゴリズムとモジュール格子ベースの KEM を組み合わせたハイブリッドグループ（X25519MLKEM768 および SecP256r1MLKEM768）を規定するドラフトを公開した。

4. 社会技術的観点からの移行課題

耐量子 PKI への移行は、暗号技術上の課題であるだけでなく、社会技術的な変革全体を意味する。アルゴリズム、鍵サイズ、 、認証枠組みに多くの注目が集まる一方で、移行におけるより困難な部分は、技術的、組織的、社会的側面の整合にある。

暗号層での変化は、組織プロセス、規制枠組み、さらにはエンドユーザーの実践にまで必然的に波及する。農業の機械化との類推は示唆に富む：戦後カリフォルニアにおけるトマト収穫機の導入は、単なる技術的代替ではなく、コミュニティ全体、労働市場、そしてトマトそのものの形さえも再構築した。 同様に、PQC 移行は周辺エコシステムの再設計、認証団体の再構築、監査員の訓練、ベンダー供給網の適応、そしてハードウェア変更やレガシーシステム更新に消極的な事業者の説得を意味する。技術的課題は、信頼基盤の広範な再編成に内在しているのだ。

PKI を重要な社会インフラと認識したオランダの HAPKIDO コンソーシアムは、政府・銀行・通信などの分野横断的なリスクマッピング手法を開拓した。彼らの社会的リスクアセスメントは、量子脅威が領域ごとに異なる形で現れることを浮き彫りにしている。例えば、企業と政府間のデータ交換は中期的機密性を伴うことが多い一方、政府と市民間や政府間データフローははるかに長期的な防御期間を必要とする。 このアセスメントは組織に対し、狭いコンプライアンスを超え「量子攻撃でデジタルインフラが崩壊した場合の社会的影響は何か」と問うことを促す。組織準備度モデルと成長モデルに基づくロードマップは、内部議論を活性化し量子移行を包括的なセキュリティガバナンスに組み込む助けとなる。成長モデルは、初期の認知段階、暗号資産棚卸（「後悔しない措置」）を伴うアセスメント段階、完全適応段階を概説する。 重要なのは、各段階間の不連続性が示すポイントだ。そこでは、標準化の更新、ベンダー製品の可用性、規制上の義務といったエコシステムレベルの条件が満たされなければ、組織はそれ以上前進できない。これは移行が直線的ではなく、技術的修正と同様に政策とガバナンスの解決策を必要とする依存関係によって断続的であることを強調している。

PKI 移行の社会技術的複雑性は、何よりもまず複数主体間の相互依存性に起因する。証明書は信頼できるルートに遡及されねばならず、適合性評価団体は実装を妥当性確認し、ベンダーは更新された HSM と暗号ライブラリを提供し、規制当局は認証を行い、ユーザーは国境を越えて検証可能でなければならない。

こうした密接な相互依存関係は、耐量子標準のガバナンスにおける機構的分断によってさらに複雑化する。地域やセクターによって実装速度は異なり、標準団体・規制当局・ 産業コンソーシアム間の連携は依然として不均一だ。オープンソースコミュニティは既に Secure Socket Shell（SSH）などのプロトコルに PQ アルゴリズム（例：ML-KEM）を導入しており、正式な標準化経路外での採用が可能であることを示している。 この多様性はアルゴリズムの乱立と地域分断のリスクを孕む。異なる主体が互換性のないアルゴリズム群を導入すれば相互運用性が損なわれる。調整されたプロファイル、認証ガイドライン、機構横断的な政策整合性なしに、公共セクターは PQ PKI 展開において「バベルの塔」的状況に直面し、グローバルな信頼の継続性を脅かす恐れがある。加えて、標準団体が組織的ニーズに遅れを取る可能性が繰り返し懸念されている。

特に、eIDAS や欧州の ID ウォレットを支える多くの標準は、PQC に関して未対応のままである。組織がパイロット導入前に標準の浸透を待たねばならない場合、移行は段階的で長期化する。専門家は並行行動の必要性を強調する：標準団体に量子技術の影響をマッピングさせ、暗号プロファイルを早期更新し、ガイダンスが動的に進化するよう確保することだ。 全体として、これはエコシステム全体の調整、知識の共有リポジトリ、継続的な学習の必要性を強調している。重要なのは、あらゆるレベルのステークホルダー（政府、中小企業、監査人、市民）が関与できるよう、多言語リソース、共有用語集、平易な要約を確保することも含まれる。

PQC はまた、社会技術的観点から経路依存性に対処することを含む。実際、PQC においてはレガシー制約が特に深刻だ。多くの産業制御システム、決済端末、組み込み IoT デバイス、国家 ID インフラは、数十年前からハードウェアやファームウェアに実装された暗号プリミティブに依存している。 これらのコンポーネントの更新はコストがかかり、業務に支障をきたし、場合によってはインフラ全体を置き換えない限り技術的に不可能だ。鉄道の軌間との類推が参考になる：オーストラリアは今なお、1 世紀前に決定された互換性のない軌間幅に悩まされている。同様に、20 年前に決定された暗号設計の選択が、今や単純なアップグレードを阻んでいる。こうした動態は、重要インフラを支える運用技術（OT）において特に顕著だ。 エンタープライズ IT とは異なり、OT 環境では数十年前から使用されている機器、独自プロトコル、リソース制約のある組込みデバイスに依存している場合が多い。ここでは可用性が最優先事項であり、エネルギー、交通、医療などの分野では停止は許されない。PQ アルゴリズムは鍵サイズが大きく計算負荷が高いため、こうしたデバイスを容易に処理不能に陥らせる。したがって移行経路は、ゲートウェイの展開や管理されたメンテナンス期間内でのアップグレード計画から、ハードウェアの全面的な交換まで多岐にわたる。 レガシーな特注システムの場合、組織は（独自暗号開発のリスクを承知の上で）社内更新、プラットフォーム移行、あるいはサービスの完全廃止を迫られる可能性がある。これら全てが実行不可能な場合、リスク受容が唯一の選択肢となる。連鎖的な影響が事態をさらに複雑化する。スタックの一層で暗号アルゴリズムを置き換えると、他の部分で障害が発生する恐れがある。 TLS エンドポイントを PQC に移行した銀行は、組み込み決済端末との相互運用性が失われる可能性がある。PQC 証明書を義務付けた政府は、標準団体が調整するまで国境を越えた電子署名を混乱させるかもしれない。グローバルサプライチェーンはこれらのリスクを増幅させる：あるプロトコルや認証プロセスでの停滞は、スエズ運河の一時的な閉塞が欧州の自動車製造を混乱させたように、複数の産業に波及する。

こうした視点で見ると、PQC 移行は単なる暗号アルゴリズムの置換ではないことが明らかになる。枠組みをショアのアルゴリズム[22] に限定すれば、対応は狭く反応的になる。枠組みを広いエコシステムに拡大すれば、より多様なリスクと戦略が浮上する。この視点は政策立案者や技術コミュニティに対し、還元主義的な枠組みを排し、PQC 移行を暗号数学と同様に主権・プライバシー・グローバル公平性に触れる体系的変革と捉えるよう促す。

ボックス 5.「Q-Day」を超えた PQC の社会技術的視点：誇大宣伝の役割

PQC に関する議論は、強力な量子コンピュータが古典暗号を突然無効化する「Q-Day」という脅威によって頻繁に盛り上がる。動員的な物語としては有用だが、この枠組みは問題を歪めるリスクがある。量子能力は津波のように突然到来するのではなく、漸進的で不均一なプロセスとして現れる。 まず少数のマシンが特定の鍵を破れるようになり、その後より広範な応用へと拡大する。並行して、グローバーのアルゴリズムのような手法は、ショーア可能なデバイスが存在するずっと前から、パスワードの総当り攻撃を加速させる。

[22] Shor のアルゴリズムは、Peter Shor (1994) によって開発された量子アルゴリズムであり、量子コンピュータを使用して大きな整数を因数分解し、離散対数を計算する。これらのタスクに対するその多項式時間のパフォーマンスは、従来のアルゴリズムとは対照的である。これが、Shor のアルゴリズムが公開鍵暗号システムの脆弱性に関する懸念の根底にある理由である。

誇大宣伝は促進と歪曲の両面を持つ。一方で、警戒心を煽る枠組みは投資を動員する。PQC 研究コンソーシアム、パイロットプロジェクト、標準プロセスの急成長がその証左だ。他方で、Q-Day 比喩への過信はリスクを伴い、時期尚早あるいは方向性の誤った投資を招く。過去の事例がこの緊張関係を示している。スノーデン暴露後、ウェブカメラカバーのような象徴的行動が広まった一方で、より深い構造改革は遅れを取った。 PQC の文脈では、組織が長期保存データの機密性維持やサプライチェーンにおける暗号の柔軟性といった、より繊細だが同様に差し迫った課題に取り組まず、注目を集める移行に資源を費やすリスクがある。問題を「Q-Day」ではなく「Q-period」として捉える現実的な枠組みは、量子技術の実際の進化と標準の準備状況に歩調を合わせた、バランスの取れた移行戦略を支えるだろう。

第 X 部　防衛セクターにおける量子安全への移行

1. 序論

量子技術は防衛・安全保障の戦略的環境を再構築している。欧州連合とその同盟国にとって課題は、こうした革新技術の採用だけでなく、急速に進化するグローバルエコシステム全体での技術的主権と相互運用性の確保にある。防衛システムへの統合は状況認識能力、レジリエンス、作戦上の優位性を高める可能性を秘める一方、量子コンピューティングが既存の暗号標準を脅かすことで新たな脆弱性も生み出す。

政府、研究機構、防衛産業は、量子技術に耐性のある移行を準備しつつ、研究開発を加速させるために連携している。しかし、量子技術が民生と軍事の境界を曖昧にするにつれ、特にデュアルユース研究、知的財産、機密分類をめぐるガバナンスと倫理上の課題も生じている。

2. 防衛セクターにおける量子技術

現代の量子技術は、量子センシング・計測、量子コミュニケーション・ネットワーク、量子コンピューティングの 3 つの主要カテゴリーに分類できる。防衛応用における各分野の成熟度は異なる。関連技術には量子レーダー・イメージングや QRNG（量子乱数発生器）が含まれる。

2.1. 量子センシングと計測技術

量子センシングは量子状態を利用し、物理量（磁場・電場、加速度、時間）を精密に検知する。防衛セクターでは従来技術より効率的である。主な応用領域は以下の通りだ：

- **精密航法・測位（PNT）**：量子強化型原子時計は貴重な時間基準を提供し、GPS- 独立航法（例：潜水艦が検知を回避するために用いる技術）を向上させる。衛星信号なしで航空機や潜水艦の航法を実現する量子加速度計が開発中である。

- **センサーと探知：**量子重力計測と量子磁力計測は、量子センシングの一形態である。これらはプラットフォームや車両に展開され、地下構造物の探知、潜在的な迷彩航空機（空中）の検知、不発弾の特定（地上）、あるいは船舶の捜索（水中）に用いられる。磁気異常探知機（MAD）は、潜水艦の金属船体が地球磁場に生じさせる擾乱を識別することで、長年潜水艦検知に用いられてきた。例えば、従来の MAD アレイ（曳航式や哨戒機搭載式が多い）は、磁気信号が距離とともに減衰するため、数百メートルという限られた探知範囲しか持たない。カナダの民間企業は、1.2km の探知範囲を持つ量子磁力計の開発に成功した。これは従来技術と量子技術の劇的な差を示している。[23]

[23] CAE MAD-XR（磁気異常検知拡張任務）を参照のこと。https://www.youtube.com/watch?v=btn288Y8G84

■ **計測とタイミング**：量子センサーは航法を超えて、軍事システム全体のタイミング同期を向上させる。量子リンクを介した安全なクロック分配は、スプーフィングや妨害に対する作戦調整を強化する将来の量子ネットワークの必須要素と見なされている。[24]

量子センシングの応用分野（量子時計から磁力計まで）が増えるにつれ、これらの技術は戦争における最初の量子技術革新の一つとして展開される見込みだ。

2.2. 量子コミュニケーション

現代の軍隊は、指揮統制、情報共有、部隊調整のために安全なコミュニケーションに依存している。量子コミュニケーション技術は、量子コンピューターによる盗聴さえも耐えうる超安全な通信路の提供を目指す。最大の懸念は、量子コンピューターが実用化されれば、ほとんどの軍事コミュニケーションの安全確保に用いられている公開鍵暗号（RSA、ディフィー・ヘルマン、楕円曲線）を急速に破られる可能性がある点だ。 量子コミュニケーションは、数学的問題の計算難度ではなく物理学に基づいている点で、 の PQC とは異なる。この分野の主要技術は QKD である。主な進展は以下の通りだ：

■ 運用段階の QKD システム：量子耐性通信リンクの試験運用が進んでいる。信頼ノード型 QKD ネットワークは既に実用化されており、中国はこの技術に多額の投資を行っている。例えば 2016 年には北京と上海間に 2000km の QKD 光ファイバー基幹網を構築し、量子暗号化リンクで複数都市を接続した。 欧州では EuroQCI イニシアチブが、地上光ファイバーネットワークと量子衛星の両方を用いた安全コミュニケーション（Security And cryptoGrAphic: SAGA）を展開中だ。防衛企業も参画しており、レオナルド社はローマに量子都市圏ネットワーク（QMAN）を構築し、自社拠点を QKD で接続している。

■ 量子安全ネットワーク：量子コミュニケーションの最終目標は、点対点の QKD リンクから統合量子ネットワークへの移行である。将来のエンタングルメントベースネットワーク（量子中継器）は信頼できる中継器を不要にし、長距離 QKD を可能にする。これらのネットワークは量子センシングと量子コンピューティングを部隊全体に分散させ、量子状態を安全に共有する。

2.3. 量子コンピューティング

防衛セクターにおいて、量子コンピューティングは攻撃・防御双方に影響を与える両刃の剣である。強力な量子コンピューターは現在の暗号プロトコルの大半を破り、軍事コミュニケーションやデータセキュリティを脅かす可能性がある。この暗号解読の脅威に対抗するため、軍や政府は量子コンピューターと従来型コンピューターの両方からの攻撃に耐える PQC（ポスト量子暗号）の開発と展開を急いでいる。

将来の量子コンピュータは、複雑な最適化問題、シミュレーション、人工知能問題をはるかに高速に解決し、防衛セクターにおける兵站、暗号化/復号化、材料科学で優位性をもたらす可能性がある。軍事兵站や作戦計画には、経路設定、スケジューリング、資源配分など、予算・地理・技術・人的制約下で達成すべき極めて複雑

---

[24] ジャミングが信号損失を引き起こすのとは異なり、スプーフィングはシステムを欺いて虚偽のデータを信頼させる。スプーフィングは自律走行車の誘導変更、ドローンの誤誘導、金融取引におけるタイムスタンプの改ざん、通信ネットワークの同期障害などに利用されうる（出典）。

な最適化問題が含まれる。グローバーの探索や量子アニーリング法などの量子アルゴリズムは、特定の最適化課題を従来のヒューリスティック手法より効率的に処理できる。例えば、補給輸送隊のルート計画、航空部隊の最適スケジュール、戦場全体での予備部品の効率的配分などが量子コンピューティングで加速される可能性がある。電子戦においては、量子最適化が周波数ホッピングパターンの選別や妨害技術の最適化に寄与する。これらの応用例は十分な量子ビット数を確保できるか否かに依存するため、現時点では理論上の可能性に留まる。量子コンピューティング能力は量子力学システムのシミュレーションにも適している。防衛セクターでは、新素材設計やセンサー向け高温超伝導といった物理プロセスの理解を支援する可能性がある。

量子センシングは最も即効性のある運用上の利点を提供する。磁気異常探知機拡張型（MAD-XR）のようなシステムは既に同盟海軍に展開されており、量子重力計はトンネル検知における戦場での有用性を示している。量子コミュニケーションはより複雑な状況だ。中国が量子鍵配送（QKD）インフラを積極的に展開する一方、西側同盟国は懐疑的で、アルゴリズムベースの耐量子ソリューションを好んでいる。量子コンピューティングは依然として主に長期的な能力であり、戦場展開ではなくクラウドベースのアクセスを必要とする。人工知能（AI）と並んで、量子技術は防衛セクターにおける破壊的イノベーションと位置付けられている。北大西洋条約機構（NATO）や EU の戦略家たちは、これを 2030 年以降に向けた重要能力領域の一つに含めている。

3. 関連する利害関係者及び量子防衛イニシアチブ

3.1. 防衛セクターにおける量子技術の概要

防衛セクターにおける量子技術の応用は、官民セクターや国際団体など幅広いステークホルダーからなる生態系を巻き込み、技術アセスメントや戦略的優先度の差異に基づく多様なアプローチを追求している。

3.2. 主要プレイヤーとイニシアチブ

世界的に、防衛計画担当者は量子技術を戦略的フロンティアと認識しており、多くの事業体が遅れを取らないよう動員している。この状況は、要件を設定する軍事機関、ソリューションを開発する産業界、そして両者を橋渡しするパートナーシップが混在していることが特徴である。

政府および同盟関係者の観点では、NATO と EU はイノベーション政策において量子技術を明示的に優先課題としている。NATO は量子技術を「新興破壊的技術（EDT）」と識別している。これらの技術は変革をもたらすと考えられており、NATO は同盟国による量子技術の採用促進と、敵対勢力による量子技術の悪用から同盟を防御することを目指している。NATO は潜在的な量子関連の課題や脅威に直面する中で、耐量子暗号技術と安全な通信の採用促進を目的としている。資金面では、NATO のイノベーション基金（10 億ユーロ規模の多国籍ベンチャー基金）と DIANA アクセラレータープログラムが、量子技術を「 」優先分野に含めている。これは同盟全体の安全保障に寄与し得るスタートアップ企業やデュアルユース技術への投資を目的としている。これにより NATO は、同盟が量子技術の発展に遅れを取らないよう、同盟国による量子イノベーションエコシステム（例：量子暗号化や量子センサーに取り組む企業）の構築に貢献している。この文脈において、大西洋横断量子コミュニティ（TQC）が重要な役割を果たしている。TQC は 24 の同盟国政府・産業界関係者・学術機関からなる、ユニークで柔軟な任意参加型コミュニティである。同盟内での量子技術の促進・拡大手法を模索するために活用されている。

欧州防衛庁（EDA）は EU 内で防衛セクターにおける量子技術導入を推進する主導的役割を担っている。EDA は量子通信の軍事応用を探るプロジェクト（ANQUOR）を開始した。目的は民間量子研究開発（例：EU 量子フラッグシップ成果）を活用し、軍事環境下でのユースケースを実証することである。具体的には QKD（量子鍵配送）に特化した軍事要件の実現可能性と作戦上の利点を検証する。こうしたプロジェクトは、民間量子技術を防衛ニーズに適応させるという、EDA のデュアルユース・イノベーションへのアプローチを示している。加盟国による個別イニシアチブ（例：フランスの防衛戦略における量子技術）は、しばしば自国の防衛主要企業に対し、スタートアップや学術研究所との協力を促している。産業界では、従来の防衛請負業者と専門量子技術企業がますます連携を深めている。知識共有と開発加速のため、産業コンソーシアムやネットワークが形成されている。入札連合を通じた調整は重複を避け、同盟国間での技術相互運用性を促進する。こうした知見が欧州関係者に競争力維持と外国量子技術への依存回避を促している。

世界的には、米国や中国なども量子技術を推進する主要な利害関係者であり、これは世界の防衛情勢に影響を与えている。米国防総省は、量子時計、GPS 遮断時の航法用慣性センサー、量子無線周波数受信機などを探求する複数のプログラム（例：サービス研究所）を有し、IBM、IonQ、マイクロソフトなどの企業と量子コンピューティング研究で協力している。中国は量子コミュニケーション（例：ミチウス衛星）に多額の投資を行っている。2025 年 4 月には、コヒーレント集団閉じ込め原子磁力計の試験に成功し、量子磁力計分野で突破口を開いたと発表した。これは、従来の磁力計が課題を抱える低高度地域などの特定運用環境で優位性を発揮する可能性があり、敵艦の尾波を検知する能力を実証した。

量子分野におけるイノベーションの多くは、政府研究所ではなく大学や中小企業で生まれていることを考えると、この分野では官民の連携が極めて重要だ。スタートアップ企業が技術を提供し、防衛関係者はその技術をどのように統合するかを検討する。公共セクターはこうした連携を重視する必要がある。欧州では、欧州防衛機関（EDA）や NATO などの欧州防衛産業（ ）組織も、資金援助の募集や作業部会を通じて、同様の連携を推進している。米国では、ロッキード・マーティンやノースロップ・グラマンなどの企業が、社内で量子研究や投資を行っている（ロッキードは D-Wave 社の量子アニーリングシステムの初期投資家である）。これらの例は、従来の防衛関連企業と最先端の量子企業が協力する、量子分野における防衛産業基盤の成長を示している。

注目すべき点は、産業界が、量子技術を実環境下で実証するためのパイロットプロジェクトにおいて、政府と緊密に連携することが多いということだ。例えば、タレス社は欧州の OPENQKD テストベッドに参加した。このような実証は、標準、セキュリティ認証、運用コンセプトの開発に役立つ。

また、関係者の国際的側面にも注目すべきだ。量子技術競争は商業的だけでなく地政学的でもある。米国と中国は PQC などの分野で特許出願を支配し、2012 年から 2024 年までの世界特許の 3 分の 2 以上を占める。NATO は研究イニシアチブや多国籍プロジェクトを開始しており、大西洋横断協力（例：量子標準とセキュリティに関する米 EU 対話）も存在する。他の世界的な勢力（例えば中国の量子コミュニケーション分野での成果）による急速な進化は、NATO や EU 加盟国が取り組みを調整する原動力となっている。

4. 防衛セクターにおける耐量子暗号への移行

防衛セクターにおける耐量子暗号への移行は、政策（NSA、EDA、NATO などの組織が定める義務と期限）、技術開発（防衛産業とサイバーセキュリティ企業による）、導入計画（脆弱性の棚卸しと移行計画の策定）にまたがる協調的な取り組みである。包括的な目標は、将来の脅威を見据えてコミュニケーションセキュリティを優先し、量子コンピューターが登場した際に、敵対者が軍事指揮統制コミュニケーションコンピュータ情報

監視偵察システム（C4ISR）を機能不全に陥らせたり、数年にわたる機密データを解読したりできないようにすることだ。 特筆すべきは、欧州防衛庁（EDA）で発表された PQC 特許動向調査で、米国と中国が耐量子暗号分野のグローバル特許ファミリーの 3 分の 2 以上を占めている事実だ。この移行は既に進行中である：実戦シナリオでの PQC 試験（例：米陸軍の戦術ネットワーク向け量子レジリエンス通信ソリューション契約）が進み、同盟全体でのガイドライン策定が進められている。 今後の課題は、膨大なレガシーシステムを期限内に更新し、現行運用を妨げずに変更を管理することだ。関係者は現在この課題に取り組んでおり、量子時代においても軍隊の安全を確保しようとしている。

防衛産業のプレイヤーはこの移行において極めて重要だ。なぜなら、アップグレードが必要な通信システム、ソフトウェア、ハードウェアの製造事業者だからだ。 実際、業界は社内の専門知識を活用し、暗号適応性の原則を採用している。レオナルド社は、VPN プロトコル（例：WireGuard）の移行による PQC 認証の実現、TLS セキュアコミュニケーションへの PQC 統合、多層セキュリティのための QKD と PQC の組み合わせなど、実用的な統合課題に取り組んでいる。こうした取り組みは業界内で認識されている。

量子技術は研究段階から展開段階へ急速に移行し、防衛能力と戦略的自律性の基盤を再定義しつつある。量子センシングが最初に運用上の優位性をもたらし、量子コミュニケーションが情報セキュリティを再構築するだろう。量子コンピューティングはより長期的な課題ではあるが、意思決定と暗号パラダイムを変革するに違いない！

第 XI 部　推奨事項

本タスクフォースは、耐量子暗号への移行を単なる技術的アップグレードではなく、包括的かつ体系的な変革として捉えるべきだと考える。 PQC への移行は暗号ライブラリの更新をはるかに超える。通常、新製品バージョンの統合、API の変更、ソフトウェア開発ライフサイクルの適応、場合によってはサプライチェーンを含む中核業務プロセスの再設計を必要とする。このプロセスは、長期計画、専門人材の採用、数年にわたる持続的な組織変革を要する経営上の課題である。

こうした背景を踏まえ、本タスクフォースは政策立案者、民間セクター、研究コミュニティに対し、EU における量子耐性への移行を強化する方法について以下の推奨事項を行う。

本節は、まず一般的な推奨事項を示し、続いて分野別推奨事項を提示する構成となっている。分野別推奨事項は、後述する一般的な推奨事項に追加される層として位置付けられることに留意すべきである。これらは包括的措置に取って代わるものでも、独立したものでもない。むしろ、各分野固有のリスク、実施上の課題、運用慣行に対処することで、それらを補完するものである。

1. 一般的な推奨事項

GR1. 暗号の俊敏性を開発する

一般的に、暗号システムは脆弱化することがあり、更新版への置き換えが必要となる場合がある。耐量子暗号への移行は、この更新の差し迫った一例に過ぎない。耐量子暗号の追求においては、数十億台のデバイスの暗号化手法の移行には特定のモデルが必要であり、技術的、組織的、政策的な観点からの設計が求められる。このような取り組みには、リスクベースのアプローチが必要である。このアプローチは、測定されたリスクとニーズに基づく暗号アジリティの原則を中心に据えるべきだ。

暗号アジリティとは、暗号プロトコルやシステムをモジュール式に設計し、暗号コンポーネントの交換を可能にする手法である。単発的なアルゴリズムの差し替えではなく、暗号アジリティアプローチでは、最小限の混乱で暗号アルゴリズムやプロトコルを迅速に変更する能力を構築する。これにより、時代遅れのアルゴリズムが抱えるセキュリティ脆弱性を回避できる。 例えば、アプリケーションはコードの大幅な変更ではなく設定変更でアルゴリズムを変更できる暗号化をサポートすべきであり、プロトコルは当事者間で利用可能な最強の標準アルゴリズムを使用するよう交渉されるべきだ。これは暗号技術的な課題であると同時に、ソフトウェア工学上の課題でもある。俊敏性とは移行中の相互運用性を維持することも意味し、これは必要不可欠とみなされる。

GR2. 暗号依存性の対応についてサプライヤーと連携する

多くの組織はサードパーティ製品・サービスに大きく依存しており、サプライチェーン上の依存関係が移行の制約と可能性を決定することが多い。重要な製品や依存関係が組織の直接管理外にある場合、PQC への移行はしばしば停滞する。 ソフトウェアベンダーやサプライヤーは段階的なアップグレードスケジュールを採用しており、多くの暗号化コンポーネントは複雑にネストされた依存関係の中に埋もれている。この課題に対処するには、組織はサプライヤーとの強固な連携、量子耐性機能のタイムラインに関する明確な要求、サプライチェーンの準備状況を追跡する仕組みが必要だ。 この文脈において、実行可能な計画は、内部および外部の依存関係、ソフトウェ

ア、ハードウェア、API、サービスのインベントリ作成から始まる。これにより組織はサプライヤーと関わり、アップグレードのタイムラインを要求し、それに応じて計画を立てられる。このマッピングは技術的な前提条件であるだけでなく、EU 規制に統合可能なサプライチェーンリスクマネジメントツールとの連携を可能にする。サプライチェーンパートナーが暗号の詳細を標準化された形式で報告すれば、より信頼性の高い自動化、コンプライアンス、政策立案が可能となる。

GR3. 暗号技術と製品のインベントリ構築・維持

耐量子暗号への移行に備え、組織は暗号資産と製品インベントリの構築方法と維持管理に注力している。インベントリ作成を優先すべきであり、まず最も関連性の高いユースケースに焦点を当てる。こうしたインベントリの優先順位付けはロードマップ構築に役立ち、移行活動の背景情報を提供する。 暗号資産のインベントリ作成は重要な作業であり、これまでの分析に基づけば、移行が必要な対象の全体像をより深く理解する助けとなる。そこから生まれるのは硬直した設計図ではなく、初期段階での計画立案、技術チームとガバナンスチーム間の連携、そしてインベントリが何を捕捉すべきか、その理由を明確に理解することで形作られる一連の指針となる実践手法である。 目標は、異なる関係者が資産リストを孤立したチェックリストではなく、より広範な移行戦略を支える進化するツールとして扱える共通言語と運用マップを開発することだ。この枠組みには、初期計画、部門横断的な調整、そして資産リストを体系的かつ構造的に扱う方法を理解するという主要目標が組み込まれる。暗号資産リストと製品リストは別個のアセスメントである。

暗号インベントリは、組織のシステム全体で暗号技術がどこでどのように使用されているかを詳細にマッピングするものである。その目的は、現在使用されている暗号アルゴリズム（RSA、ECC、AES）、その実装コンテキスト（コード署名、コミュニケーション用 TLS）、量子耐性ステータス（レガシーか PQC か）、暗号モジュールと標準の依存関係を識別することにある。 暗号資産インベントリの重要なテーマは、リスクベースのアプローチを採用し、PQC を最優先で必要とする重要システムから優先的にインベントリを実施することだ。暗号資産をカタログ化する際には、マッピング対象システムの相互に絡み合ったインフラ構造を認識することが不可欠である。

こうしたインベントリに記録されるデータは、細分化され詳細である必要があり、以下を含むべきだ：

- ■ 使用されているアルゴリズムの種類（RSA-2048、ECC、AES-128、SHA-2 など）
- 当該暗号技術の機能目的（認証、機密性、完全性など）
- プロトコルコンテキスト（例：TLS 1.2、IPsec、S/MIME）
- 使用される資産（例：ルーターのファームウェア更新署名、アプリケーションの内部 API、VPN コンセントレータ）
- 暗号機能の起源（自社開発、サードパーティライブラリ、OS カーネルモジュールなど）
- PQC 標準との互換性、またはハイブリッド方式の一部であるかどうか
- 防御対象データの保存期間（短期保存データか長期保存データか）

■　防御対象データの機密性（専有情報、機密情報）。

製品インベントリは、組織が使用する外部製品・サービス・ハードウェア（例：サードパーティプロバイダ）に焦点を当て、これらの製品の暗号特性をマッピングする。組織は製品インベントリの暗号評価に実用的なツールやプロセスを活用できる。 調達ガイドラインを更新し、暗号要件を含め、問い合わせに対応することも選択肢となり得る。つまり、新しいソフトウェア、ハードウェア、クラウドサービスを購入する際、組織はベンダーに対し、製品で使用されている暗号アルゴリズムとプロトコルの開示を要求し、場合によっては耐量子アップグレードのロードマップも求めることになる。

GR4. 量子耐性をデジタルシステムに最初から組み込む

欧州委員会と加盟国は、欧州デジタル ID ウォレットなどのデジタルシステムが最初から量子耐性を備えた設計となるよう確保すべきだ。言い換えれば、暗号技術を必要とする新サービス・システム・標準を導入する場合、その暗号技術は初日から量子耐性を持つ必要がある。 これは、ポスト量子暗号を将来的な後付けではなく、システムアーキテクチャ、認証、調達プロセスに統合することを意味する。EU 団体は適合性試験を調整し、デバイスやネットワークを横断した性能評価のためのパイロット展開に資金を提供し、分断を防ぐための規範的な技術ガイダンスを発行すべきだ。これらの原則を今組み込むことで、今後数十年にわたり欧州のデジタルインフラを保護し、導入後のコストのかかる混乱を招くアップグレードを回避できる。

GR5. 誇大宣伝を超えて：Q-Day から Q-period へ

PQC に関する議論は、強力な量子コンピュータが古典暗号を突然無効化する「Q-Day」という脅威に煽られることが多い。動員手段としては有用だが、この枠組みは問題を歪めるリスクがある。量子能力は津波のように一気に到来するのではなく、漸進的かつ不均一なプロセスとして現れる。 まず少数のマシンが特定の鍵を破れるようになり、その後より広範な応用へと拡大する。並行して、グローバーのアルゴリズムのような手法は、ショーア可能なデバイスが存在するずっと前から、パスワードの総当り攻撃を加速させる。

誇大宣伝は促進と歪曲の両面を持つ。一方では警戒心を煽る枠組みが投資を動員する。他方では Q-Day 比喩への過信が時期尚早あるいは方向性の誤った投資を招く。PQC（耐量子暗号）の文脈では、 組織が注目を浴びる移行に資源を費やす一方で、保存データの長期機密性やサプライチェーンにおける暗号適応性といった、より微妙だが同様に差し迫った課題に対処しないリスクがある。 より現実的な枠組みとして、問題を「Q-Day」ではなく「Q-period」と捉えることで、量子能力の実際の進化や標準の準備状況に合わせた、バランスの取れた移行戦略が支援されるだろう。

[25]GR6. 耐量子暗号移行ロードマップと量子移行戦略および既存法規の連携

調整されたリスク認識型移行戦略なしに EU 量子耐性ロードマップを推進することは重大なリスクを伴う。ロードマップは必要なマイルストーンとその期限を明記すべきだが、加盟国・ベンダー・機構がそれらを達成する方法を定義できるのは支援戦略のみである。標準・認証スキーム・相互運用性枠組み・試験インフラが同期しなければ、規制が準備態勢を追い越す恐れがある。 したがって、このロードマップは、国家計画、産業の取り組み、規制ツ

[25] 耐量子暗号への移行に向けた調整済み実施ロードマップ（本ロードマップ）

ールを整合させるより広範な EU 枠組みに組み込まれるべきである。DORA、CRA、NIS2 間の調整を確保し、ENISA、欧州委員会、ETSI、CEN/CENELEC といった標準化団体によって導かれることで、一貫性があり実行可能な移行を実現する。

GR7. ロードマップ間の整合性と一貫性を確保する

量子耐性への移行に向けた複数のロードマップが現在、EU レベルおよび各国レベルで策定・議論されている。これらは耐量子暗号、量子通信、関連インフラ構想を網羅している。各ロードマップは重要な優先事項と指標となるマイルストーン（例：2026 年、2030 年、2035 年）を設定しているが、適切に調整されなければ、要求事項や実装が断片化したり、さらに悪い場合には互換性を欠くリスクがある。 欧州委員会は加盟国や標準化団体と連携し、タイムライン・依存関係・目標の一貫性を確保するため、ロードマップ間の調整を推進すべきだ。この調整は、異なる時間軸で進行する標準開発・ベンダー実装・大規模展開の各段階において特に重要である。

グローバルな整合性を確保し断片化を回避するため、EU は米国やその他の G7 経済圏とも緊密に連携し、量子耐性移行に向けたロードマップ、技術要件、タイムラインの調整を図るべきである。

GR8. ロードマップへの並列化の導入

現行のロードマップ構造は段階的・直線的アプローチを暗黙に前提としており、特にある領域の進展が別の領域の完了に依存する場合、意図せずボトルネックを生む恐れがある。EU 域内の暗号システムの複雑性と多様性を考慮し、進展加速とシステムリスク低減のため、ロードマップへの並列化強化を推奨する。 以下に、調整と整合性を維持しつつ並列性を高めるための具体的かつ実行可能な提案を示す。活動の一連の流れ（例：インベントリ→リスクアセスメント→パイロット→展開）を厳格に推奨する代わりに、ロードマップをモジュール化され組み合わせ可能なマイルストーンパッケージとして構成することを提案する。これらのモジュールは条件が許せば独立して開始でき、加盟国、セクター、事業者が先行する全タスクの完了を待たずに前進することを可能にする。

例えば：

- プロトコル対応評価と並行して、資産の棚卸しと暗号資産分類を進めることができる。
- ベンダーとの協議や調達計画は、規制調整に関する議論が進行中でも開始できる。
- ロードマップを役割別トラックに分解することを提案する。各トラックは独自の活動、成果物、タイムラインを持つ。これらはエコシステム全体の自然な分業を反映し、異なるステークホルダーが並行して進めることを可能にする。
- 政策・規制トラック：義務付け事項、法的調和、公共セクターの資金調達手段に焦点を当てる。
- 標準化と相互運用性トラック：プロファイリング、適合規準、新興国際標準の統合に焦点を当てる。
- ベンダー支援トラック：PQC 対応製品の開発、認証、ベンチマークを促進することに焦点を当てる。

- 運用展開トラック：資産インベントリ、暗号部品表（Cryptography Bill of Materials）、公共サービスの移行、インシデント対応の更新に焦点を当てる。

- 監視と測定指標トラック：測定枠組み、監査、成熟度モデルに焦点を当てる。

この構造により、各ステークホルダーグループは他のグループの進捗に関係なく、関連するタスクに取り組むことが可能となる。

GR9. 認識向上、協力、より良いガバナンスの促進

サイバー空間では、すべての国々が国境を越えてつながり、この移行においても互いに依存している。したがって、加盟国は組織、事業体、ステークホルダーが知識と経験を共有できる環境やコミュニティを構築すべきだ。

国際的に事業を展開する欧州企業にとって、既に公表されているグローバルなタイムラインやアルゴリズムに関する推奨事項との緊密な連携は不可欠である。 多くの欧州企業は既に、自社製品・サービスにおける ML-KEM、ML-DSA、SLH-DSA の開発・実装に深く関与し、野心的な 2030-2035 年 PQC 展開スケジュール達成に向けて取り組んでいる。各加盟国が単独で、IETF、3GPP、米国政府、主要米国企業などのグローバル組織・事業体・関係者を惹きつけるコミュニティを構築できると期待するのは非現実的だ。 EU レベルでの調整すら極めて困難である。代わりに加盟国は、IETF や 3GPP といったオープンな国際標準化団体やオープンソース暗号コミュニティに積極的に参加し、国際レベルでの連携・影響力・知識共有を確保すべきだ。

加盟国は透明性のある移行計画で率先垂範すべきだ。政府の移行ロードマップを公表し、タイムライン、マイルストーン、予算を含め定期的に更新することで、知識共有とベストプラクティスを促進する。ロードマップは「ステークホルダー」の定義を省庁、規制機関、技術専門家を超えて拡大すべきだ。市民社会、マイノリティネットワーク、草の根 DEI 組織は単なる「相談相手」ではなく、共同リーダーとして認識されるべきである。 調達、パートナーシップ、政策評価への社会条項とコミュニティ配当の統合は、「ベストプラクティス」としてだけでなく、測定可能な包摂の要件として不可欠である。

啓発キャンペーンや研修モジュールは、汎用的あるいは画一的であってはならない。本 CEPS タスクフォースは、市民教育とデジタル教育の抜本的拡充を要請する。PQC（耐量子暗号）の認知、量子リスク、デジタル権利といったテーマを、技術チームだけでなく社会全体、学校、介護機構、コミュニティセンターに浸透させる必要がある。

ロードマップは、市民が情報を受け取るだけでなく戦略を積極的に形成できる仕組み（市民議会、諮問パネル、定期的な透明性のある更新）を確立すべきだ。ロードマップは、2030 年までに国境を越えたサービスにおける PQC の相互運用性を試験する EU レベルの共同パイロットプロジェクトを促進すべきだ。

ENISA 傘下に官民共同の PQC 移行監視機関を設置し、進捗を監視するとともに、必要に応じてスケジュールの前倒しを推奨することを提案する。

我々は移行戦略と標準に関する国際対話の継続を提唱する。一つの可能性として、G7 が金融セクターにおける現行の量子セキュリティイニシアチブの範囲を拡大し、全分野にわたる広範な議論を含めることを歓迎する。

GR10. 技能開発と管理構造の促進

最後に、移行の成功は管理構造とスキル開発にも依存する。暗号技術の移行はもはやニッチな技術専門家の領域ではなく、部門横断的なチーム、透明性のあるガバナンス、明確なプロセス所有権が必要だ。移行を監督する責任を持つ単一のチームが存在せず、必要なスキルが不足しているため、多くの組織が苦戦している。摩擦を減らすには、教育、内部の専門センター、チーム間の連携への投資が不可欠だ。 即効性のあるインセンティブと経営陣レベルの関心の欠如が、この課題への取り組みをためらわせる要因となっている。組織は、明確な事業レベルの優先事項から始まる、確立され、資金提供され、権限を与えられたプログラムを持つべきだ。現在の進捗の多くはボトムアップであり、経営陣の支援が不足している。

2. 金融セクター向け追加推奨事項

FS1. 臨時的な PQC ガバナンス体制の構築

ガバナンス体制は極めて重要である。企業は PQC 移行運営委員会またはタスクフォースを設置すべきだ。この組織は暗号技術の使用状況の把握、標準の追跡、事業優先順位と規制要件に沿った移行スケジュールの設定を監督する。多くの大手銀行は既にこの目的で内部の「量子リスク」または「暗号技術対応」チームを編成している。

FS2. ベンダーやパートナーとの連携強化

金融セクターの暗号インフラは、単一機構の枠を超えて存在する。ベンダー、サードパーティサービスプロバイダー、ハードウェア製造事業者を含む。これらの主体に依存しているのだ。主要なボトルネックは、技術プロバイダの PQC 対応準備状況である。したがって、企業は早期にベンダーと関わり、そのロードマップに PQC サポートが含まれるよう確保すべきだ。新規調達においては、設計段階からの暗号適応性を効果的に求めることになる。 金融機関が共通の調達標準で合意できれば、ベンダーのインセンティブを高め、分断を減らせる。

FS3. 金融セクター基盤インフラのアップグレード

企業は基盤インフラをアップグレードし、HSM、暗号ライブラリ、VPN アプライアンス、その他関連コンポーネントが量子耐性アルゴリズムをサポートできるようにする必要がある。重要な推奨事項として、進行中の広範な IT 近代化イニシアチブの一環としてアルゴリズムを近代化することが挙げられる。例えば、銀行がサービスをクラウドに移行したり、コアバンキングシステムを置き換えたりする場合には、暗号の俊敏性に関する考慮事項を最初から組み込むべきである。

FS4. リスクアセスメントに基づく行動の優先順位付け

移行の規模を考慮すると、全てを一度に変更することは不可能だ。どのシステムとデータを優先的に保護すべきかを決定するには、リスクベースのアプローチが不可欠である。このプロセスは暗号資産の棚卸しから始まる。 コストがかかり、実際の移行開始後に陳腐化する恐れのある包括的なインベントリ作成を目指すのではなく、事業レベルのリスク・リターン分析に基づき、事業の特定部分のみを移行対象とするトップダウンかつリスクベースのアプロ

ーチによるインベントリ作成を推奨する。特定の依存関係は維持する必要があるものの、これにより移行中に事業の正当性と価値を識別・追跡できる。

特定プロジェクトのインベントリ作成にあたり、金融機関はアルゴリズム、鍵長、証明書、それらの使用場所と方法を含む全ての暗号資産をカタログ化すべきだ。インベントリでは、長期にわたる機密保持要件を持つ資産（例：10 年以上秘密保持が必要なデータ）を識別しなければならない。このインベントリを用いて、各資産の量子脆弱性を推定できる。重要なのは、リスクアセスメントにおいて暗号強度とビジネス影響の両方を考慮することだ。全てのシステムが同等のリスクを負うわけではない。PQC を最優先で必要とする重要システムを優先すべきである。決済システムや銀行間認証を支える PKI など、影響度が高くセキュリティ寿命が長い資産は早期に移行すべきだ。

FS5. 緩和オプションの費用便益分析を実施する

解決策は全て同じではない。ハードウェア変更を伴うもの（ハードウェア上のハイブリッドソリューション、QRNG や QKD リンクの展開）もあれば、純粋にソフトウェアベースのもの（PQC アルゴリズムへの切り替え）もある。タスクフォースは、大手銀行における暗号技術の完全移行には数億ドル規模の費用がかかる可能性があると指摘している。取締役会や経営陣にとって、達成されるリスク低減に対して支出を正当化するには、定量化されたリスクアセスメントが不可欠である。何もしない場合のコスト（将来の侵害による潜在的な罰金、損失、評判の毀損など）が移行コストを上回る場合、PQC 投資のビジネスケースは明らかになる。

FS6. 組織的・技術的ギャップの克服

金融機関は全レベルで暗号技術のスキルと認識が不足している。暗号技術は IT 分野においてニッチな領域であったが、今や主流の関心事となる必要がある。多くの金融機関では暗号技術を静的なユーティリティとして扱う文化が根付いている。この考え方を継続的な暗号技術の改善へと転換することは組織的な課題である。

3. 公共セクター向け追加推奨事項

PS1. PKI およびデジタル ID エコシステム全体での段階的移行計画の実施

行政機関は、PKI とデジタル ID システムのアップグレードに際し、調整されたリスクベースのアプローチを採用すべきだ。移行は、国民 ID 登録システム、越境認証サービス、公共の信頼を支える認証局など、最も重要かつ影響力の大きいコンポーネントから開始し、その後依存システムへ拡大すべきである。行政機関は、依存関係をマッピングし量子リスクに最も晒されている領域を特定するため、包括的な暗号技術インベントリを実施すべきだ。このマッピングは、短期的な継続性のためのハイブリッド暗号技術と、長期的な耐量子標準の採用を組み合わせた段階的な移行ロードマップの策定に活用されるべきである。持続可能な実装を確保するため、デジタルアイデンティティおよびトラストサービスの新規調達には、暗号技術の柔軟性と耐量子対応要件を含め、システムが標準と共に進化できることを保証しなければならない。この調整されたリスク情報に基づくアプローチは、断片的なアップグレードを回避し、移行期間中も重要な認証および署名サービスが稼働し続けることを保証する。

PS2. 分断化とサービス中断を防ぐため、認証レイヤーを同期させる

認証システム、ルート証明書、中間証明書、ブラウザ、失効サービスは、量子移行期における信頼性と相互運用性を維持するため、歩調を合わせて進化しなければならない。欧州委員会と各国当局は、これらの層全体で同時対応を確保するため、移行を調整すべきだ。これには、性能影響のベンチマーク、相互運用性テストと負荷テストの実施、大規模な証明書や増加する計算要求に対応するフォールバック機構の確立が含まれる。同期化されたアプローチは、断片化した実装を防ぎ、サービス停止を最小限に抑える。

PS3. 国境を越えたロードマップの調整と国家移行戦略の整合化

欧州委員会と加盟国は、量子耐性移行のための共同ロードマップを策定し、各国の PKI アップグレード、タイムライン、政策枠組みを整合させるべきだ。この調整は国境を越えた相互運用性に焦点を当て、信頼チェーン、認証プロセス、ガバナンスモデルが EU 域内で一貫性を保つことを保証する。定期的な報告と共有された準備状況のベンチマークを制度化し、各国のインフラが同期して進化し相互信頼を維持することを確保すべきだ。

PS4. 量子移行を社会技術プログラムとして調整管理する

公共セクターにおける耐量子移行は、単なる暗号化アップグレードではなく、エコシステム全体での取り組みとして取り組むべきだ。欧州委員会と加盟国は、技術機関、規制当局、標準団体、産業関係者を結集する調整メカニズムを確立し、移行を導くべきである。移行計画は、レガシーシステムや運用技術上の制約を考慮し、アップグレードのスケジュール設定や並行する標準更新を可能にすることでボトルネックを防止しなければならない。

4. 防衛セクター向け追加推奨事項

DS1. 耐量子移行ロードマップの策定

防衛産業関係者は、政府の政策マイルストーンと産業展開を同期させる耐量子移行ロードマップを策定すべきだ。このロードマップは、包括的な暗号資産の棚卸しを義務付け、ミッションクリティカルかつ高リスクシステムを優先し、PQC 実装のクロスベンダーテストを調整すべきである。共通の移行ベンチマークを開発することで、防衛サプライチェーン全体の相互運用性が向上し、重複作業が防止され、重要な運用を妨げることなくレガシー の指揮・統制・コミュニケーションインフラの近代化が可能となる。

DS2. 産業連携の支援

機構関係者は、欧州のバリューチェーンを優先し非 EU サプライヤーへの依存を減らす資金調達メカニズムを通じて、防衛プライム企業、量子産業の中小企業、研究機関間の産業連携を支援すべきだ。

DS3. サプライチェーン依存性の解消

同様に、欧州の関連機構（欧州防衛庁（EDA）、欧州委員会、欧州防衛基金（EDF）など）は、サプライチェーンの依存性に対処すべきである。現在、いくつかの主要な量子アルゴリズムやハードウェア部品は米国やアジアに由来している。欧州の関係者は、欧州における独自の量子アルゴリズム、フォトニクスプラットフォーム、極低温技術の開発を優先すべきである。

DS4. 官民量子イノベーション枠組みの正式化

国際的・欧州の防衛機構（EDA、NATO、EDF）は、既存の防衛請負業者と新興企業・学術研究所を結ぶ官民量子イノベーション枠組みを正式に構築すべきだ。これらの連携には、共有テストベッド、機密・公開両方の研究開発トラック、技術移転加速のための共同出資実証機を含めるべきである。 優先すべきは、民生用と防衛用の両方に使える量子センシング・コミュニケーションシステムであり、民生向け研究開発（量子フラッグシップや国家プログラムによるもの）を防衛用途に適応させる必要がある。

DS5. 構造化されたパイロットから認証までの経路を確立する

運用段階に向けた新興量子システムの妥当性確認のため、EU と NATO は構造化されたパイロットから認証までの経路を確立すべきである。OPENQKD のようなプログラムは恒久的な量子防衛試験基盤へと発展させ、企業（例：タレス、レオナルド、中小企業）が軍事条件下でプロトタイプを試験できるようにすべきである。 その結果は、欧州標準化団体（ETSI、ENISA）に直接反映され、セキュリティと相互運用性のベンチマークを定義すべきだ。これにより、展開までの時間を短縮し、信頼できる欧州のソリューションを確保できる。

DS6. 防衛量子技術の研究を促進する

防衛量子技術の研究を促進するためには、学術研究者が防衛上の制約に抵触することなくキャリアを継続できる、安全な知識共有メカニズム（機密研究コンソーシアム、モジュール式出版、機密解除期間など）を確立することが不可欠である。

附属書 I. タスクフォースメンバー及び招待講演者リスト

調整役・報告者：ロレンツォ・プピロ（CEPS）

報告者：スワン・アッシュワース（CEPS）、アフォンソ・フェレイラ（CNRS）、カロリナ・ポリート（CEPS）

諮問委員会

ソフィー・リンドスコフ・ハンセン、デンマーク外務省

ミケーレ・モスカ、ウォータールー大学（カナダ）

マイケル・オズボーン、IBM チューリッヒ研究所

バート・プレネル、ルーヴェン・カトリック大学

ティム・ワトソン、アラン・チューリング研究所、ロンドン

企業

デロイト、バーバラ・ウェルマン、トマソ・ストラニエリ

アーンスト・アンド・ヤング、サラ・アンペ、スーラヴ・シンハ

エリクソン、ジョン・マットソン

インテル、リッカルド・マッスッチ、マティアス・シュンター

インベリアント、アレッサンドロ・ルオンゴ

KPMG、ベント・ダラガー

マイクロソフト、ケビン・ライフステック

クアルコム、サブリナ・スタニスラス＝ブミエ

クアンティニウム、ダンカン・ジョーンズ、マリオン・ルマソン

サンタンデール、ハイメ・ゴメス・ガルシア

スパークル、アントネッラ・サンギネティ

欧州の機構及び機関

欧州議会、ブランド・ベニフェイ、アンジェリカ・ペトロフ

欧州委員会、ファビアナ・ダ・ピエーヴェ

ENISA、フィリップ・ブロ

EDA、ゲオルギオス・スタマトゥコス、イシドロス・モノギウディス

ECCC、ロディカ・ティルテア

ESA、マッシモ・パンゼリ

ETSI、マーティン・ウォード

EIB、ハルド・グルーバー、デジレ・ルッカート

EU Quantum Flagship、エンリケ・サンチェス・バウティスタ

BSI、エレン・ステファン

研究機構

イタリア技術研究所、カミラ・コレッティ、アントニオ・ロッシ

学者・シンクタンク

GMF、アストリッド・ジーバース

I-COM、アントニオ・マンガネッリ

アムステルダム大学、ライマ・ヤンチュテ

マラガ大学、ハビエル・ロペス

プリモルスカ大学、ナスチャ・チェパク

サレント大学、アントニオ・フィカレッラ、アレッサンドロ・ラザリ

ユトレヒト大学、フェデリカ・ルッソ

市民社会

物の人間性エージェンシー、マリサ・モンテイロ・ボルスブーム、ディルク・ブルーム

招待講演者

シモーナ・アウトリターノ、BSI

フレデリック・バルバレスコ、タレス

オリヴィエ・ブラジー、エコール・ポリテクニーク

ミルコ・カルヴァレーシ、欧州委員会

ソフィア・チェリ、ブレイブ

カレン・デ・ウィンター、IBM

マウロ・デ・サンティス、イタリア中央銀行

マッシミリアーノ・ディスペンザ、レオナルド

アンジェラ・デュポン、国際決済銀行

アレックス・フェラッツィーニ、GovStrat

エドアルド・ジリオ、デロイト

フランシスコ・エレーラ、欧州中央銀行

イニ・コン、デルフト工科大学

ストラヴォス・コウシディス、BSI

カーン・サーヒ、NATO

アビラム・シェメシュ、マイクロソフト

マイケル・シルバーマン、FS-ISAC

ピーター・フェルマース、デルフト工科大学

ヨハネス・フェルスト、QBN

ファーン・ワトソン、英国金融行動監視機構

附属書 II 用語集

冷原子：レーザーとドップラー効果を用いた技術で極低温まで冷却された原子である。これらは冷原子量子コンピュータと呼ばれる特定の量子コンピュータに用いられる。使用される原子は中性原子（イオン化されていない）であり、アルカリ金属であるルビジウムがよく用いられる。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

極低温技術：冷却技術のこと。超伝導量子ビットや電子スピン量子ビットを用いたコンピュータでは、極低温冷却技術が用いられる。 量子ビットを安定化させ誤り率を低減するために必要な温度は、絶対零度に近い約 15 ミリケルビンである。最も一般的に使用されるシステムは、ヘリウム 3 とヘリウム 4 を用いた希釈冷凍機である。極低温技術は光子発生装置や光子検出システムにも用いられるが、その場合は 2K から 10K というより高い温度帯となる。

出典：Understanding Quantum Technologies 2024、Olivier Ezratty、2024 年。

暗号の敏捷性：NIS 協力グループロードマップで定義されているように、暗号プロトコルおよびシステムをモジュール式に設計し、暗号コンポーネントの交換を可能にするもの。

出典：NIS Cooperation Group (2024)、Roadmap for the Transition to 耐量子 Cryptography。

暗号部品表（CBOM）：CBOM は、暗号資産とその依存関係を記述するためのオブジェクトモデルである。これは、アルゴリズム、鍵の長さ、証明書、その使用方法など、製品やシステムで使用されるすべての暗号資産のインベントリまたはリストである。

出典：IBM、ETSI Quantum Safe Cryptography Conference 2024。

暗号関連量子コンピュータ：CRQC は、現代の暗号システムを破壊または大幅に弱体化させるほど強力な量子コンピュータである。つまり、CRQC は、従来のコンピュータでは実行不可能な攻撃（ショーのアルゴリズムなど）を実行できる量子コンピューティングシステムであり、広く使用されている公開鍵暗号およびデジタル署名方式を損なうものである。

出典: CEPS タスクフォース報告書

量子もつれ：量子現象の一つで、二つの量子物体が互いに関連し合う状態を指す。この状態では、二つの物体に対して測定を行うと、相関した（ただしランダムな）値が生成される。このプロセスは量子コンピュータにおいて、2 つまたは 3 つの量子ビットを量子ゲートで連結するために用いられる。また量子暗号や、QKD におけるもつれた光子に基づく通信システムにも利用される。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

エントロピー：物理系の無秩序さとランダムさの度合いを測る。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

ゲートベース量子コンピューティング：量子ビットと量子回路に基づく量子コンピューティングシステムのより広範なカテゴリーであり、1、2、3 量子ビットに対して同時に量子ゲートを実装する。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

グローバー（アルゴリズム）：インデックスのない配列内の要素、あるいはオラクル機能が 1 を返す唯一の要素を見つけるための量子アルゴリズムである。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

ハードウェアセキュリティモジュール：HSM はデータを保護するための暗号操作を実行し、外部物理インターフェース上でこれらの操作を利用するための特定の機能を提供する。

出典: BSI, VS-Anforderungsprofile 2024.

ハイブリッド暗号化：複数の暗号学的入力を組み合わせるあらゆる戦略を包括する、文脈認識型かつ技術的に包括的なアプローチを指す。

出典：タスクフォース報告書。

イオン：正または負の電荷を持つ非中性原子である。電子数が陽子数を上回れば負（陰イオン）、逆の場合は正（陽イオン）となる。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

鍵カプセル化機構（KEM）：特定の条件下で、2 つの当事者が公開チャネルを介して共有秘密鍵を確立するために使用できるアルゴリズム群である。KEM を用いて安全に確立された共有秘密鍵は、対称鍵暗号アルゴリズムと共に使用され、暗号化や認証といった安全なコミュニケーションの基本的なタスクを実行できる。

出典: NIST FIPS 203

論理量子ビット：ハードウェアおよびソフトウェアによる量子誤り訂正を実装した物理量子ビットの集合体である。ソフトウェア開発者の視点から見ると、非常に低い誤り率を持つ仮想的な論理量子ビットを生成する。論理量子ビットの忠実度は、含まれる物理量子ビットの数、誤り訂正コードの品質、そして物理量子ビット数の増加に伴う量子ビットの忠実度安定性に依存する。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

ノイズの多い中間規模量子（NISQ）：NISQ とは、現在のゲートベース量子コンピュータおよび近い将来のものを指す名称である。量子ビット数が中間規模（数十から数百）であり、能力を制限する量子ノイズの影響を受ける。この頭字語はジョン・プレスキルによって考案された。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

クローン禁止定理：量子状態の同一複製を禁じる。したがって、元の量子ビットから独立して利用するためにその状態を複製することは不可能だ。いかなる複製も原本を破壊する。

量子技術の理解 2024、オリヴィエ・エズラティ、2024 年。

光子：電波（長波、低周波）から可視光線を経てガンマ線（極短波、超高周波）に至る電磁波に関連するエネルギーの量子である。質量はゼロである。スピンは 1 であり、したがってボゾンの仲間である。光子は原子によるエネルギー準位の変化の際に吸収され、また放出される。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

耐量子暗号：PQC とは量子コンピューターによる暗号解読アルゴリズムに耐性を持つ暗号技術である。従来型・量子コンピューターのいずれでも分解不可能な公開鍵の使用を基盤とする。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

秘密鍵：秘密鍵暗号システムで使用される鍵である。鍵は事前に、暗号化アルゴリズム（ハッシュやディフィー・ヘルマン方式など）を用いて当事者間で交換される。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

公開鍵：相手方に公開鍵を送信し、その鍵で相手から送られてくるメッセージを暗号化する方式。この公開鍵の作成に使用された要素は、送信されたメッセージの復号に用いられる。通常、公開鍵を分解して作成要素を特定することは不可能か極めて困難である。PQC は公開鍵に基づいている。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

量子鍵配送：量子もつれ（光ファイバーまたは衛星）に基づく光リンクを介して対称鍵を安全に送るプロトコルである。これらの鍵は改ざん防止性を持つ、あるいは少なくとも鍵の傍受は検知可能である。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

量子乱数生成器：QRNG は量子暗号で使用される光学的乱数生成器であり、スイスの IDQ 社の製品などが該当する。

出典:『Understanding Quantum Technologies 2024』オリヴィエ・エズラティ著、2024 年。

量子優位性：量子コンピュータが、実用的なアルゴリズムを用いて、スーパーコンピュータに最適化された処理よりも高速に処理を実行する場合に生じる。この優位性は、計算時間以外の側面で現れることもある。例えば、量子エネルギー優位性は、計算時間ではなくエネルギー消費に関連するものだ。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024

量子ビット（qubit）または物理量子ビット：量子コンピューティングにおける量子コンピューターや量子通信の基礎的な情報単位である。粒子や量子系（電子スピン、超伝導ループのエネルギー準位、閉じ込められた原子やイオンのエネルギー準位、光子の偏光やその他の特性）の二つの異なる状態を関連付ける量子状態を保持する。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

RSA：2 つの巨大な素数を乗算して形成された公開鍵の因数分解の難度に基づく公開鍵暗号システムである。この因数分解は理論上、ショーアの量子アルゴリズムで可能である。しかし、最も一般的な 1024 ビットまたは 2048 ビットの RSA 鍵を破るには、膨大な数の量子ビットが必要となる。 2048 ビット鍵の場合、99.9%以上の忠実度を持つ 2000 万個の物理量子ビットが必要であり、これは量子コンピュータのロードマップにおいて非常に長期的な目標である。

出典:『Understanding Quantum Technologies 2024』, Olivier Ezratty, 2024 年

ショア（アルゴリズム）：1994 年にピーター・ショアが考案した整数量子因数分解アルゴリズム。理論上、RSA 公開鍵を素因数分解することで破ることが可能となる。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

ソフトウェア部品表（SBOM）：ソフトウェア製品に含まれる全てのコンポーネントと依存関係、およびそれらの出所を記載した正式な記録である。ソフトウェアの「原材料リスト」に相当し、オープンソースライブラリ、モジュール、その他ソフトウェアに含まれるサードパーティ製または独自開発のコンポーネントを網羅する。SBOM はソフトウェア構成を明示化することで、更新やコンプライアンス対応を容易にする。

出典: CISA

対称性：物理的性質が、空間回転、平行移動、鏡像反転、時間反転などの特定の変換をシステムに適用しても変化しない状況を指す。対称性は物理学の保存則と深く結びついており、エネルギー、運動量、角運動量などの特定の量が特定の変換下で不変であることが、それらの量の保存につながる。

出典: Understanding Quantum Technologies 2024, Olivier Ezratty, 2024.

タスクフォースの原則と指針

タスクフォースのプロセスは、専門家、（元）政治家、外交官、政策立案者、NGO、学術界、シンクタンクが数回の会合のために集められ、構造化された対話を行うものである。タスクフォース報告書は、CEPS とそのパートナーが独立して、またタスクフォースの枠組みの中で実施した研究の最終成果物である。

タスクフォースの参加者

■　議長は専門家であり、会議中の議論を主導し、タスクフォースの活動全般の運営について CEPS に助言する。

■　メンバーは独立した専門家として意見を提供する。

■　報告者は CEPS の研究者であり、タスクフォースを組織し、独立して研究を行い、最終報告書をドラフトする。

タスクフォース報告書の目的

■　タスクフォース報告書は、入手可能なデータ、文献、見解に基づき、バランスの取れた議論を提示することで政策論議に貢献することを目的とする。

■　報告書は読者に建設的な議論の基盤を提供することを目指す。特定の立場を押し付けたり、主題の複雑さを歪曲したりすることを意図していない。

■　タスクフォース報告書は教育的な目的も果たし、専門用語を使わず、技術用語は完全に定義した上で、理解しやすい形でドラフトされる。

報告書のドラフト

■　タスクフォース報告書はメンバーの見解を反映している。

■　ただし、報告書に記載されるすべての推奨事項について、タスクフォースメンバー間の合意や広範な合意が必ずしも必要ではない。重大な異論を招いた推奨事項は、その旨を明記する。

■　タスクフォース報告書には、報告責任者が関連性と正確性を認めたデータが掲載される。他のタスクフォースメンバーとの協議を経て、報告責任者はデータの除外、あるいは本文中での懸念事項の言及のいずれかを決定することがある。