3. サイバーセキュリティ枠組みのマッピング

表 1 は、量子耐性アルゴリズムへの移行をサポートするツールと CSF のマッピングを示す。ツールの安全な運用に必要な CSF 成果と、プラットフォームがサポートする CSF 成果の両方を含む。現在の PQC 移行プロジェクトは暗号システムの運用利用を伴わず、制御された環境下での実験室での実証と測定のみを対象としていることに留意すること。その結果、多くの組織的・運用上のセキュリティ目標は、本論文のマッピングには適用されない。

表 1 アーキテクチャと CSF のマッピング

論理アーキテクチャコンポーネント（実証済み PQC 機能）	コンポーネントの機能	機能と CSF サブカテゴリーの関係（および関係特性）	関係の説明
発見およびインベントリツール			
暗号化データ収集ツール	デジタルフットプリント内に展開された技術やシステムをスキャンし、暗号化を検出するために使用されるセンサー。スキャン対象の技術には、ホスト（ファイルシステム、バイナリデータ、実行中のプロセス、証明書ストアなど）、ネットワークインターフェース、CI/CD パイプライン、アプリケーションリポジトリ、鍵管理システム、PKI システム、HSM システムが含まれる。	**ID.AM01** をサポートする（前提条件）：組織が管理するハードウェアのインベントリを維持する	暗号データの収集は、暗号インベントリ構築の第一歩である。このインベントリは、組織が依存する PQC セキュリティサービスの継続的な妥当性を理解するために必要である。
		ID.AM02 をサポートする（前提条件）：組織が管理するソフトウェア、サービス、システムのインベントリが維持されている	
		ID.AM07 をサポートする（前提条件）：指定されたデータタイプに対応するデータ及びメタデータのインベントリが維持される	
暗号資産管理ツール	組織が、暗号鍵、キーストア、X.509 証明書、暗号ライブラリ、暗号アルゴリズム、暗号プロトコルなど、デジタルフットプリント全体に展開されている全ての暗号資産の包括的な集中管理インベントリを構築することを可能にする製品。	**ID.AM-01** をサポートする（不可欠要素）：組織が管理するハードウェアのインベントリが維持されている	暗号資産管理ツールは、HSM や暗号ハードウェアモジュールを含む全ての暗号資産について、組織が包括的な集中管理型インベントリを構築することを可能にする。
		ID.AM-02 をサポートする（不可欠要素）組織が管理するソフトウェア、サービス、システムのインベントリを維持する。	暗号資産管理ツールは、組織が管理する全てのソフトウェア、サービス、システムにおける暗号資産（暗号鍵、キーストア、X.509 証明書、暗号ライブラリ、暗号アルゴリズム及びプロトコルを含む）の包括的な集中管理型インベントリ構築を可能にする。
		ID.AM-07 をサポートする（不可欠要素）：指定されたデータタイプに対応するデータおよびメタデータのインベントリが維持される	暗号資産管理ツールは、組織がすべての暗号データと対応するメタデータの包括的な集中管理型インベントリを構築・維持することを可能にする。

論理アーキテクチャコンポーネント（実証済み PQC 機能）	コンポーネントの機能	機能と CSF サブカテゴリーの関係（および関係特性）	関係の説明
暗号解析ツール	暗号インベントリを検証し、ポリシーに基づいて暗号の脆弱性、コンプライアンスのギャップ、量子脆弱性のあるオブジェクトを識別する製品。設定可能なポリシーに基づきセキュリティおよび暗号情報を抽出し、処理環境のスナップショットを提供するプロバイダ。プロセッサやアプリケーションが管理する鍵の詳細情報を提供し、安全でない鍵、アルゴリズム、有効化されたサービスの識別をサポートする。	**GV.PO-01** にサポートされる（不可欠要素）サイバーセキュリティリスク管理ポリシー。組織の文脈、サイバーセキュリティ戦略、優先事項に基づいてサイバーセキュリティリスク管理ポリシーが確立され、伝達され、実施される。	暗号解析ツールは、組織のサイバーセキュリティポリシーに基づき、暗号資産を検証し、暗号の脆弱性、コンプライアンスのギャップ、量子脆弱性のあるオブジェクトを特定する。セキュリティおよび暗号情報の抽出プロセスは、設定可能なポリシーに基づいている。
		ID.RA-01 をサポートする（例示）：資産の脆弱性を識別、妥当性確認、記録する	暗号解析ツールは暗号資産を調査し、暗号の脆弱性、コンプライアンスの欠如、量子脆弱性を持つオブジェクトを識別する。
		ID.RA-05 にサポートされる（例示）**：** 脅威、脆弱性、発生可能性、影響を用いて固有リスクを理解し、リスク対応の優先順位付けに反映する	耐量子暗号の リスクアセスメントに内在する脅威、脆弱性、発生可能性、影響は、暗号解析ツールの出力を基に判断される。
		PR.AA-01 にサポートされる（例示）：認可されたユーザー、サービス、ハードウェアの識別情報と認証情報は組織によって管理される	暗号解析ツールは、運用上実装された場合、認可されたユーザー、サービス、ハードウェアの認証情報の完全性を損なう可能性のある暗号的弱点、コンプライアンスのギャップ、および／または量子脆弱性のあるオブジェクトを識別する。これらは組織によって管理される。
		PR.AA-02 をサポートする（例示）：相互作用の文脈に基づき、身元が証明され認証情報に紐付けられる	暗号解析ツールは、運用上実装された場合に、アイデンティティと認証情報の紐付けの完全性を損なう可能性のある暗号の脆弱性、コンプライアンスのギャップ、および量子脆弱性のあるオブジェクトを識別する。
		PR.AA-03 をサポートする（例示）：ユーザー、サービス、ハードウェアは認証される	暗号解析ツールは、認証メカニズムにおける暗号 の脆弱性とコンプライアンス上の欠陥を識別する。これらは運用段階で実装された場合、認証プロセスの完全性を損なう可能性がある。
		PR.AA-04 をサポートする（例示）：アイデンティティ主張は保護され、伝達され、検証される	暗号解析ツールは、運用上実装された場合にアイデンティティ主張の完全性を損なう可能性のある暗号的脆弱性、コンプライアンス上の不備、

論理アーキテクチャコンポーネント（実証済み PQC 機能）	コンポーネントの機能	機能と CSF サブカテゴリーの関係（および関係特性）	関係の説明
			および／または量子脆弱性を持つオブジェクトを識別する。
		PR.AA-05 をサポートする（例示）：アクセス許可、権限、認可はポリシーで定義され、管理、施行、レビューされ、最小権限の原則と職務分離の原則を取り入れている	暗号解析ツールは、運用上実装された場合にポリシーで定義された認可の強制を低下させる可能性のある、暗号の脆弱性、コンプライアンスのギャップ、および量子脆弱性を持つオブジェクトを識別する。
		PR.DS-01 サポートをサポートする（例示）：保存データの機密性、完全性、可用性が保護される	暗号解析ツールは、運用上実装された場合に保存データの機密性、完全性、可用性を低下させる可能性のある暗号の脆弱性、コンプライアンスのギャップ、量子脆弱性のあるオブジェクトを識別する。
		PR.DS-02 をサポートする（例示）を：転送中のデータの機密性、完全性、可用性が保護される	暗号解析ツールは、運用上実装された場合に転送中データの機密性、完全性、可用性を低下させる可能性のある暗号の脆弱性、コンプライアンスの欠如、および／または量子脆弱性のあるオブジェクトを識別する。
		PR.DS-10: 使用中のデータの機密性、完全性、可用性が保護されている	暗号解析ツールは、運用上実装された場合に使用中のデータの機密性、完全性、可用性を低下させる可能性のある暗号の脆弱性、コンプライアンスの欠如、および／または量子脆弱性のあるオブジェクトを識別する。
		PR.DS-11: 使用中のデータのバックアップが作成され、保護され、維持され、テストされる	暗号解析ツールは、 の暗号的脆弱性、コンプライアンス上の不備、および量子脆弱性を持つオブジェクトを識別する。これらが運用上実装された場合、データバックアップの保護を低下させる可能性がある。
証明書発見・管理ツール	デジタル証明書の脆弱性や非準拠を識別するため、集中管理による可視性、ガバナンス、ライフサイクル自動化を提供する証明書検出・ライフサイクル自動化ツール。	**GV.PO-01 にサポートされる（**不可欠要素）：サイバーセキュリティリスク管理方針によってサポートされる組織の文脈、サイバーセキュリティ戦略、優先事項に基づいてサイバーセキュリティリスク管理方針が確立され、伝達され、実施される。	証明書発見およびライフサイクル自動化ツールは、組織のポリシーに従って脆弱な証明書や準拠していない証明書を識別する。

論理アーキテクチャコンポーネント（実証済み PQC 機能）	コンポーネントの機能	機能と CSF サブカテゴリーの関係（および関係特性）	関係の説明
		ID.RA-05 にサポートされる（例示）：脅威、脆弱性、発生可能性、影響を用いて固有リスクを理解し、リスク対応の優先順位付けに反映する。	耐量子リスクアセスメントに内在する脅威、脆弱性、発生可能性、影響は、脆弱な証明書や非準拠証明書を特定する証明書発見ツールの出力を基に把握される。
		PR.IR01 サポートさえる（不可欠要素）： ネットワークと環境を不正な論理的アクセスや使用から保護されている。	分析結果の完全性は、プロジェクト施設およびネットワークへのアクセス管理に依存する。プログラムやプロセスへの不正アクセスは、誤った結果を招く可能性がある。
耐量子暗号の実装			
量子対応アルゴリズム実装	PQC アプリケーションおよびライブラリ。	**GV.PO-01** サポートされている（不可欠要素）：サイバーセキュリティリスク管理方針は、組織の文脈、サイバーセキュリティ戦略、優先事項に基づいて確立され、伝達され、実施される。	暗号アルゴリズムとライブラリの選定および実装は、組織の文脈、サイバーセキュリティ戦略、優先順位に基づくポリシーによって制約される。
		PR.AA-01 をサポートする（例示）：認可されたユーザー、サービス、ハードウェアの識別情報と認証情報は組織によって管理される。	量子対応アルゴリズム実装の成功した実証は、量子脆弱性アルゴリズムの代替手段の実装可能性を示す。量子脆弱性アルゴリズムの使用は、組織が管理する認証情報（ ）の完全性を危険にさらす可能性がある。
		PR.AA-02 をサポートする（例示）：相互作用の文脈に基づき、身元が証明され認証情報に紐付けられる	量子対応アルゴリズムの実装が成功裏に実証されたことで、量子脆弱性を持つアルゴリズムの代替手段の実装可能性が示された。量子脆弱性を持つアルゴリズムの使用は、身元と認証情報の結びつきの完全性を危険にさらす可能性がある。
		PR.AA-03 をサポートする（例示）：ユーザー、サービス、ハードウェアは認証される	量子対応アルゴリズムの実装が成功裏に実証されたことで、認証目的において量子脆弱性を持つアルゴリズムの代替手段を実装する可能性が示された。
		PR.AA-04 をサポートする（例示）：身元主張は保護され、伝達され、検証される	量子対応アルゴリズムの実装成功は、量子脆弱性アルゴリズムの代替手段の実装可能性を示す。量子脆弱性アルゴリズムの使用は、 身元

論理アーキテクチャコンポーネント（実証済み PQC 機能）	コンポーネントの機能	機能と CSF サブカテゴリーの関係（および関係特性）	関係の説明
			主張の完全性を危険にさらす可能性がある。
		PR.AA-05 をサポートする（例示）：アクセス許可、権限、認可はポリシーで定義され、管理、強制、レビューされ、最小権限と職務分離の原則を組み込んでいる	量子対応アルゴリズムの実装が成功裏に実証されたことで、量子脆弱性を持つアルゴリズムの代替手段の実装可能性が示された。量子脆弱性を持つアルゴリズムの使用は、アクセス許可と認可の完全性を危険にさらす可能性がある。
		PR.DS-01 をサポートする（前提条件）：保存データの機密性、完全性、可用性が保護される	量子対応アルゴリズム実装の成功した実証は、量子脆弱性アルゴリズムの代替手段の実装可能性を示す。量子脆弱性アルゴリズムの使用は、保存データの機密性、完全性、可用性を危険にさらす可能性がある。
		PR.DS-02 をサポートする（前提条件）：転送中のデータの機密性、 完全性、可用性が保護される	量子対応アルゴリズム実装の成功した実証は、 量子脆弱性アルゴリズムの代替手段の実装可能性を示す。量子脆弱性アルゴリズムの使用は、転送中のデータの機密性、完全性、可用性を危険にさらす可能性がある。
		PR.DS-10: 使用中のデータの機密性、完全性、可用性が保護されている	量子対応アルゴリズムの実装が成功裏に実証されたことで、量子脆弱性のあるアルゴリズムの代替手段の実装可能性が示された。量子脆弱性のあるアルゴリズムの使用は、使用中のデータの機密性、完全性、可用性を危険にさらす可能性がある。
		PR.DS-11: データのバックアップが作成、保護、維持、テストされる	量子耐性アルゴリズムの実装の成功した実証は、量子脆弱性アルゴリズムの代替手段の実装可能性を示している。量子脆弱性アルゴリズムの使用は、データおよびプログラムバックアップの機密性と完全性を危険にさらす可能性がある。
		PR.PS-01 にサポートされる（不可欠要素）：構成管理の実践が確立され適用されている。	構成管理は、アルゴリズム実装の相互運用性テストの効果性と時間的有効性、およびアルゴリズム実装の性能テストの時間的有効性にとって必要である。
		PR.PS-05 にサポートされる（不可欠要素）：不正なソフトウェアのインストールと実行を防止する	アルゴリズム実装性能テスト結果の継続的な正確性は、不正なソフトウェアの実行を防止することに依存する。

論理アーキテクチャコンポーネント（実証済み PQC 機能）	コンポーネントの機能	機能と CSF サブカテゴリーの関係（および関係特性）	関係の説明
		PR.IR01 にサポートされる（不可欠要素）：（ネットワークと環境を不正な論理的アクセスや使用から保護する	解析結果の完全性は、プロジェクト施設およびネットワークへのアクセス管理に依存する。プログラムやプロセスへの不正アクセスは、相互運用性や性能に関する誤った結果を招く可能性がある。
		GV.PO-01 にサポートされる（不可欠要素）：サイバーセキュリティリスク管理方針は組織の文脈、サイバーセキュリティ戦略、優先事項に基づいて確立され、伝達され、実施される。	通信プロトコル、プロトコルプログラミングインターフェース、ID 管理プロトコルを含むプロトコルの選択と実装は、組織のサイバーセキュリティポリシーによって制約される。
量子耐性暗号サービス実装	耐量子暗号の実装、および／または PQC をサポートするプロトコルの実装。これには通信プロトコル、プロトコルプログラミングインターフェース、アイデンティティ管理プロトコルが含まれる。	**PR.AA-01** をサポートする（例示）：認可されたユーザー、サービス、ハードウェアの識別情報と認証情報は組織によって管理される。	量子対応暗号サービス実装の成功した実証は、認可されたユーザー、サービス、ハードウェアへの認証情報提供において公開鍵暗号を使用する量子脆弱性サービスへの代替手段の実装可能性を示すことができる。
		PR.AA-02 をサポートする（例示）相互作用の文脈に基づいて身元が証明され、認証情報に紐付けられる。	量子対応暗号サービス実装の成功した実証は、量子脆弱性を持つサービスに代わる代替手段の実現可能性を示す。この代替手段は、耐量子環境において公開鍵暗号を用いて身元情報を認証情報に紐付けるものである。
		PR.AA-03 をサポートする（例示）：ユーザー、サービス、ハードウェアは認証される	の量子対応暗号サービス実装において、認証プロセスで公開鍵暗号が使用される成功した実証は、量子脆弱な認証サービスに代わる量子耐性のある代替手段の実装可能性を示すことができる。
		PR.AA-04 をサポートする（例示）：身元主張は保護され、伝達され、検証される	量子対応暗号サービス実装の成功した実証は、公開鍵暗号を用いて身元主張を保護する量子脆弱性サービスへの代替手段の実装可能性を示すことができる。
		PR.AA-05 をサポートする（例示）：アクセス許可、権限、認可はポリシーで定義され、管理、施行、レビューされ、の最小権限と職務分離の原則を取り入れる	量子対応暗号サービス実装の成功した実証は、アクセス許可、権限付与、認可の強制に公開鍵暗号を用いる量子脆弱性サービスへの代替手段の実装可能性を示すことができる。

論理アーキテクチャコンポーネント（実証済み PQC 機能）	コンポーネントの機能	機能と CSF サブカテゴリーの関係（および関係特性）	関係の説明
		PR.DS-01 をサポートする（前提条件）：保存データの機密性、完全性、可用性が保護される	量子対応暗号サービス実装の成功した実証は、保存データの機密性、完全性、可用性を危険にさらす可能性のある量子脆弱性サービスへの代替手段の実装可能性を示す。影響を受けるサービスには、プログラミングインターフェース、ファイル暗号化、鍵変数保存、ファイル暗号化が含まれる。
		PR.DS-02 をサポートする（前提条件）：転送中のデータの機密性、完全性、可用性が保護される	量子対応暗号サービス実装の成功した実証は、量子脆弱性を持つサービスの代替手段の実装可能性を示している。これらのサービスの使用は、転送中のデータの機密性、完全性、可用性を危険にさらす可能性がある。影響を受けるサービスには、通信プロトコル、鍵確立プロトコル、 プロトコル、プロトコルプログラミングインターフェース、および ID 管理プロトコルが含まれる。
		PR.DS-10 をサポートする（前提条件）：使用中のデータの機密性、完全性、可用性が保護される	量子対応暗号サービス実装の成功した実証は、量子脆弱性を持つサービスの代替手段の実装可能性を示すものである。これらのサービスの使用は、使用中のデータの機密性、完全性、可用性を危険にさらす可能性がある。
		PR.DS11 をサポートする（前提条件）：データのバックアップが作成、保護、維持、テストされる	量子対応暗号サービス実装の成功した実証は、量子脆弱性を持つサービスの代替手段の実装可能性を示す。これらのサービスの使用は、データおよびプログラムバックアップの機密性と完全性を危険にさらす可能性がある。
		PR.PS-01 にサポートされる（不可欠要素）構成管理の実践が確立され適用されること）によって支えられる	構成管理は、相互運用性テストの効果性と時間的有効性、ならびに量子耐性暗号サービス実装の性能テストの時間的有効性にとって必要である。
		PR.PS-05 にサポートされる（不可欠要素）：不正なソフトウェアのインストールと実行は防止される	暗号サービス実装の性能試験結果の継続的な正確性は、不正なソフトウェアの実行を防止することに依存する。
		PR.IR01 にサポートされる（不可欠要素）ネットワークと環境を不正	解析結果の完全性は、プロジェクト施設およびネットワークへのアクセス管理に依存する。プログラムやプロセ

論理アーキテクチャコンポーネント（実証済み PQC 機能）	コンポーネントの機能	機能と CSF サブカテゴリーの関係（および関係特性）	関係の説明
		な論理的アクセスおよび使用から保護する	スへの不正アクセスは、相互運用性や性能に関する誤った結果を招く可能性がある。
量子対応統合ツールおよびアプリケーションプラグイン	暗号ツールキット、ネットワークインフラ、セキュリティインフラ（PKI、HSM、ブロックチェーン）、プロキシ／コネクタ、メッセージングツール、 ウェブアプリケーションサーバーおよびクライアント向けの、耐量子および／またはポスト量子ハイブリッド化対応の統合ツールとアプリケーションプラグイン。	**GV.PO-01** にサポートされる（不可欠要素）サイバーセキュリティリスク管理方針は組織の文脈、サイバーセキュリティ戦略、優先事項に基づいて確立され、 伝達され、実施される。	暗号ツールキット、ネットワークインフラ、セキュリティインフラ（PKI、HSM、ブロックチェーン）、プロキシ/コネクタ、メッセージングツール、 ウェブアプリケーションサーバーおよびクライアント向けの耐量子および／またはポスト量子ハイブリッド化対応統合ツールとアプリケーションプラグインの選定と実装は、組織のサイバーセキュリティポリシーによって制約される。
		PR.AA-01 をサポートする（例示）：認可されたユーザー、サービス、ハードウェアの識別情報と認証情報は組織によって管理される	量子対応統合ツールとアプリケーションプラグインの実証成功は、量子脆弱性暗号の代替手段導入の実現可能性を示す。量子脆弱性暗号の使用は、アイデンティティ認証情報の完全性を危険に晒す可能性がある。
		PR.AA-02 をサポートする（例示）：身元確認は相互作用の文脈に基づいて行われ、認証情報に紐付けられる	量子対応統合ツールとアプリケーションプラグインの成功した実証は、公開鍵暗号がアイデンティティと認証情報の紐付け保護に使用される量子脆弱暗号の代替手段実装の実現可能性を示す。
		PR.AA-03 をサポートする（例示）：ユーザー、サービス、ハードウェアは認証される	量子対応統合ツールとアプリケーションプラグインの成功した実証は、量子脆弱暗号の代替手段として、 公開鍵暗号を用いた認証を実装する可能性を示すことができる。
		PR.AA-04 をサポートする（例示）：身元主張は保護され、伝達され、検証される	量子対応統合ツールとアプリケーションプラグインの成功した実証は、量子脆弱暗号の代替手段として、公開鍵暗号を用いてアイデンティティ主張の保護を行う方式の実装可能性を示すことができる。
		PR.AA-05 をサポートする（例示）：アクセス権限、権限付与、認可はポリシーで定義され、管理、施行、レビューされ、最小権限の原則と職務分離の原則を取り入れる	量子対応統合ツールおよびアプリケーションプラグインの成功した実証は、アクセス許可、権限、認可の保護に公開鍵暗号が使用される量子脆弱暗号の代替手段を実装する実現可能性を示すことができる。

論理アーキテクチャコンポーネント（実証済み PQC 機能）	コンポーネントの機能	機能と CSF サブカテゴリーの関係（および関係特性）	関係の説明
		PR.DS-01 をサポートする（前提条件）：の保存データ（data-at-rest）の機密性、完全性、可用性が保護される	量子対応統合ツールおよびアプリケーションプラグインの成功した実証は、 における量子脆弱性暗号の代替手段の実装可能性を示す。その使用は保存データの機密性、完全性、可用性を危険にさらす可能性がある。
		PR.DS-02 をサポートする（前提条件）：転送中のデータの機密性、完全性、可用性が保護されている	量子対応統合ツールおよびアプリケーションプラグインの実証成功は、量子脆弱性サービスへの代替手段の実装可能性を示す。量子脆弱性サービスの使用は、転送中データの機密性、完全性、可用性を危険にさらす可能性がある。
		PR.DS-10: 使用中のデータの機密性、完全性、可用性が保護されている	量子対応統合ツールとアプリケーションプラグインの実証成功は、量子脆弱性サービスへの代替手段の実装可能性を示している。これらのサービスの利用は、使用中のデータの機密性、完全性、可用性を危険にさらす可能性がある。
		PR.DS-11: データのバックアップが作成され、保護され、維持され、テストされる	量子対応統合ツールとアプリケーションプラグインの成功した実証は、 量子脆弱性を持つサービスの代替手段の実装可能性を示す。これらのサービスの使用は、バックアップの機密性と完全性を危険にさらす可能性がある。
		PR.IR01: にサポートされる（不可欠要素）ネットワークと環境は不正な論理的アクセスおよび使用から保護されている。	分析結果の完全性は、プロジェクト施設およびネットワークへのアクセス管理に依存する。プログラムやプロセスへの不正アクセスは、相互運用性や性能に関する誤った知見をもたらす可能性がある。
量子対応認証局の実装	耐量子および／またはポスト量子ハイブリッド化対応の X.509 認証局。	**GV.PO-01 にサポートされる（不可欠要素）**（組織の文脈、サイバーセキュリティ戦略、優先事項に基づきサイバーリスク管理方針を確立し、伝達・実施する。	耐量子および／または耐量子ハイブリッド化対応の X.509 認証局の選択は、組織のサイバーセキュリティポリシーによって制約される。
量子対応ハードウェアセキュリティモジュール（HSM）	耐量子および／または耐量子ハイブリッド化対応の 鍵確立・保管メカニズムであり、組み込みの量子耐性暗号機能を提供する。	**ID.RA-03** にサポートされる（例示）：組織に対する内部および外部の脅威を識別し記録する	量子対応アルゴリズム 実装に対する内部・外部脅威の特定は、HSM の要件定義と選定に資する。

論理アーキテクチャコンポーネント（実証済み PQC 機能）	コンポーネントの機能	機能と CSF サブカテゴリーの関係（および関係特性）	関係の説明
		PR.AA-01 をサポートする（例示）：認可されたユーザー、サービス、ハードウェアの識別情報と認証情報は組織によって管理される	量子対応 HSM の実証成功は、量子脆弱性を持つ暗号情報とプロセスの物理的保護の実現可能性を示す。これらが侵害されると、認証情報の完全性が脅かされる。
		PR.AA-02 をサポートする（例示）：身元は相互作用の文脈に基づき証明され、認証情報に紐付けられる	量子対応 HSM の成功した実証は、公鍵メカニズムを用いた ID と認証情報の紐付けに関連する量子脆弱性情報、そしておそらくプロセスそのものを物理的に保護する実現可能性を示している。
		PR.AA-03 をサポートする（例示）：ユーザー、サービス、ハードウェアは認証される	量子対応 HSM の成功した実証は、認証に使用される情報の物理的保護、および その情報を使用するプロセスの物理的保護の実現可能性を示す。
		PR.AA-04 をサポートする（例示）：身元主張は保護され、伝達され、検証される	量子対応 HSM の成功した実証は、認証メカニズムにおいて、またはそれによって使用される情報を物理的保護する実現可能性を示す。
		PR.AA-05 をサポートする（例示）：アクセス権限、権限付与、認可はポリシーで定義され、管理、施行、レビューされ、最小権限の原則と職務分離の原則を取り入れている	量子対応 HSM の成功した実証は、アクセスおよび認可の強制に用いられる情報を物理的に保護する実現可能性を示す。
		PR.DS-01 をサポートする（前提条件）保存データの機密性、完全性、可用性を保護する。	量子対応 HSM の成功した実証は、量子脆弱性を持つ暗号化コンポーネントに対する物理的保護の実現可能性を示す。これらのコンポーネントのエクスポージャーにより、 における保存データの機密性、完全性、可用性が危険に晒される可能性がある。
		PR.DS-02 をサポートする（前提条件）転送中データの機密性、完全性、可用性が保護される	量子対応 HSM の実証成功は、量子脆弱性を持つ暗号情報とプロセスを物理的に保護する実現可能性を示している。これらがエクスポージャーされると、データ転送中の機密性、完全性、可用性が危険に晒される。
		PR.DS-10: 使用中のデータの機密性、完	量子対応 HSM の成功した実証は、量子脆弱な暗号情報とプロセスを物理的に保護する実現可能性を

論理アーキテクチャコンポーネント（実証済み PQC 機能）	コンポーネントの機能	機能と CSF サブカテゴリーの関係（および関係特性）	関係の説明
		全性、可用性が保護される	示している。これらがエクスポージャーされると、使用中のデータの機密性、完全性、可用性が危険にさらされる可能性がある。
		PR.DS-11: データのバックアップが作成され、保護され、維持され、テストされる	量子対応 HSM の成功した実証は、量子脆弱な暗号情報とプロセスを物理的に保護する実現可能性を示している。これらがエクスポージャーされると、バックアップの機密性（ ）と完全性が危険に晒される。

4. SP 800-53 マッピング

表 2 は、量子耐性アルゴリズムへの移行をサポートするツールと製品を SP 800-53 の制御項目にマッピングしたものである。ツールの安全な運用に必要な制御項目と、プラットフォームがサポートする制御項目の両方が含まれる。CSF マッピングの場合と同様に、現在の PQC 移行プロジェクトは暗号システムの運用を伴わず、制御された環境下での実験室での実証と測定のみを対象としていることに留意すること。したがって、多くの組織的・運用上のセキュリティ管理項目は適用されない。

表 2 NIST 特別刊行物 800-53 へのアーキテクチャマッピング

論理アーキテクチャコンポーネント（実証済み PQC 機能）	コンポーネントの機能	機能と SP 800-53 管理策との関係（および関係特性）	関係の説明
発見およびインベントリツール			
暗号データ収集ツール	デジタルフットプリント内に展開された技術やシステムをスキャンし、暗号技術を探知するためのセンサー。スキャン対象の技術には、ホスト（ファイルシステム、バイナリデータ、実行中プロセス、証明書ストアなど）、ネットワークインターフェース、CI/CD パイプライン、アプリケーションリポジトリ、鍵管理システム、PKI システム、HSM システムが含まれる。	**CM-8** をサポートする（不可欠要素）：システムコンポーネントインベントリ	暗号データの収集は、暗号インベントリを作成する上で不可欠要素。暗号データ収集ツールは、特に複雑なサブシステム、システム、インフラストラクチャにおいて、暗号コンポーネントの特定をサポートする。
		CM-8 をサポートする（不可欠要素）：システムコンポーネントインベントリ	
		CM-12 をサポートする（前提条件）：情報位置特定	暗号コンポーネントの発見は、コンポーネントの位置特定の前提条件である。
		CP2 をサポートする（前提条件）（強化 08）：緊急時 計画 - 重要なシステム資産を識別する	暗号化コンポーネントの発見は、重要な暗号化資産を特定するために必要である。これらの資産は、必須の任務および業務機能をサポートし、緊急時対応計画の策定に情報を提供する。
暗号資産管理ツール	組織が、暗号鍵、キーストア、X.509 証明書、暗号ライブラリ、暗号アルゴリズム、暗号プロトコルなど、デジタルフットプリント全体に展開されている全ての暗号資産の包括的な集中管理インベントリを構築することを可能にする製品。	**CM-8** をサポートする（不可欠要素）：システムコンポーネントインベントリ	暗号資産管理ツールは、HSM や暗号ハードウェアモジュールを含む全ての暗号資産の包括的な集中管理型インベントリ構築を可能にする。このインベントリは、エンタープライズの暗号コンポーネントを理解し、エンタープライズとその外部関係者が依存するポスト量子暗号セキュリティサービスの継続的な妥当性を評価するために必要である。
		CP2 をサポートする（前提条件）（強化 08）：緊急時 計画 - 重要なシステム資産を識別する	暗号資産管理ツールは、組織が HSM や暗号ハードウェアモジュールを含む全ての暗号資産、およびそれらが支える業務機能の包括的な集中管理を実現する。この は、量子コンピュータに脆弱なコンポーネントの優先的な交換と、既存の暗号技

			術の脆弱性による侵害への対応計画をサポートする。
暗号解析ツール	暗号資産をレビューし、ポリシーに基づいて暗号の弱点、コンプライアンスのギャップ、量子脆弱性のあるオブジェクトを識別する製品。設定可能なポリシーに基づき、セキュリティおよび暗号情報の抽出を行い、処理環境のスナップショットを提供するプロバイダ。プロセッサやアプリケーションが管理する鍵の詳細を提供し、安全でない鍵、アルゴリズム、有効化されたサービスの識別をサポートする。	**CA-2** をサポートする（例示）：制御アセスメント	暗号解析ツールは、暗号の脆弱性、コンプライアンスのギャップ、量子脆弱性のあるオブジェクト、プロセッサやアプリケーションが管理する鍵の詳細、安全でない鍵、アルゴリズム、有効化されたサービスの識別が可能である。これは暗号制御の評価に必要である。
		CM-8 にサポートされる（不可欠要素）：システムコンポーネントインベントリ	暗号化コンポーネントは、分析する前に識別されなければならない。
		RA-3 をサポートする（例示）リスクアセスメント	暗号解析ツールは、システムやホストアプリケーション内の暗号脆弱性を識別し、リスクアセスメントに情報を提供する。
		RA-3 にサポートされる（例示）：リスクアセスメント	リスクアセスメントは、暗号解析ツールが探すべき対象を特定し、脆弱性を識別・優先順位付けするための基礎を提供する。
		RA-5 をサポートする（例示）：脆弱性監視およびスキャンをサポートする	暗号解析ツールは、システムおよびホスト型アプリケーション内の暗号脆弱性を識別できる。
		RA-7 をサポートする（例示）**：** リスク対応	解析結果により対応と復旧が可能となる。例えば、証明書のインベントリ管理により、証明書の交換や脆弱な暗号コンポーネントの影響からの復旧が可能となる。
		SA-11 をサポートする（例示）：開発者によるテストと評価	暗号解析ツールは、脆弱なアルゴリズムや暗号コンポーネントを識別することで、開発者のテストと評価をサポートできる。
		SA-15 をサポートする（例示）開発プロセス、標準、ツール	暗号解析ツールは、脆弱なアルゴリズムや暗号コンポーネントを識別することで、システムおよびアプリケーション開発プロセスをサポートできる。
		SC- 8 をサポートする（例示）：伝送の機密性と完全性	暗号化 の脆弱性、コンプライアンスのギャップ、量子脆弱性のあるオブジェクト、プロセッサやアプリケーションが管理する鍵の詳細、安全でない鍵・アルゴリズム・有効化サービスの特定を理解することは、外部関係者が依存する耐量子暗号セキュリティサービスの適切性を把握し、移行措置

			の優先順位付けを行うために必要である。
		SC-12 をサポートする（例示）：暗号鍵の鍵確立と管理	暗号鍵の確立と管理のための暗号機能の使用事例を理解することは、脆弱性を持つアルゴリズムや鍵確立メカニズムが使用されている、あるいは設定の選択により使用される可能性があるケースの識別をサポートする。これにはプロセッサやアプリケーションが管理する鍵の詳細が含まれ、安全でない鍵、 アルゴリズム、有効化されたサービスの識別に役立つ。
		SC-13 にサポートされる（不可欠要素）：暗号保護	暗号解析ツールは、組織のサイバーセキュリティポリシーに基づき、暗号資産を検証し、暗号の脆弱性、コンプライアンスの欠如、量子脆弱性のあるオブジェクトを特定する。セキュリティおよび暗号情報の抽出プロセスは、設定可能なポリシーに基づいている。
		SC-28 をサポートする（例示）保存データの保護	暗号解析ツールは、保存状態の情報を保護するために使用される暗号コンポーネントを検証し、その保護を損なう可能性のある暗号の脆弱性、コンプライアンスのギャップ、および/または量子脆弱性のあるオブジェクトを識別する。
		SI-7（強化 06）サポートさｓれる（例示）：ソフトウェア、ファームウェア、情報完全性 – 暗号保護	暗号解析ツールが、組織に対する内部または外部の脅威を可能にする、または代表する暗号の脆弱性、コンプライアンスのギャップ、量子脆弱オブジェクトを識別する効果は、ツールとその入力データの完全性に依存する。
証明書発見・管理ツール	デジタル証明書の脆弱性や非準拠を識別するため、集中管理による可視性、ガバナンス、ライフサイクル自動化を提供する証明書検出・ライフサイクル自動化ツール。	**CM-8 をサポートする（前提条件）：**システムコンポーネントインベントリ	デジタル証明書はエンタープライズ暗号セキュリティの重要構成要素であるため、インベントリ目的での可視化が必要である。
		CP-2（強化 08）をサポートする（例示）：緊急時対応計画 – 重要資産の識別	デジタル証明書は重要なシステム資産であり、特に大規模データセンター環境において、証明書の発見とインベントリは、証明書交換と復旧のための緊急時対応計画の要素である。
		RA-3 をサポートする（例示）：リスクアセスメント	本ツールは、リスクアセスメントに有用な脆弱性に関する情報をプロバイダできる。

		RA-7 をサポートする（例示）：リスク対応	証明書の棚卸しは、証明書の交換と復旧を可能にする。
		SC-17 にサポートされる（不可欠要素）：公開鍵基盤証明書	証明書検出およびライフサイクル自動化ツールは、脆弱な証明書や準拠していない証明書を識別する。組織が依存する耐量子暗号セキュリティサービスを実施するには、デジタル証明書の集中管理による可視性、ガバナンス、 ライフサイクル自動化による脆弱な証明書や準拠していない証明書の識別が必要である。
耐量子暗号の実装			
量子対応アルゴリズムの実装	PQC アプリケーションとライブラリ。	**AC-3** をサポートする（例示）：アクセス強制	耐量子暗号アプリケーションとライブラリは、アクセス強制のための暗号メカニズムを提供する。
		CM-1 にサポートされる（不可欠要素）：構成管理方針と手順	構成管理は、アルゴリズム実装の相互運用性テストの効果性と時間的有効性、およびアルゴリズム実装の性能テストの時間的有効性にとって必要である。
		CM-3 にサポートされる（例示）：構成変更管理）	構成変更管理は、量子耐性能力の確立と維持において、暗号ライブラリの修正と管理をサポートする。
		CM-6 にサポートされる（例示）：構成設定	構成設定の管理は、PQC アプリケーションおよびライブラリの意図しない不安全な実装を防止できる。
		CM-8 にサポートされる（前提条件）：システムコンポーネントインベントリ	コンポーネントインベントリは、PQC 実装の特定と選択を容易にする。
		CM-9 にサポートされる（例示）：構成管理計画	PQC アプリケーションおよびライブラリ要素の実装には管理が必要である。これには、システムまたはサブシステムの開発ライフサイクル全体において暗号構成項目を識別し、それらの構成管理が含まれる。構成管理計画は、システム向けの暗号構成項目を定義し、それらを構成管理下に置くものである。
		CM-11: をサポートする（例示） ユーザーインストールソフトウェア	承認済みソフトウェアの識別子を用いて、ユーザーがインストールするソフトウェアを制限する。
		CM-11: にサポートされる（例示） ユーザーインストールソフトウェア	必要な権限がプロバイダによって提供されれば、ユーザーはエンタープライズシステムに暗号ソフトウェアをインストールできる。暗号セキュリティポリ

		ユーザーインストールソフトウェア	シーをサポートし、インストールされる暗号技術に対する管理を維持するため、組織は許可されたライブラリコンポーネントと禁止されたライブラリコンポーネント、およびソフトウェアインストール時に実行される暗号アプリケーションとアクションを識別する必要がある。
		IA-7 にサポートされる（例示）**:** 暗号モジュール認証	暗号アプリケーションやライブラリ要素を使用する際には、適用法、大統領令、指令、方針、規制、標準、ガイドラインで定められた要件を満たす暗号モジュールへの認証メカニズムを実装すること。
		RA-3 にサポートされる（例示）：リスクアセスメント）	暗号アプリケーションおよびコンポーネントの選定と実装は、リスクアセスメントに基づく 組織のサイバーセキュリティポリシーによって制約される。
		SC-8 をサポートする（不可欠要素）**:** 伝送の機密性と完全性	量子対応アルゴリズムの実装が成功裏に実証されたことで、量子脆弱性アルゴリズムの代替手段の実装可能性が示された。量子脆弱性アルゴリズムの使用は、転送中のデータの機密性、完全性、可用性を危険にさらす可能性がある。
		SC-12 をサポートする（不可欠要素）**:** 暗号鍵の鍵確立と管理）	耐量子暗号アプリケーションおよびライブラリは、安全な鍵伝送や鍵確立に用いられるその他の手法で使用される。
		SC-13 をサポートする（不可欠要素）**:** 暗号保護	敵対者がショアのアルゴリズムを実行可能な量子コンピュータを入手可能となった時点で、様々な形態の暗号保護に耐量子暗号アプリケーションとライブラリが必要となる。
		SC-17 にサポートされる（例示）：公開鍵 インフラストラクチャ証明書	多くの PQC 実装では、公認認証局が発行する PKI 証明書が必要となる。
		SC-28 をサポートする（不可欠要素）：保存状態の情報保護	量子対応アルゴリズム実装の成功実証は、保存データの機密性・完全性・可用性を危険に晒す量子脆弱性アルゴリズムの代替手段実装の実現可能性を示す。
		SC-40 をサポートする（例示）：無線リンク保護の	耐量子暗号の実装は、認可のないシステム利用者に可視化される可能性のある無線リンクの保護に利用できる。
		PR.PS-05 をサポートする（不可欠要素）**:**	アルゴリズム実装の性能テスト結果の継続的な正確性は、不正なソフ

		不正なソフトウェアのインストールと実行を防止する	トウェアの実行を防止することに依存する。
		SI-7 をサポートする（不可欠要素）：ソフトウェア、ファームウェア、および情報の完全性	量子対応暗号機能は、ソフトウェア、ファームウェア、情報への不正な変更を検知するために使用できる。メカニズムには、コード署名、 メッセージのデジタル署名、取引の否認防止が含まれる。
量子耐性暗号サービス実装	耐量子暗号の実装、および／または PQC をサポートするプロトコルの実装。これには通信プロトコル、プロトコルプログラミングインターフェース、アイデンティティ管理プロトコルが含まれる。	**CM-1** にサポートされる（不可欠要素）：構成管理方針および手順	構成管理は、運用実装の継続的な有効性だけでなく、相互運用性テストの時間的妥当性確認および量子耐性暗号サービス実装の性能テストの時間的妥当性確認にも必要である。
		IA-9 にサポートされる（例示）：サービス識別と認証	識別と認証を必要とする可能性のあるサービスには、暗号サービスやデジタル署名を使用するその他のアプリケーションが含まれる。システムサービスやアプリケーションの識別および認証方法には、情報またはコード署名、プロバンスグラフ、サービスの出所を示す電子署名などがある。
		RA-3 にサポートされる（例示）：リスクアセスメント	量子対応アルゴリズム実装に対する内部・外部脅威、使用制限、 潜在的な実装脆弱性の特定は、暗号サービスの選択に情報を提供できる。
		SA-2 にサポートされる（前提条件）：資源配分	サービス取得には以下が含まれる：ミッション及び業務プロセス計画における量子耐性システムサービスの高レベル暗号セキュリティ要件の決定；組織の資本計画及び投資管理プロセスの一環として、システムサービスを保護するために必要なリソースの決定、文書化、及び配分；組織のプログラミング及び予算文書における情報セキュリティとプライバシーのための個別の項目設定。
		SA-4 にサポートされる（不可欠要素）：調達プロセス	安全な処理サービスの調達契約には、耐量子セキュリティ機能要件、メカニズム強度要件、セキュリティ保証要件、セキュリティ及びプライバシー要件を満たすために必要な統制、セキュリティ文書化 要件、セキュリティ文書保護要件、システムが動作する予定の環境の説明、情報セキュリティ及びサプライチェーンリスクマネジメントの責任の配分または責任当事者の特定を含める。

		SA-9 にサポートされる（例示）**：** 外部システムサービス	外部システムサービスは外部プロバイダによって提供され、組織は必要な統制の実施を直接制御できない。外部システムサービス提供者が組織のポスト量子暗号セキュリティ要件を遵守することを要求する。外部システムサービスに関連する組織の監督およびユーザーの役割と責任を定義し文書化する。 外部サービスプロバイダによる統制遵守を継続的に監視するため、以下のプロセス、方法、技術を採用する。
		SC-8 をサポートする（不可欠要素：伝送の機密性と完全性	量子対応暗号サービス実装の成功した実証は、量子脆弱性サービスへの代替手段の実装可能性を示すものである。量子脆弱性サービスの使用は、転送中のデータの機密性、完全性、可用性を危険にさらす可能性がある。影響を受けるサービスには、通信プロトコル、鍵確立プロトコル、プロトコルプログラミングインターフェース、アイデンティティ管理プロトコルなどのプロトコルが含まれる。
		SC-13 をサポートする（不可欠要素）：保存情報保護	量子対応暗号サービス実装の成功した実証は、量子脆弱性を持つサービスの代替手段の実装可能性を示すものである。量子脆弱性を持つサービスの使用は、保存データの機密性、完全性、可用性を危険にさらす可能性がある。影響を受けるサービスには、プログラミングインターフェース、鍵変数 ストレージ、ファイル暗号化などが含まれる。
量子対応統合ツールとアプリケーションプラグイン	耐量子および／またはポスト量子ハイブリッド化対応の統合ツールとアプリケーションプラグイン、暗号ツールキット、ネットワークインフラ、セキュリティインフラ（PKI、HSM、ブロックチェーン）、プロキシ／コネクタ、メッセージングツール、Web アプリケーションサーバーおよびクライアント向け。	**AC-3** にサポートされる（例示）：アクセス強制	分析結果の完全性は、プロジェクト施設およびネットワークへのアクセス管理に依存する。プログラムやプロセスへの不正アクセスは、相互運用性や性能に関する誤った知見をもたらす可能性がある。
		CM-4 にサポートされる（例示）：影響分析	暗号ツールキット、ネットワークインフラ、セキュリティインフラ向けのアプリケーションプラグインをインストール・実装する前に、潜在的なセキュリティおよびプライバシーへの影響を分析することで、運用上およびセキュリティ上の失敗を回避できる。
		CM-5 にサポートされる（前提条件）：変更に対するアクセス制限	システム変更に伴うアクセス制限を定義、文書化、承認、実施することで、暗号アプリケーションプラグインの不正または誤ったインストールを防止できる。

		CM-11 をサポートする（例示）**:** ユーザーインストールソフトウェア	承認済みプラグインの識別子は、ユーザーインストールソフトウェアを承認済みセットに制限するための基盤として使用できる。
		CM-11 にサポートされる（例示）：ユーザーがインストールしたソフトウェア	必要な権限がプロバイダされれば、ユーザーはエンタープライズシステムに暗号化プラグインをインストールできる。暗号化セキュリティポリシーをサポートし、インストールされる暗号化技術に対する管理を維持するため、組織は許可される暗号化アプリケーションとプラグイン、禁止されるものを識別する必要がある。
		RA-3 にサポートされる（例示）：リスクアセスメント	量子耐性アルゴリズム実装に対する内部・外部脅威の特定は、暗号ツールやアプリケーションプラグインの選択に役立つ。
		SC-8 をサポートする（不可欠要素）**:** 伝送の機密性と完全性	量子対応統合ツールおよびアプリケーションプラグインの成功した実証は、量子脆弱性サービスへの代替手段の実装可能性を示す。量子脆弱性サービスの使用は、転送中のデータの機密性、完全性、可用性を危険にさらす可能性がある。
		SC-12 をサポートする（例示）**:** 暗号鍵の鍵確立と管理	量子対応アプリケーションプラグインは、安全な鍵 輸送や鍵確立に用いられるその他の手法で使用できる。
		SC-13 をサポートする（不可欠要素）：暗号保護	敵対者がショアのアルゴリズムを実行可能な量子コンピュータを入手可能となった時点で、様々な暗号保護形態に耐量子暗号アプリケーションおよびライブラリが必要となる。
		SC-28 をサポートする（不可欠要素）：保存状態の情報保護	量子対応統合ツールおよびアプリケーションプラグインの実証成功は、量子脆弱性のある暗号技術に代わる代替手段の実装可能性を示すものである。量子脆弱性のある暗号技術の使用は、保存データの機密性、完全性、可用性を危険にさらす可能性がある。
量子対応認証局の実装	耐量子および／またはポスト量子ハイブリッド化に対応した X.509 認証局。	**CM-3**（強化 06）にサポートされる（例示）：構成管理 – 暗号管理	暗号化メカニズムが構成管理下にあることを保証する。例えば、システムコンポーネントが識別と認証に証明書を使用する場合、それらの証明書の有効期限に対処するプロセスが実装される。

		SC-12 をサポートする（例示）：暗号鍵の鍵確立と管理	量子コンピューティングが実用レベルでショーアルゴリズムを実行可能な環境において、安全な鍵確立を実施するには量子対応認証局が必要である。
		SC-17 をサポートする（不可欠要素）：公開鍵基盤証明書	多くの PQC 実装では、公認認証機関が発行する PKI 証明書が必要となる。
		SC-23（強化 05）をサポートする（例示）：セッション真正性－許可された認証局	組織は、受け入れ/使用する認証局のセットを制限することがある（例：米国の移民取締機関は、一部の外国の発行元からの証明書を受け入れない場合がある）。
量子対応ハードウェアセキュリティモジュール（HSM）	耐量子および／または耐量子ハイブリッド化対応の鍵確立・保管メカニズム。組み込みの量子耐性暗号機能を提供する。	**RA-3** にサポートされる（例示）**：**リスクアセスメント）	量子対応アルゴリズム実装に対する内部・外部脅威の脆弱性を特定することで、HSM の要件定義と選定に資する。
		SC-12 をサポートする（例示）：暗号鍵確立および管理	HSM は暗号鍵の鍵確立機能を実行し、管理サポートを提供することが多い。
		SC-28 をサポートする（例示）：保存中の情報の保護	量子対応 HSM の成功した実証は、量子脆弱性を持つ暗号コンポーネントに対する物理的保護の実現可能性を示すものである。これらのコンポーネントのエクスポージャーにより、保存データの機密性、完全性、可用性が危険にさらされる可能性がある。