耐量子計算機暗号への移行に関する
技術動向調査

株式会社日立製作所

2026 年 1 月

エグゼクティブサマリ

本報告書は、耐量子計算機暗号（PQC）への移行を、暗号アルゴリズムの置換にとどまらないシステム全体の取り組みとして整理する。移行は、業務や、業務で使用する機器が利用する暗号方式の把握（クリプト・インベントリ）、影響評価と優先度付け、方針・計画の策定、段階的な導入・運用という複数段階で進める。移行期には既存の暗号と PQC の併用（ハイブリッド構成）が中心的な選択肢となる。

ハイブリッド構成は、アルゴリズム・プロトコル・システムの各レイヤーで設計される。本報告書では、既存の暗号と PQC を組み合わせる構成を、両者を同時に必須利用して結果を統合する合成（composite）方式と、処理をそれぞれ独立に行い後方互換性を実現する混成（hybrid）方式に分類して整理する。具体的には、鍵共有では複数の鍵共有方式から得られた共有秘密を鍵導出関数(KDF)に入力して統合する枠組みが用いられ、署名では合成方式の署名（コンポジット署名）による安全性維持や代替署名・複数証明書の活用といった混成方式により後方互換性を確保する。安全性に関する整理は、複数要素の組み合わせに依存することから、設計目標と仕様が保証する範囲の区別、実装・運用に起因するリスクへの留意が必要である。

実装・運用面では、OQS／liboqs、OQS-OpenSSL、Bouncy Castle、wolfSSL 等のオープンソースソフトウェア（OSS）やライブラリが検証基盤を提供しており、PKI／メール等では段階的導入の事例が提案されている。性能影響はユースケースに依存するが、クリプトグラフィック・アジリティ（暗号の俊敏性）の確保が移行コストを大きく左右する。

標準化動向として、NIST（ML-KEM／ML-DSA、SP 800-227、SP 800-56C Rev.2）、IETF（TLS ハイブリッド鍵共有、ハイブリッド KEM／署名、MLS コンバイナ、RFC 9794）、ETSI（TS 103 744）が挙げられ、産業連携では Post-Quantum Cryptography Coalition（PQCC）がロードマップ等を通じて、移行戦略と設計指針の枠組みを提供している。

本報告書では、移行課題、導入プロセス、ハイブリッド構成の具体化、安全性整理、実装・運用事例、標準化動向を体系的に記述する。最終的な完全移行を見据えつつ、移行期間のリスク低減と相互運用性の確保を重視する。

目　次

用語

略称	正式名称	日本語訳
OSS	Open Source Software	オープンソースソフトウェア
CMS	Cryptographic Message Syntax	暗号メッセージ構文
OID	Object IDentifier	オブジェクト識別子
PQC	Post-Quantum Cryptography	耐量子計算機暗号
ML-KEM	Module-Lattice-based Key Encapsulation Mechanism	モジュール格子ベース鍵カプセル化方式
ML-DSA	Module-Lattice-based Digital Signature Algorithm	モジュール格子ベースデジタル署名アルゴリズム
RSA	Rivest-Shamir-Adleman	RSA（公開鍵暗号）
DH	Diffie-Hellman	ディフィー・ヘルマン
ECDH	Elliptic Curve Diffie-Hellman	楕円曲線ディフィー・ヘルマン
ECDSA	Elliptic Curve Digital Signature Algorithm	楕円曲線電子署名
KEM	Key Encapsulation Mechanism	鍵カプセル化方式
HKDF	HMAC-based Key Derivation Function	HMAC ベース鍵導出関数
KDF	Key Derivation Function	鍵導出関数
KDM	Key Derivation Method	鍵導出方法
TLS	Transport Layer Security	トランスポート層セキュリティ
MLS	Messaging Layer Security	メッセージング層セキュリティ
PKI	Public Key Infrastructure	公開鍵暗号基盤
X.509	ITU-T X.509	ITU-T 勧告 X.509
PQ/T	Post-Quantum and Traditional	耐量子計算機暗号と既存の公開鍵暗号のハイブリッド構成を指す

1. はじめに

1.1 目的

本報告書の目的は、CRYPTREC が 2025 年に公表した暗号技術ガイドライン [1]や研究動向調査報告書 [2]を踏まえ、耐量子計算機暗号（PQC）への移行に関する最新の技術動向を整理することである。移行期間においては、RSA や楕円曲線暗号などの既存の公開鍵暗号方式と PQC を併用するハイブリッド構成が現実的な選択肢となる。また、ハイブリッド構成については 2020 年のハイブリッドモード[1]の技術動向調査 [3]で技術動向が示されているが、その後の標準化や実装の進展を反映したアップデートが必要である。これらを背景に、移行プロセスの体系化、ハイブリッド構成の整理、安全性評価の枠組み、実装事例の収集、標準化動向の包括的調査を通じて、移行期間のリスク低減と相互運用性の確保を支援することを目的とする。

1.2 本書の構成

本書の構成は以下の通りである。

第 2 章：

移行時・導入時の技術的課題を用途横断で整理する。

第 3 章：

暗号使用状況の把握（クリプト・インベントリ）、優先度付け、計画策定、段階的導入といった PQC 導入アプローチを整理する。

第 4 章：

ハイブリッド構成をアルゴリズム／プロトコル／システムの各層で解説する。

第 5 章：

各標準化文書に記述されているハイブリッド構成の安全性概念を整理する。

第 6 章：

OSS（OQS/liboqs 等）や PKI／メール／ブラウザなどの 実装・運用事例を紹介する。

第 7 章：

NIST、IETF、ETSI、ITU、IEEE、ISO、X9、NSA、CSA、PQCRYPTO、PQCC の標準化動向を整理する。

第 8 章：

調査結果の考察を述べる。

第 9 章：

参考文献を掲載する。

[1] 2020 年の報告書では、本報告書の「ハイブリッド構成」に相当する用語として「ハイブリッドモード」が用いられていたため、当該箇所では当時の用語をそのまま記載している。

2. PQC 移行時・導入時における課題

本章では、用語の定義を含む PQC 移行における前提整理を行い、PQC への移行時および導入時に直面する技術的課題を整理する。

CRYPTREC の暗号技術ガイドライン [1]や研究動向調査報告書 [2]では、PQC 移行は暗号アルゴリズム単体の置換に留まらず、業務や業務で使用する機器が利用している暗号方式の棚卸し、鍵管理、通信方式、システム更新サイクル、相互運用性などを含むシステム全体の問題として捉える必要があることが指摘されている。

また、PQC 移行は短期間で完了するものではなく、既存方式との共存を含む移行期間を前提として段階的に進められることが想定されている。このため、本章では、CRYPTREC が示す「PQC の導入における課題」の整理を踏まえ、移行期において顕在化する技術的課題を体系的に整理し、2.1 節以降で述べる用途別の課題整理および 3 章における導入アプローチの検討につなげることを目的とする。

2.1 用語の整理と定義

PQC 移行における前提整理を行う前に、本報告書で頻出する用語を以下の通り定義する。

鍵カプセル化（Key Encapsulation Mechanism: KEM）：

鍵カプセル化とは、セッション鍵を生成する機能と、生成された鍵を暗号化する機能を組み合わせた暗号化方式である。暗号化処理をカプセル化（encapsulation）、復号処理をデカプセル化（decapsulation）と呼ぶ。なお、NIST SP 800-227 [4]では、KEM および KEM を用いた鍵共有プロトコルの両方を、明示的に宣言することなく KEM と表現しているため、注意が必要である。本報告書では、後者の用法については「KEM を用いた鍵共有」と呼ぶ。

前方秘匿性（(perfect) forward secrecy）：

前方秘匿性とは、鍵共有プロトコルを通じて共有されたセッション鍵の独立性を意味する。多くの場合、セッション鍵の生成に毎回異なる乱数を付加することで、前方秘匿性を実現する。たとえば、DH 鍵共有（$(g^x)^y=(g^y)^x$）において、指数 x, y を毎回ランダムに生成する ephemeral DH（DHE）は前方秘匿性を満たすことが知られている。前方秘匿性を満たす鍵共有プロトコルは、一部のセッション鍵や長期保存鍵（long term key）が漏洩した場合であっても、漏洩する情報の範囲を限定することができる。

後方互換性：

TLS などの通信プロトコルは、接続する端末ごとに実装されているプロトコルのバージョン、暗号スイートが異なることがある。新しい規格において、古い規格との接続可能性を後方互換性（backward compatibility）と呼ぶ。例えば、TLS は ClientHello の中にプロトコルのバージョンと暗号スイートを含んでおり、サーバは ServerHello で提示されたプロトコルのバージョンと暗号スイートの中から自身が対応可能かつ優先度が高いものを返信する。

鍵素材（keying material）：

DH 鍵共有や KEM を用いた鍵共有などで共有された shared secret と追加の補助情報(other input)を入力として、鍵導出方法（key derivation method）を用いて出力されたビット列。

「ハイブリッド」について

PQC への暗号移行では、既存の公開鍵暗号と PQC を組み合わせる方式をまとめてハイブリッド方式と呼んでいた。しかし、IETF などでは、後方互換性（既存システムとの相互接続性）と安全性の観点から、ハイブリッド方式を合成（composite）と混成（hybrid）の 2 つに分けるようになっている。

合成（composite）：

署名検証もしくは鍵共有において、既存の公開鍵暗号方式と PQC を同時に必須利用し、その結果を統合して一つの処理として扱う方式。その特徴から、合成方式は後方互換性を持たない。必ず既存の公開鍵暗号方式と PQC の両方を使う、安全性を重視した方式である。

混成（hybrid）：

署名検証もしくは鍵共有において、既存の公開鍵暗号方式と PQC の処理をそれぞれ独立に行い、パーサ等の上位の処理で既存の公開鍵暗号方式と PQC の使い方を規定する方式のこと。既存の公開鍵暗号方式の処理を従来通りとすることで、後方互換性を実現できる。その一方で、混成方式は既存の公開鍵暗号方式単独での使用が可能となるため、将来的にダウングレード攻撃の対象となる可能性がある。混成方式を用いる場合、適切なタイミングで既存の公開鍵暗号方式単体での使用を禁止する措置を講じる必要があり、クリプトグラフィック・アジリティの実装がより重要となる。

本報告書では、既存の公開鍵暗号方式と PQC を組み合わせる方式を総括して「ハイブリッド」と呼び、上に挙げた各々の構成方法については「合成」「混成」と呼ぶことにする。

鍵確立／鍵合意／鍵共有／鍵交換について

本報告書では、主に公開鍵暗号の署名および鍵共有について取り扱う。しかし、本報告書の中で頻繁に引用される NIST 文書や IETF 文書では、鍵共有について別の用語が用いられていることが多く、分類の境界も異なる。混乱を避けるため、ここでそれぞれの用語の使い方について整理する。

CRYPTREC：

CRYPTREC 暗号リスト [5]は公開鍵暗号の用途を署名、守秘、鍵共有の 3 種類に分類している。電子政府推奨暗号リスト、もしくは推奨候補暗号リストに掲載されているアルゴリズムの中で、守秘に分類されているものは RSA-OAEP のみであり、DH, ECDH, PSEC-KEM が鍵共有に分類されている。なお、[1]では「また、RFC7525 においても、4.1 節において（守秘用途である）RSA key transport は利用すべきでないと記載されており...」と述べており、守秘と後述する鍵配送（key transport）を同一視している。

NIST：

NIST は単純な秘匿目的の守秘に相当する公開鍵暗号を標準化していない。その代わりに、NIST SP 800-56A, B において（二者間の）鍵確立（key establishment）を導入している。鍵確立は、エンティティの双方が共有される鍵素材（keying material）を提供する鍵合意（key agreement）と、一方のエンティティのみが鍵素材を提供する鍵配送（key transport）に分類される。2.2 節で触れるが、KEM は鍵配送と同一視されることがある。一方、NIST は、KEM をその内部構造に応じて鍵合意的に、または鍵配送的に見なすことができると述べている。たとえば SP 800-227 では「ML-KEM could be viewed as a key-agreement scheme」と記されており、ML-KEM は鍵合意として見なすことができる。同様に、RSA-OAEP は一般に鍵配送として見なされる [4]。

IETF：
CRYPTREC暗号リストで守秘に分類されているRSA-OAEPは、[6]ではRSAES-OAEP（RSA Encryption Scheme)であるが、 [7]では“RSA key transport mechanisms [RFC8017]”と引用されている。このように、IETF では用語の選び方に揺らぎがあるが、key transport を暗号化方式（守秘）とほぼ同義に取り扱っている。また、鍵確立（鍵合意）の代わりに鍵交換（key exchange）という用語を用いている。

本報告書の対象は主として（NIST の用語で）鍵合意を扱い、鍵配送は取り上げない。そこで、本報告書では原則として CRYPTREC の用語に従い、紹介する文献による呼称ではなく、一貫して鍵共有を用いる。

なお、CRYPTREC では RSA-OAEP を守秘、PSEC-KEM を鍵共有に分類している。しかし、本報告書は鍵カプセル化（KEM）および KEM を用いた鍵共有（鍵合意）プロトコルを主な調査対象としており、KEM を鍵共有に含めると混乱を生じる懸念がある。そこで、本報告書では、読者の混乱を避けるため、鍵カプセル化は CRYPTREC の特定の分類に入れずにそのまま「鍵カプセル化」（もしくは KEM）と呼ぶことにする。

2.2 PQC 移行における前提整理

PQC の導入は、従来の公開鍵暗号アルゴリズムを別の方式に単純に置き換える問題ではない。安全性の評価や影響範囲はアルゴリズム単体に留まらず、実装、プロトコル設計、運用形態を含むシステム全体として検討する必要がある。そのため、PQC 移行は暗号方式の更新ではなく、既存システム構成との整合を前提とした設計・運用上の課題として捉える必要がある。

また、PQC に関する標準化の進展状況や移行時に顕在化する課題は、暗号の利用用途によって性質が異なる。署名用途では、モジュール格子ベースデジタル署名アルゴリズム（Module-Lattice-based Digital Signature Algorithm: ML-DSA）等のアルゴリズム標準化は進みつつあるものの、X.509 証明書や暗号メッセージ構文（Cryptographic Message Syntax: CMS）、長期署名といった既存 PKI 基盤への組込みに関しては、証明書サイズの増大、相互運用性、後方互換性の確保など、運用およびデータ構造上の課題が残されている。このため、署名用途における主な論点は、署名アルゴリズム自体よりも、その利用基盤との整合にある。

一方、鍵共有用途では、従来の Diffie-Hellman（DH）系方式から鍵カプセル化（KEM）系方式への移行が通信プロトコルの設計に直接的な影響を及ぼす。その結果、アルゴリズムの置換に留まらず、通信手順やメッセージ構成、状態管理、前方秘匿性の扱いを含むプロトコル全体の再検討が必要となり、実装依存性および用途依存性が特に高いという特徴を有する。

さらに、CRYPTREC 等でも指摘されているように、PQC 移行は短期間で完了するものではなく、段階的かつ長期にわたる可能性が高い。この前提の下では、最終的な完全移行のみならず、移行途中におけるリスクの抑制を考慮した構成や運用方針を検討することが重要である。以上の点は、本章における課題整理全体の共通前提として位置付けられる。

2.3 PQC の導入における課題

本節では、2.1 節で整理した前提条件を踏まえ、PQC を既存システムへ導入する際に顕在化する課題を整理する。

PQC 移行は既存方式との共存を含む移行期を前提とするものであり、課題の性質は暗号の利用用途によって大きく異なる。

このため本報告書では、署名、守秘、鍵共有の各用途に分けて整理するとともに、これらに共通

する実装・運用および相互運用性に関する課題についても整理する。

2.3.1 署名用途の PQC 移行における課題

一般に、PQC 署名方式は従来方式と比較して鍵長および署名サイズが大きくなる傾向があり、これに伴い証明書サイズや署名付きデータ量の増加が生じる。このような変化は、X.509 証明書や CMS 等に代表される既存 PKI のデータ構造や運用設計に直接的な影響を及ぼす。

また、長期にわたって検証可能性を維持することが求められるアーカイブ用の署名においては、署名生成時点では安全と考えられていた署名方式が、将来的に破られた場合の影響を考慮する必要がある。すなわち、耐量子計算機性を持たない署名方式が、将来、実用的な量子コンピュータが開発され、署名を付したドキュメントの改ざんが行われる等、署名が破られることは十分考えられる。この場合、過去に正当と検証された署名の真正性が事後的に否定される可能性が存在する。このような長期的な真正性に関するリスクは、たとえば証明書の更新が想定されていない IoT 機器や有効期限が長いパスポートなどの ID カードにおいて顕在化する可能性があり、近年の一部の実務文献において、守秘用途における Harvest Now, Decrypt Later（HNDL）に対比する形で言及されている[2]。

さらに、署名は検証者が多数存在するケースが一般的であり、後方互換性の確保が特に重要となる。単独の PQC 署名方式への移行は、既存の検証環境や運用との断絶を招く可能性がある。このため、移行期においては、既存方式との連続性を保ちながら段階的な導入を可能とする手法として、ハイブリッド構成の署名が検討対象となっている。

2.3.2 守秘用途における課題

守秘用途における課題は、公開鍵暗号方式の変更が通信システム全体の設計および運用に広範な影響を及ぼす点にある。RSA や楕円曲線暗号から PQC 方式への移行は、暗号アルゴリズムの更新に留まらず、既存の通信プロトコルやその運用形態との整合性を慎重に検討する必要がある。

CRYPTREC では、守秘目的の公開鍵暗号の用途として Key Encapsulation Mechanism - Data Encapsulation Mechanism（KEM-DEM）構成によるデータ暗号化や、鍵配送プロトコルを挙げている[1] [5]。

このうち、KEM-DEM 構成によるデータ暗号化の用途について、[1]ではドキュメントデータや（他の用途での）鍵情報を通信当事者間で共有する、暗号鍵所有者が鍵情報をバックアップするといったユースケースを挙げている。特にデータや鍵情報のバックアップでは、暗号化データの長期秘匿性が必要になると考えられる。このようなケースは「暗号化データを今から収集し、量子計算機が利用できるようになったら解読する（Harvest Now, Decrypt Later: HNDL）」という脅威に直面するため、PQC の導入が不可欠である。導入に際しては、バックアップされている大量のデータを再暗号化するコストや、再暗号化処理の途中でデータが破損するリスクが課題となると想定される。

なお、鍵配送における PQC 導入の課題は鍵共有と同様であるため、説明は 2.3.4 節に譲る。

---

[2] 将来の量子計算機により現在用いられている公開鍵署名方式が破られた場合、過去に生成・検証された署名や証明書が事後的に偽造可能となるリスクについて、近年の一部の実務・業界文献では“Trust Now, Forge Later（TNFL）”という呼称が用いられている例がある（例：Trust Now, Forge Later (TNFL) - The Overlooked Quantum Threat）。ただし、この用語は現時点では NIST、IETF、ETSI 等の標準文書において確立した専門用語として定義されているものではなく、本報告書では概念的表現として補足的に紹介するに留める。

2.3.3 鍵共有用途における課題

TLS 1.3 などの主要な鍵共有プロトコルでは、DH や楕円曲線 Diffie-Hellman（ECDH）が主流である。現在、標準化された PQC アルゴリズムは KEM のみであり DH や ECDH を直接代替する方式が無い。したがって、鍵共有用途については、従来の DH や ECDH に基づくプロトコルから、KEM に基づくプロトコルへの移行という設計上の大きな転換が求められる。また、実際の鍵共有プロトコルは中間者（Man-in-the-Middle）攻撃を避けるために公開鍵証明書ベースの認証を行うことが多いため、前述の署名に関する課題も併せて検討する必要がある。特に、インターネット標準は多種多様な条件で運用されているサーバ、端末との接続を維持するため、移行を完了していないシステムを考慮した後方互換性が重要であり、既存プロトコルとの整合を前提とした設計が不可欠となる。

2.3.4 実装・運用・相互運用性に関する共通課題

用途に共通する課題として、実装、運用および相互運用性に関する問題が挙げられる。PQC 実装の成熟度にはばらつきがあり、オープンソースソフトウェア（OSS）、ハードウェアセキュリティモジュール（Hardware Security Module: HSM）、ハードウェアアクセラレータ等の対応状況も一様ではない。また、暗号方式の変更は相互接続試験の実施を不可避とし、鍵更新、失効、ロールオーバーといった運用設計にも影響を及ぼす。

これらの課題は、CRYPTREC による PQC 移行に関する整理においても指摘されており、本節ではそれらを用途横断的な視点から再解釈した。

3. PQC 導入へのアプローチ

PQC 導入に関する基本的な考え方については、CRYPTREC の暗号技術ガイドライン［1]や研究動向調査報告書［2]、本報告書に先行するハイブリッドモード[1]に関する調査報告書［3]をはじめ、産業・実務文献や行政文書において整理が行われている。これらの文献では、PQC 移行を暗号アルゴリズム単体の置換としてではなく、業務や業務で使用する機器が利用する暗号方式の把握、既存方式との共存、段階的な更新を含む中長期的な取り組みとして進める必要性が示されている。

本章では、これらの整理を踏まえ、PQC 導入に関する全体プロセス、移行計画策定の検討事項、用途別の導入アプローチ、ならびに段階的な移行モデルであるハイブリッド構成の位置付けについて整理する。

3.1 PQC 導入に関する全体プロセス

PQC 導入への取り組みは、暗号アルゴリズム単体の置換としてではなく、複数の段階を経て進められる移行プロセスとして整理されている。PQCC（Post-Quantum Cryptography Coalition）が公表している PQC Migration Roadmap［8]においても、PQC 導入は単一の完了時点を目標とするものではなく、準備段階、移行期、移行後の運用といった複数のフェーズに分けて整理されている。

図 3-1 に示す PQC Roadmap Categories では、まず初期段階として、利用中の暗号技術やその用途を把握する作業が位置付けられている。これには、暗号アルゴリズム、プロトコル、鍵管理方式、証明書構成などを整理することが含まれており、後続の検討を行うための基礎情報として重要な工程とされている。

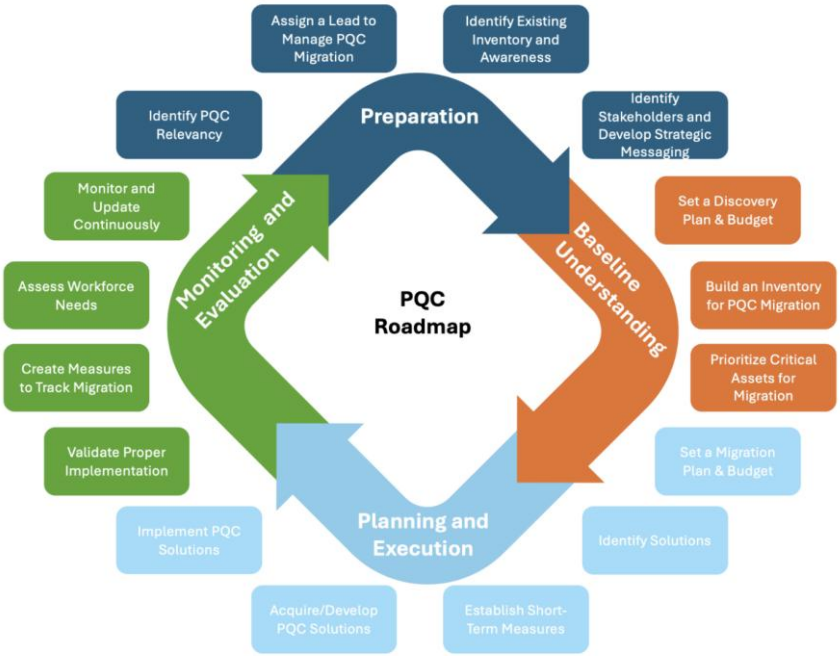


図 3-1 PQC ロードマップ［8]

次の段階では、把握された暗号方式を整理した資産を基に、影響評価や優先度付けを行い、どの領域から移行を進めるべきかを検討する工程が示されている。この段階では、暗号方式の安全性だけでなく、データの保護期間、システムの重要度、更新サイクル、外部組織との相互運用性といった要素を考慮した判断が求められる。

移行期においては、既存方式と PQC を併用する構成や、段階的な切り替えを前提とした運用が想定されている。PQCC のロードマップでは、この期間を通じてシステムの継続運用を維持しながら、

順次構成を更新していくことが前提とされており、一斉置換を想定しない点が特徴となっている。

さらに、移行後の段階では、導入したPQC構成を運用・維持しつつ、将来的な暗号方式の更新や標準化動向への対応を継続的に行うことが位置付けられている。このことから、PQC導入は一度限りの対応ではなく、長期的な運用プロセスの一部として捉えられている。

このような段階的な整理は、CRYPTREC の暗号技術ガイドラインや金融庁の報告書において示されている考え方とも整合しており、PQC導入を計画に基づき中長期の視点で進める上での全体像を示すものと位置付けられる。本章では、この全体プロセスを踏まえた上で、3.2節以降において、移行計画策定における検討事項、用途別の導入アプローチ、段階的導入モデルおよびハイブリッド構成の位置付けについて整理する。

3.2 移行計画策定における検討事項

PQC導入計画を策定するにあたっては、導入対象や影響範囲を事前に整理することが不可欠である。特に、既存システムにおいてどの暗号技術がどの用途で利用されているかを把握する作業は、導入計画全体の基盤となる。さらに、移行計画の実現可能性を確保するためには、必要な予算の見積もりと確保がプロセスとして不可欠である。以下では、このような移行計画策定において主要となる検討事項として、暗号使用状況の把握と移行対象・優先度の整理について述べる。

3.2.1 暗号使用状況の調査・把握（クリプト・インベントリ）

暗号使用状況の調査・把握（クリプト・インベントリ）では、利用中の暗号アルゴリズム、プロトコル、証明書、鍵管理方式などを一覧化し、それらがどのシステムやデータ保護に用いられているかを整理する。この作業は、PQC移行において何が影響を受けるかを明確化するための出発点として位置付けられる。

具体的には、通信路における暗号化や認証、電子署名や証明書管理、鍵生成・保管・更新といった各機能について、使用されている暗号方式と運用形態を把握することが重要となる。また、暗号技術が利用されている箇所はアプリケーション層に限らず、プロトコル層やミドルウェア、ハードウェアに組み込まれている場合もあるため、システム全体を俯瞰した整理が求められる。

このように暗号使用状況を整理することで、PQC移行が必要となる対象や、移行時に影響を受ける範囲を把握することが可能となる。さらに、後続の優先度付けや移行計画策定において、前提情報として活用することができる。

3.2.2 移行対象や優先度の検討

クリプト・インベントリを作成した後には、収集した情報を基に、移行対象や優先度を検討する必要がある。すべての暗号技術を同時に更新することは現実的ではないため、どの領域から移行を進めるかを整理することが重要となる。

優先度の検討にあたっては、暗号によって保護されるデータの保護期間や重要度、関連するシステムの役割、更新頻度や保守性といった要素が考慮される。また、外部システムや取引先との接続関係がある場合には、相互運用性や移行時期の調整が必要となる。また、確保した予算の範囲内で、移行対象の優先順位を調整することにより、限られたリソースを効果的に活用し、計画的な移行を進めることが求められる。

これらの観点を踏まえて移行対象と優先度を整理することで、限られたリソースの中でも現実的な移行計画を策定することが可能となる。このような段階的な検討は、PQC移行を中長期的な取り組みとして進める上での基本的なプロセスとして、多くの文献において共通して示されている。

3.3 用途別の導入アプローチ

PQC 導入における具体的な対応は、暗号の利用用途によって性質が異なる。本節では、2.3 節で整理した用途別の課題に対応する形で、導入アプローチを示す。

3.3.1 署名用途における導入アプローチ

署名用途では、2.3.1 節で整理したとおり、鍵長や署名サイズの増大による証明書構造への影響、長期真正性の確保、後方互換性といった課題が存在する。このため、導入アプローチとしては、既存 PKI と独立しない形で段階的に PQC を導入することが基本となる。具体的には、既存の証明書・署名形式を維持しつつ PQC を追加する合成方式や混成方式の活用、検証者側の移行状況を踏まえた複数署名の併存期間の設定、長期検証性を確保するためのタイムスタンプや署名更新の運用ルール整備が挙げられる。これにより、既存の検証環境を保持しつつ PQC を段階的に適用でき、将来的な単独 PQC 署名への移行に向けた基盤整備を進めることが可能となる。

3.3.2 守秘・鍵共有用途における導入アプローチ

守秘用途および鍵共有用途では、2.3.2 節や 2.3.3 節に示したように、量子コンピュータの実用化を前提とした長期秘匿性の確保や、DH／ECDH から KEM を用いた鍵共有への構造転換、大規模な後方互換性確保が課題となる。これらに対する導入アプローチとしては、まず長期秘匿性が求められるデータ暗号化から優先的に PQC KEM を適用し、保管データ・バックアップデータの再暗号化を段階的に実施することが重要である。また、通信プロトコルにおいては、既存方式との連続性を確保するため、PQC KEM と従来の ECDH を併用するハイブリッド鍵共有を導入し、接続性を維持しながら KEM を用いた鍵共有ベースの設計へと移行を進めることが有効である。これにより、運用環境の多様性を損なうことなく、将来的な PQC への完全移行に向けた整合的なステップを構築できる。

3.4 クリプトグラフィック・アジリティの確保

PQC 導入にあたっては、今回の移行に対応するだけでなく、将来的な暗号方式の更新にも対応可能な設計とすることが重要である。CRYPTREC や金融庁の文献においても、暗号方式の更新を前提とした柔軟な設計の必要性が指摘されている。これらは一般に、クリプトグラフィック・アジリティとして整理される。

クリプトグラフィック・アジリティの確保により、暗号アルゴリズムやパラメータの変更をシステム全体の大規模な改修を伴わずに実施することが可能となる。PQC 移行は一度限りの対応ではなく、長期的な継続対応が求められる取り組みであることから、この観点は導入アプローチ全体に共通する重要な要素となる。

3.5 ハイブリッド構成の位置付け

段階的な PQC 移行を進める上で、既存暗号方式と PQC を併用するハイブリッド構成は、移行期における代表的な選択肢として各種文献で取り上げられている。ハイブリッド構成は、既存システムとの連続性を確保しつつ、新たな暗号方式を段階的に導入するための構成として位置付けられる。

一方で、ハイブリッド構成は構成や運用が複雑化する可能性があるため、その適用範囲や設計上の留意点を整理した上で利用する必要がある。本章では、ハイブリッド構成を段階的導入モデルの一例として位置付けるに留め、具体的な方式構成や技術的詳細については、4 章以降で整理する。

4. ハイブリッド構成の構成方法に関する解説

ハイブリッド構成は、PQC 移行期における後方互換性の確保と安全性維持を目的とする構成である。CRYPTREC のガイドライン [1]で示された分類を踏まえ、既存基盤との連続性を保ちつつ、耐量子計算機性を付与するための設計指針を整理する。本章では、ハイブリッド構成の目的と適用主体を体系化し、アルゴリズム・プロトコル・システムの各レイヤーにおける技術仕様例を示す。

4.1 ハイブリッド構成の整理

ハイブリッド構成は、CRYPTREC のガイドライン [1]において、「移行期における後方互換性の確保」と「耐量子計算機性の付与による安全性維持」の両立を目的とする構成として整理されている。本報告書では、この定義を踏まえ、ハイブリッド構成を目的（後方互換性確保／安全性維持）および適用主体（アルゴリズム・プロトコル・システム）の観点から体系化する。本節では、これらの対応関係を表 4-1 に示し、4.2 節以降で各レイヤーの技術仕様を解説する。

- アルゴリズム層（鍵共有アルゴリズム／署名アルゴリズム）
  アルゴリズム層は、鍵カプセル化アルゴリズムと署名アルゴリズムを対象とする。
  アルゴリズム層では、合成方式のみ規定されており、後方互換性を考慮した混成方式のアルゴリズムは定義されていない。混成方式の仕様は個々のプロトコルに任されている。NIST SP 800-227 [4]では合成方式の KEM を用いた鍵共有プロトコルを定めている。また、DH を KEM とみなして利用する方法も定めており、ECDH+ML-KEM(Module-Lattice-based Key Encapsulation Mechanism, モジュール格子ベース鍵カプセル化方式)を合成方式の KEM を用いた鍵共有として記述するための基盤を与えている。
  署名についても複数署名を 1 つの署名構造として統合する合成方式の署名（コンポジット署名）が標準化されつつある。本方式では、既存の公開鍵暗号による署名と PQC 方式による署名の両方の検証が成功することが合成方式の署名の検証アルゴリズムとなる。また、署名生成においても、それぞれの署名を分離して悪用するリスクを避けるため、補助入力の追加する方式などが提案されている。
- プロトコル層（通信プロトコル／証明書構造）
  プロトコル層は、アルゴリズムを実際の通信・認証処理でどのように活用するかを規定する層である。TLS、MLS、ETSI TS 103 744、IEEE 802.11 Proposal では、複数の KEM を組み合わせる、合成方式のハイブリッド鍵共有方式が定義されている。証明書構造もプロトコル層で利用され、Discovery-enabled（混成）、Dual-signature（混成）、Composite-signature（合成）など、後方互換性重視の方式と安全性重視の方式の双方が標準化されている。
- システム層
  システム層は、アルゴリズムおよびプロトコルを PKI、メールシステム、鍵管理方針、更新運用などの実環境に統合する領域である。単一仕様としてハイブリッド方式が定義されているわけではなく、複数の方式を組み合わせて移行期の後方互換性と安全性維持を両立するシステム設計が重要となる。実装・運用例として、Hybrid PKI の階層設計や、メールシステムにおける段階的移行方式などがあり、これらは 6 章で実装の事例を紹介する。

ハイブリッド構成は、単一の技術要素ではなく、複数のレイヤーにまたがる設計課題を含む。目的別（後方互換性確保／安全性維持）と主体別（アルゴリズム、プロトコル、システム）に分類することで、どの層でどの標準仕様や設計指針が必要かを明確化し、後続の詳細解説に向けた体系的な理解を提供することを意図している。

表 4-1 ハイブリッド構成の目的と適用主体による整理

目的 / 主体	後方互換性確保	安全性維持
アルゴリズム	なし	鍵共有アルゴリズム • NIST SP 800-227(4.6. Multi-Algorithm KEMs and PQ/T Hybrids) [4] • NIST SP 800-56C Rev.2[3] [9] • draft-irtf-cfrg-hybrid-kems-07 [10] • draft-ietf-lamps-pq-composite-kem-12 [11][4]
		署名アルゴリズム • draft-ietf-lamps-pq-composite-sigs-14 [12][4]
プロトコル	通信プロトコル • RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3 [13] ※4.1.1 Cryptographic Negotiation により後方互換性を提供するが、混成方式ではない	通信プロトコル • draft-ietf-tls-hybrid-design-16 [14] • draft-ietf-mls-combiner-02 [15] • ETSI TS 103 744 [16] • IEEE 802.11 Hybrid PQC Proposal [17] • draft-ietf-lamps-pq-composite-kem-12 [11][4]
	証明書構造 • draft-ietf-lamps-certdiscovery-02 [18] • ITU-T X.509(9.8 Alternative cryptographic algorithms and digital signature extensions) [19]	証明書構造 • draft-ietf-lamps-pq-composite-sigs-14 [12][4]
システム[5]	（後方互換性確保／安全性維持　共通） • 耐量子移行を考慮した PKI ベースのハイブリッド設計・実装 Architecting PKI Hierarchies for Graceful PQ Migration(PQC Conference) [20] Hybrid PQC E-Mail Communication: Easing Migration Pain(PQC Conference) [21]	

4.2 ハイブリッド構成のアルゴリズム

[3] 本文献は、複数鍵素材を同時依存で統合する汎用 KDF を規定する仕様であり、ハイブリッド構成を直接目的とした設計ではないが、draft-irtf-cfrg-hybrid-kems-07 や draft-ietf-lamps-pq-composite-kem-12 における鍵結合の基盤技術として位置付けられる。

[4] 本文献は、合成方式による暗号アルゴリズム仕様と、証明書・プロトコルでの利用方法を併せて規定しているため、アルゴリズム層およびプロトコル層の双方に記載している。

[5]システム層については、アルゴリズム層やプロトコル層のように単一の技術仕様として規定されたハイブリッド方式は存在しない。このため本表では、複数の技術仕様を組み合わせて構成される実運用上の設計例や実装案を通じて、システムとしてのハイブリッド構成を整理している。また、システム層では、利用目的や運用段階に応じて、後方互換性確保を目的とする構成と安全性維持を目的とする構成を選択または組み合わせて用いることが想定される。

4.2.1 鍵共有アルゴリズム

ハイブリッド構成における鍵共有アルゴリズムは、複数の暗号方式を組み合わせることで安全性を強化し、耐量子計算機性を確保することを目的として設計されている。

本節では、まず IETF が前提とする鍵結合モデルの基礎を与える文書、NIST SP 800-227 を取り上げる。NIST SP 800-227 では、Multi-Algorithm KEM の設計指針が示されており、耐量子計算機性を有する（post quantum）方式と既存（traditional）の方式を組み合わせる post quantum/traditional ハイブリッド構成（以下、PQ/T ハイブリッド構成と呼ぶ）の基本的な考え方を理解する上で参照すべき文書である。なお、NIST SP 800-227 では Section 4.6「Multi-Algorithm KEMs」の中で、複数 KEM を結合した方式を Composite KEM と呼んでいる。本節では、同セクションタイトルに合わせて「Multi-Algorithm KEM」を包括的な用語として使用する。

ハイブリッド構成の Multi-Algorithm KEM は、以下の二段階で構成される。

1. 共有秘密を生成する。
   複数の KEM を用いた鍵共有を個別に実行し、方式ごとに共有秘密を生成する。これにより、アリスとボブは複数の共有秘密を保持する。
2. 共有秘密を結合する。
   生成された複数の共有秘密を、承認済みの鍵結合器（Key Combiner）を用いて単一の共有鍵を導出する。

図 4-1 に示すように、鍵生成、カプセル化（Encapsulation）、デカプセル化（Decapsulation）の各フェーズで複数の KEM を用いた鍵共有が並列に動作し、最終的に Key Combine 関数によって単一の共有鍵が導出される。

なお、図 4-1 は NIST SP 800-227 の Fig. 1. Outline of key establishment using a KEM に Multi-Algorithm KEM の構築手順を反映した図である。

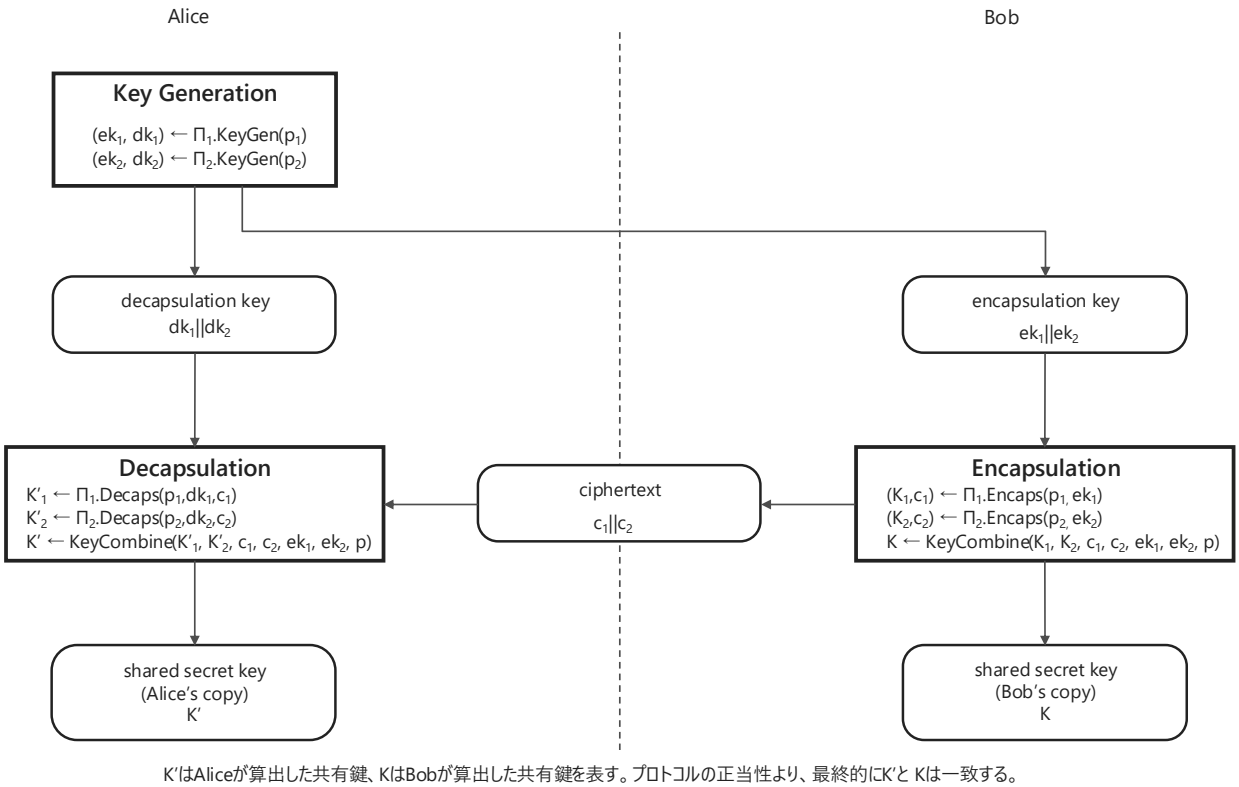


図 4-1 Multi-Algorithm KEM の概要

表 4-1 のアルゴリズム層に記載するその他の標準化文書の概要および位置付けは次の通りである。

draft-irtf-cfrg-hybrid-kems-07 は、ハイブリッド鍵カプセル化方式（ハイブリッド KEM）の設計フレームワークを定義しており、複数の KEM を組み合わせる際のセキュリティモデルや鍵結合器の要件を明確化している。具体的には、ML-KEM などの耐量子計算機性を有する KEM と従来の DH ベースの KEM を組み合わせる構成を想定している。本仕様では、DH を KEM と同じ入出力形式に抽象化して扱う枠組みを導入し、DH と PQCKEM を共通の KEM モデルに揃えた上でハイブリッド構成を定義している。

draft-ietf-lamps-pq-composite-kem-12 は、X.509 証明書や CMS などの PKI 環境において、ハイブリッド KEM を定義しており、本仕様ではコンポジット KEM という名称で規定されている。すなわち、複数の鍵共有方式（例：ML-KEM + ECDH）を一つの構造体にまとめることで、証明書や鍵管理の互換性を維持しつつハイブリッド構成を実現する。特に、証明書内で複数の公開鍵を保持し、暗号操作時に両方の鍵共有方式を実行する仕組みを提供する点で、NIST SP 800-227 の Multi-Algorithm KEM の概念を実装レベルに落とし込んでいる。なお、本仕様は証明書に格納される static 公開鍵を対象としている。

また、本仕様では表 4-2 のアルゴリズムリストが規定されている。

表 4-2 コンポジット KEM のアルゴリズムリスト

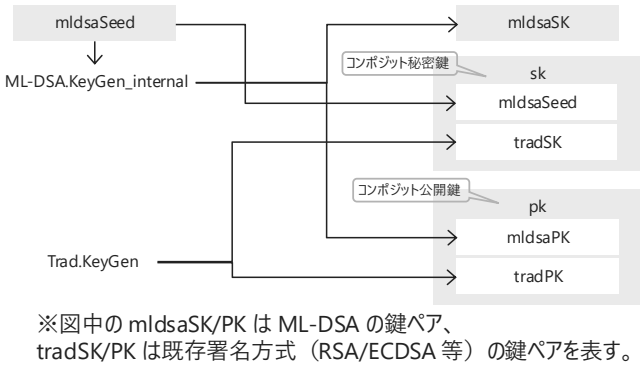
OID Name	OID	ML-KEM Variant	Traditional Algorithm	Key Size / Curve
id-MLKEM768-RSA2048-SHA3-256	1.3.6.1.5.5.7.6.55	ML-KEM-768	RSA	2048
id-MLKEM768-RSA3072-SHA3-256	1.3.6.1.5.5.7.6.56	ML-KEM-768	RSA	3072
id-MLKEM768-RSA4096-SHA3-256	1.3.6.1.5.5.7.6.57	ML-KEM-768	RSA	4096
id-MLKEM768-X25519-SHA3-256	1.3.6.1.5.5.7.6.58	ML-KEM-768	X25519	X25519
id-MLKEM768-ECDH-P256-SHA3-256	1.3.6.1.5.5.7.6.59	ML-KEM-768	ECDH	secp256r1
id-MLKEM768-ECDH-P384-SHA3-256	1.3.6.1.5.5.7.6.60	ML-KEM-768	ECDH	secp384r1
id-MLKEM768-ECDH-brainpoolP256r1-SHA3-256	1.3.6.1.5.5.7.6.61	ML-KEM-768	ECDH	brainpoolP256r1
id-MLKEM1024-RSA3072-SHA3-256	1.3.6.1.5.5.7.6.62	ML-KEM-1024	RSA	3072
id-MLKEM1024-ECDH-P384-SHA3-256	1.3.6.1.5.5.7.6.63	ML-KEM-1024	ECDH	secp384r1
id-MLKEM1024-ECDH-brainpoolP384r1-SHA3-256	1.3.6.1.5.5.7.6.64	ML-KEM-1024	ECDH	brainpoolP384r1

id-MLKEM1024-X448-SHA3-256	1.3.6.1.5.5.7.6.65	ML-KEM-1024	X448	X448
id-MLKEM1024-ECDH-P521-SHA3-256	1.3.6.1.5.5.7.6.66	ML-KEM-1024	ECDH	secp521r1

4.2.2 署名アルゴリズム

本節では、IETF LAMPS WG において標準化が進められているコンポジット署名方式（draft-ietf-lamps-pq-composite-sigs-14）について説明する。本方式は、PQC 署名アルゴリズムと従来署名アルゴリズムを一つの署名構造に統合することを目的として設計されている。コンポジット署名は、証明書やメッセージ署名において両方の署名を同時に生成・検証する仕組みを提供し、既存の PKI 基盤との整合性を維持するための不可欠な技術である。

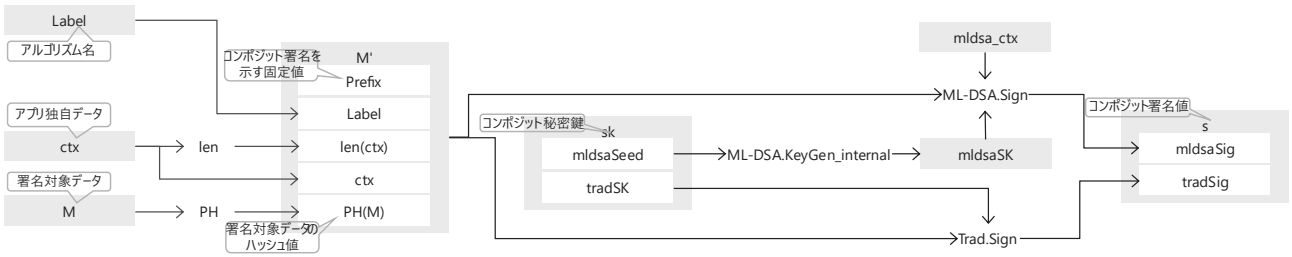
図 4-2 は、コンポジット署名方式における鍵生成の手順を示す。コンポジット署名では、PQC 署名アルゴリズム（例：ML-DSA）と従来署名アルゴリズム（例：RSA ベースの署名方式や ECDSA）の鍵ペアをそれぞれ生成し、両者を一つの構造に統合する。この統合により、証明書や署名操作において両方の鍵を同時に利用可能となる。



※図中の mldsaSK/PK は ML-DSA の鍵ペア、
tradSK/PK は既存署名方式（RSA/ECDSA 等）の鍵ペアを表す。

図 4-2 コンポジット鍵生成の概要

図 4-3 は、コンポジット署名の生成手順を示す。署名対象データに対してハッシュ関数による前処理を行い、その結果を両方の署名アルゴリズムに入力する。各アルゴリズムは独立に署名を生成し、最終的にコンポーネント署名構造に統合する。この構造には署名値、アルゴリズム識別子、関連パラメータが含まれ、検証者が両方の署名を確認できるよう設計されている。



※図中の mldsaSK/PK は ML-DSA の鍵ペア、tradSK/PK は既存署名方式（RSA/ECDSA 等）の鍵ペアを表す。

図 4-3 コンポジット署名の概要

図 4-4 は、コンポジット署名の検証手順を示すものである。検証者は署名構造から各署名値と対

応する公開鍵を取得し、両方のアルゴリズムで検証を実施する。検証処理は、コンポジット署名構造に含まれるアルゴリズム識別子とパラメータに基づいて行われ、証明書の整合性も確認対象となる。

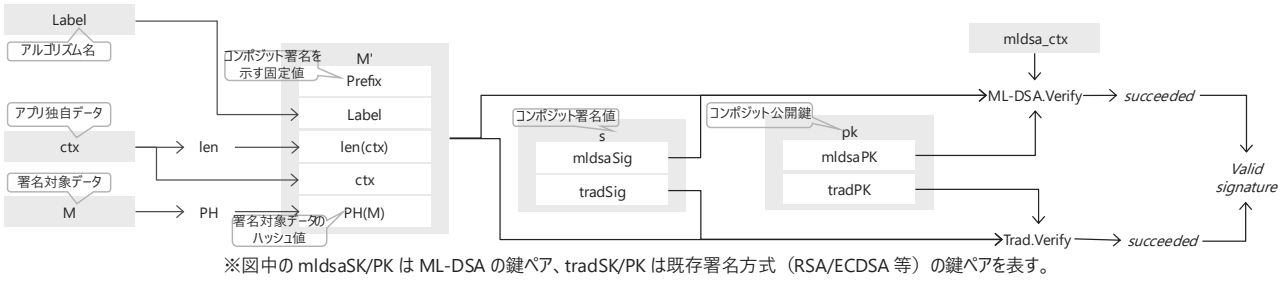


図 4-4 コンポジット署名検証の概要

また、表 4-3 のアルゴリズムリストが規定されている。

表 4-3 コンポジット署名のアルゴリズムリスト

OID Name	OID	Pre-Hash Function	ML-DSA Variant	Traditional Algorithm	Key Size / Curve
id-MLDSA44-RSA2048-PSS-SHA256	1.3.6.1.5.5.7.6.37	SHA256	ML-DSA-44	RSA	2048
id-MLDSA44-RSA2048-PKCS15-SHA256	1.3.6.1.5.5.7.6.38	SHA256	ML-DSA-44	RSA	2048
id-MLDSA44-Ed25519-SHA512	1.3.6.1.5.5.7.6.39	SHA512	ML-DSA-44	EdDSA	Ed25519
id-MLDSA44-ECDSA-P256-SHA256	1.3.6.1.5.5.7.6.40	SHA256	ML-DSA-44	ECDSA	secp256r1
id-MLDSA65-RSA3072-PSS-SHA512	1.3.6.1.5.5.7.6.41	SHA512	ML-DSA-65	RSA	3072
id-MLDSA65-RSA3072-PKCS15-SHA512	1.3.6.1.5.5.7.6.42	SHA512	ML-DSA-65	RSA	3072
id-MLDSA65-RSA4096-PSS-SHA512	1.3.6.1.5.5.7.6.43	SHA512	ML-DSA-65	RSA	4096
id-MLDSA65-RSA4096-PKCS15-SHA512	1.3.6.1.5.5.7.6.44	SHA512	ML-DSA-65	RSA	4096
id-MLDSA65-ECDSA-P256-SHA512	1.3.6.1.5.5.7.6.45	SHA512	ML-DSA-65	ECDSA	secp256r1
id-MLDSA65-ECDSA-P384-SHA512	1.3.6.1.5.5.7.6.46	SHA512	ML-DSA-65	ECDSA	secp384r1
id-MLDSA65-ECDSA-brainpoolP256r1-SHA512	1.3.6.1.5.5.7.6.47	SHA512	ML-DSA-65	ECDSA	brainpoolP256r1

id-MLDSA65-Ed25519-SHA512	1.3.6.1.5.5.7.6.48	SHA512	ML-DSA-65	EdDSA	Ed25519
id-MLDSA87-ECDSA-P384-SHA512	1.3.6.1.5.5.7.6.49	SHA512	ML-DSA-87	ECDSA	secp384r1
id-MLDSA87-ECDSA-brainpoolP384r1-SHA512	1.3.6.1.5.5.7.6.50	SHA512	ML-DSA-87	ECDSA	brainpoolP384r1
id-MLDSA87-Ed448-SHAKE256	1.3.6.1.5.5.7.6.51	SHAKE256	ML-DSA-87	EdDSA	Ed448
id-MLDSA87-RSA3072-PSS-SHA512	1.3.6.1.5.5.7.6.52	SHA512	ML-DSA-87	RSA	3072
id-MLDSA87-RSA4096-PSS-SHA512	1.3.6.1.5.5.7.6.53	SHA512	ML-DSA-87	RSA	4096
id-MLDSA87-ECDSA-P521-SHA512	1.3.6.1.5.5.7.6.54	SHA512	ML-DSA-87	ECDSA	secp521r1

4.3 ハイブリッド構成のプロトコル

4.3.1 通信プロトコル

本節では、通信プロトコルにおけるハイブリッド鍵共有の代表例として TLS 1.3 の構成を説明する。他にも、MLS における鍵素材の結合方式（draft-ietf-mls-combiner-02）、ETSI TS 103 744 にけるハイブリッド鍵共有方式、IEEE 802.11 におけるハイブリッド鍵共有の検討などが存在するが、本報告書では TLS 1.3 の事例に焦点を当てる。

TLS 1.3 のハイブリッド鍵共有は、ECDHE と KEM を用いた鍵共有とを独立に実行し、その結果を鍵導出で結合する合成(composite)方式に該当する。複数アルゴリズムの公開鍵や暗号文を送信する際に 連結アプローチが採用される。具体的には以下の通りである。

- KeyShareEntry.key_exchange フィールドに、構成アルゴリズムの key_exchange 値を連結して格納する。
- 追加の符号化や長さフィールドは不要で、アルゴリズムが固定されれば長さも固定される。
- NamedGroup がハイブリッド（例：MyECDHMyPQKEM）の場合、key_exchange は MyECDH.KeyGen()と MyPQKEM.KeyGen()の結果を連結したものになる。

```
例:
MyECDHMyPQKEM.KeyGen() = (MyECDH.KeyGen(), MyPQKEM.KeyGen())
KeyShareEntry {
    NamedGroup: MyECDHMyPQKEM,
    key_exchange: MyECDHMyPQKEM.KeyGen()
}
```

図 4-5 は、TLS 1.3 におけるハイブリッド鍵共有の処理手順を示すものである。ハイブリッド鍵共有では、従来の ECDHE と耐量子計算機性を有する KEM を用いた鍵共有(ephemeral)とを組み合わせ、複数の鍵素材を連結して利用する構成を採用する。クライアントおよびサーバは、それぞれ ECDHE と KEM を用いた鍵共有により 2 つの鍵を生成し、ClientHello メッセージにおいて公開鍵を

送信する。サーバは受信した公開鍵に基づき、ECDHE による共有秘密と KEM によるカプセル化処理を実行し、ServerHello メッセージでカプセル化データを返送する。

その後、クライアントはカプセル化データを復号し、ECDHE と KEM の結果を連結してハイブリッド共有秘密(ss_hybrid)を生成する。

この共有秘密は HKDF-Extract に入力され、ハンドシェイク用トラフィック秘密(handshake_secret)が導出され、client_handshake_traffic_secret(クライアント→サーバ方向のハンドシェイクメッセージを暗号化する鍵)および server_handshake_traffic_secret(サーバ→クライアント方向のハンドシェイクメッセージを暗号化する鍵)が生成される。以降の EncryptedExtensions、Certificate、CertificateVerify、Finished メッセージは、この秘密値に基づいて暗号化される。

図 4-5 は、鍵生成、カプセル化、デカプセル化、HMAC ベース鍵導出関数(HMAC-based Key Derivation Function: HKDF)による鍵生成、ハンドシェイクメッセージの暗号化までの一連の流れを視覚的に示している。

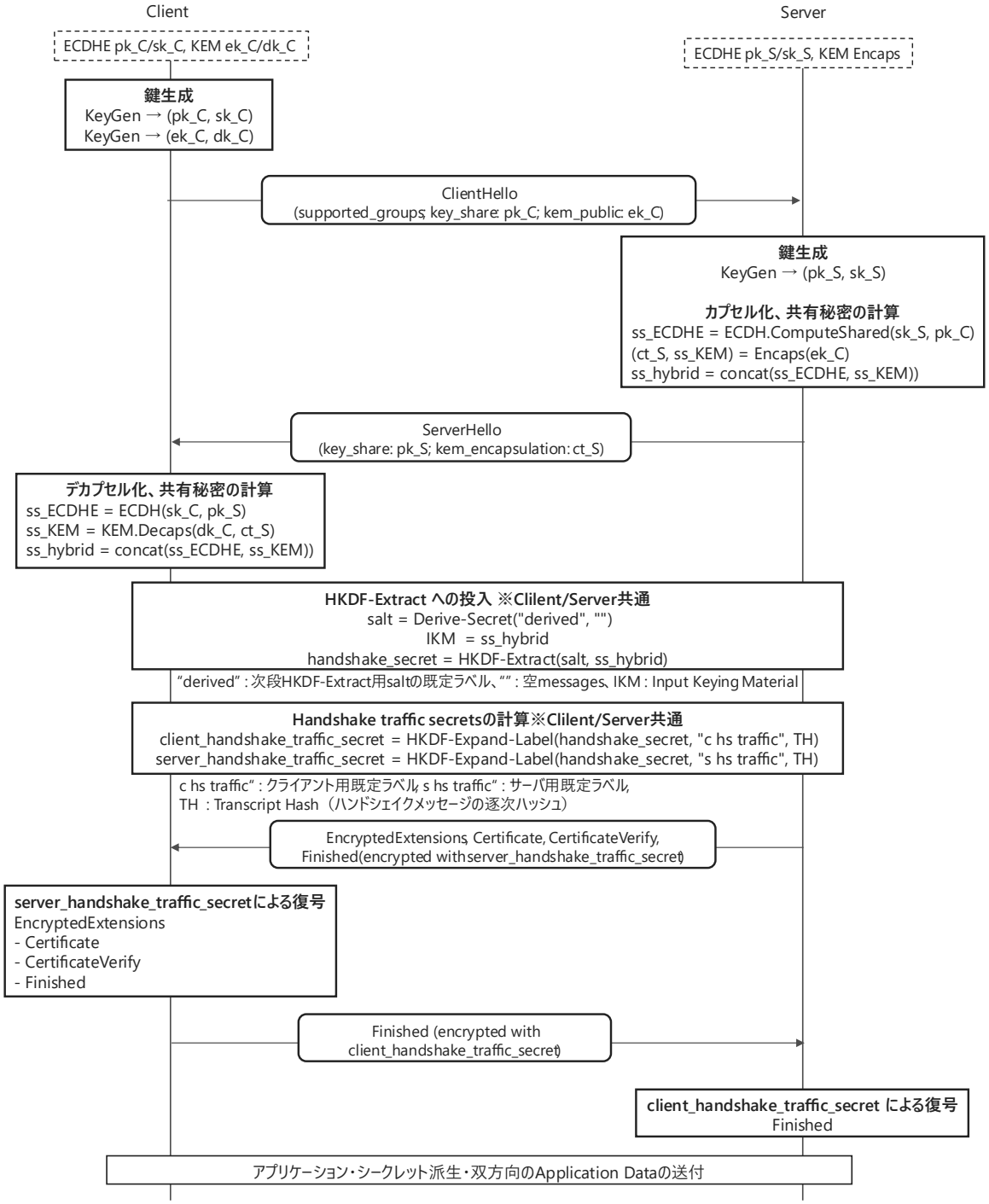


図 4-5 TLS 1.3 におけるハイブリッド鍵共有のシーケンス概要

4.3.2 証明書構造

本節では、ハイブリッド構成に対応した証明書構造の代表的な例を示し、それぞれの特徴を説明する。

図 4-6 は、ハイブリッド構成対応の証明書構造を示すものであり、後方互換性確保を目的とする方式と、安全性維持を目的とする方式の両方を含んでいる。なお、図中の名称（Discovery-enabled certificate、Dual-signature certificate、Composite-signature certificate）は、本報告書において説明の便宜上付与したものである。ハイブリッド構成の証明書構造には、標準化文書で定義された複数のアプローチが存在し、ここでは代表的な三つの例を示す。

1. Discovery-enabled certificate（draft-ietf-lamps-certdiscovery-02）
   本方式は、複数の証明書を並列に運用し、それらを証明書発見・選択可能とする構造である。Extensions フィールドに Subject Information Access を追加し、accessMethod および accessLocation により、関連する別の証明書(例：PQC または既存暗号)への参照情報を提供する。この方式では、既存の公開鍵暗号方式による証明書だけでも検証を継続できるため、2.1 節で定義する混成（hybrid）方式に該当する。
2. Dual-signature certificate（ITU-T X.509 Alternative cryptographic algorithms）
   本方式は、既存暗号の署名と PQ の署名をそれぞれ独立に保持する証明書構造である。Extensions フィールドに subjectAltSigAlg および subjectAltPubKey を追加し、追加の署名アルゴリズムと公開鍵を格納する。検証者は、従来署名のみを利用することも、PQC 署名を利用することも可能であり、移行期においてどちらの署名方式でも検証可能となる。このため、本方式は、2.1 節で定義する混成（hybrid）方式に該当する。
3. Composite-signature certificate（draft-ietf-lamps-pq-composite-sigs-14）
   本方式では、複数の署名アルゴリズム(既存暗号と PQC)を一体の署名構造として統合する。証明書には複数の公開鍵をまとめて保持し、署名アルゴリズムは

   CertSigAlg = MLDSA44-ECDSA-P256-SHA256

   のように、連結された単一の AlgorithmIdentifier として扱われる。この構成は、署名検証時にすべての構成署名が正しく検証される必要があるという前提のため、既存署名単独では利用できず、後方互換性を持たない。したがって本方式は2.1節で定義する合成(composite)方式に該当する。

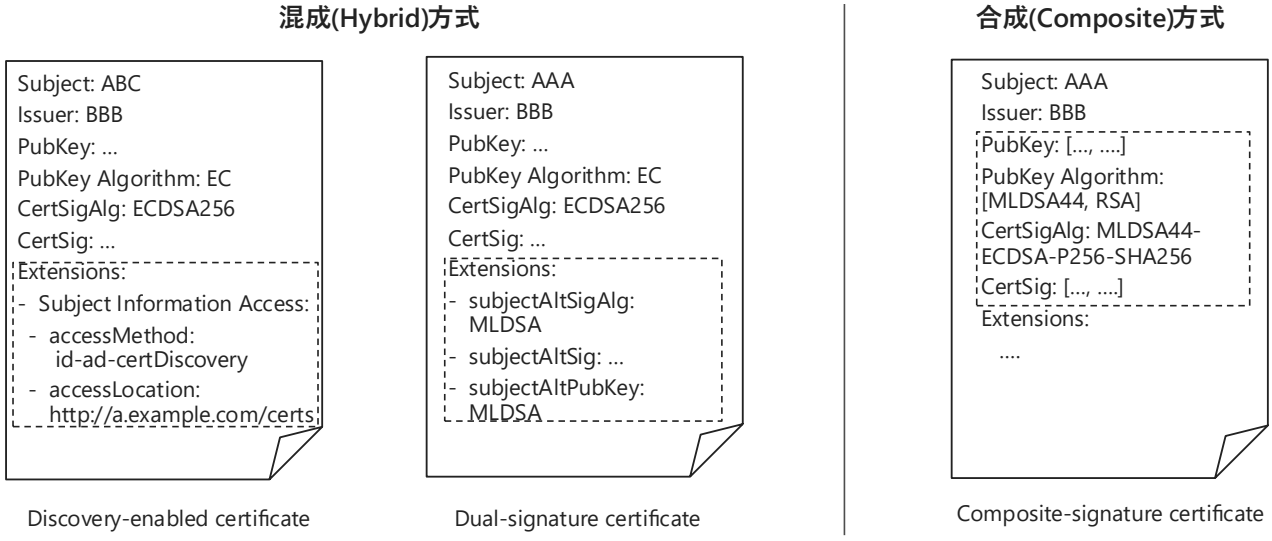


図 4-6 ハイブリッド構成における証明書構造の例

4.4 ハイブリッド構成のシステム

ハイブリッド構成は、アルゴリズムおよびプロトコルの設計のみならず、PKI 階層や証明書運用を含むシステムレベルの構成にも影響を及ぼす。近年では、PQC 移行を考慮した PKI 構成や電子メールシステムにおける段階的移行方式が検討されており、これらは実装・運用の観点から重要な論点となる。具体例については 6 章において詳述する。

5. ハイブリッド構成の安全性に関する解説

本章では、個別のアルゴリズム仕様やプロトコルの詳細な解説は行わず、標準化文書に記述されている内容を基に、ハイブリッド構成における安全性の整理を行う。特に、安全性がどのような条件で成立すると整理されているか、ならびにそれらの条件が鍵共有構成や合成構造、運用上の取扱いの中でどの構成要素に依存して具体化されているかに着目する。

5.1 脅威と移行前提

PQC への移行を扱う文書では、従来の公開鍵暗号が前提としてきた現在の計算機による攻撃に加え、将来の量子コンピュータの利用を想定した攻撃が整理されている。NIST IR 8547 [22]では、PQC への移行は段階的に進行するものであり、移行期間中は複数の暗号アルゴリズムが併存する状況が想定されている。

NIST SP 800-227 Section 4.6 [4]では、このような移行前提の下で、複数の鍵共有アルゴリズムを組み合わせるハイブリッド鍵共有アルゴリズム構成が示されている。これらの記述は、PQC への移行を一時点で完了することを前提としない構成が想定されていることを示している。

5.2 ハイブリッド構成に求められる性質

5.2.1 ハイブリッド構成の安全性の性質

RFC 9794 [23]では、既存の公開鍵暗号方式と耐量子計算機性を持つ暗号方式を組み合わせたハイブリッド構成に期待される性質として、秘匿性、認証、相互接続性、後方互換性、前方互換性を挙げている。以下、それぞれの性質について簡単に紹介する。

秘匿性（PQ/T hybrid confidentiality）：
秘匿性を実現するための構成要素である暗号方式のうち少なくとも 1 つ（たとえば ML-KEM）が安全であれば、ハイブリッド構成の秘匿性が実現されるという性質。

認証（PQ/T hybrid authentication）：
認証を実現するための構成要素である暗号方式の少なくとも 1 つ（たとえば ML-DSA）が安全であれば、ハイブリッド構成の認証が実現されるという性質。

相互接続性（PQ/T hybrid interoperability）：
当事者双方が、構成要素である暗号方式のうち少なくとも一つを共通にサポートしていれば、ハイブリッド構成のプロトコルを成功裏に完了できるという性質。

後方互換性（PQ/T backwards compatibility）：
当事者双方が既存の公開鍵暗号方式をサポートしていれば、ハイブリッド構成のプロトコルを成功裏に完了できるという性質。 [23]ではさらに、当事者双方が既存の公開鍵暗号方式と PQC 方式の両方をサポートしている場合には、その両方を用いることを要求している。

前方互換性（PQ/T hybrid forward compatibility）：
当事者双方が同じ PQC 方式の構成要素をサポートしている場合には、PQC 方式を用いて PQ/T ハイブリッド構成のプロトコルを成功裏に完了できるという性質。 [23]ではさらに、当事者双方が

既存の公開鍵暗号方式と PQC 方式の両方をサポートしている場合には、その両方を用いる選択肢を持つことを要求している。

上に挙げた性質のいくつかは互いに排他的であり、すべての性質を満たすハイブリッド構成を実現することはできない。例えば、相互接続性、後方互換性、前方互換性はいずれも相反する性質である。また、これらのいずれかが成立する場合、PQ/T ハイブリッド秘匿性（もしくは認証）を満たさない可能性がある。

なお、上記の性質の秘匿性と認証について、個別の暗号方式に対しては、それぞれ代表的な安全性を前提としている。鍵共有方式に対しては、IND-CCA（Indistinguishable under Chosen Ciphertext Attack）安全性が一般に設計上の前提条件として参照される一方、電子署名方式に対しては、EUF-CMA（Existential Unforgeability under Chosen Message Attack）や SUF-CMA（Strong Existential Unforgeability under Chosen Message Attack）といった偽造困難性に関する安全性定義が用いられている。本節では、個々の方式の安全性には立ち入らず、ハイブリッド構成における安全性成立条件との対応関係を整理する。

5.2.2 ハイブリッド署名と分離困難性

ハイブリッド署名構成の中で特に合成方式の基本的なアイデアは、署名において既存の公開鍵暗号の署名方式による署名値と PQC 署名方式による署名値を連結し、検証において 2 つの署名値がいずれも正しい場合に正当なハイブリッド署名と判定する。ハイブリッド構成の署名は、従来の署名に求められる安全性を満たす必要があるが、ハイブリッド署名特有の安全性要件として分離困難性（non-separability）が挙げられる。

簡単なハイブリッド署名の例として、メッセージ M に対して既存の公開鍵暗号による署名 $sig_T(M)$ と PQC 署名 $sig_{PQ}(M)$ を並べた（M, $sig_T(M)$, $sig_{PQ}(M)$）を考える。このとき、(M, $sig_T(M)$)は既存の公開鍵暗号のみをサポートするシステムにおいて正当な署名である。このような、ハイブリッド署名の一部を抜き出し、新たに正当なメッセージと署名の組を作る攻撃を stripping attack と呼ぶ。stripping attack は cross protocol attack の一種である。また、ハイブリッド署名から既存（もしくは PQC)の署名単体を取り出して使うので、ダウングレード攻撃の一種とみなすこともできる。

IETF は [24]の中で、stripping attack と、stripping attack に対する安全性として分離困難性（non-separability）について紹介している。分離困難性は、弱分離困難性と強分離困難性に分けられる。

弱分離困難性（weak non-separability）：
攻撃者が既存の署名もしくは PQC の署名のいずれかを痕跡を残さずに取り除くことはできないという性質。

強分離困難性（strong non-separability）：
攻撃者がメッセージとハイブリッド署名の組から、正しく検証に通る構成要素の署名を出力することができないという性質。

また、[24]では、強分離困難性よりも強い安全性として同時検証可能性を紹介している。

同時検証（simultaneous verification）：
ハイブリッド構成のすべての要素について検証が終わらない限り、ハイブリッド署名としての検証が完了しないという性質。

同時検証は、故障利用攻撃などの方法で検証の一部をスキップさせるような攻撃者に対する安全性を保証する。

分離困難性を実現する手段として、artifact と呼ばれる付加的な情報が用いられる。artifact は署名や公開鍵証明書など処理の各レイヤーに埋め込まれる情報である。Hybrid Signature Spectrums で定義される弱分離困難性と強分離困難性が、draft-ietf-lamps-pq-composite-sigs-14 では以下のとおり実現されている。

- 弱分離困難性
  draft-ietf-lamps-pq-composite-sigs-14 では、署名対象 M から構成される M′ (Section 2.2 の Prefix・Label・ctx を含むデータ) を ML-DSA と既存方式の双方に渡して署名を生成する。なお、ctx (context string) は、アプリケーション固有の文脈を示す補助データである。攻撃者が Composite ML-DSA 署名(M, (mldsaSig, tradSig))を分割しても、既存署名側には Prefix が静的に残るため、署名が composite 由来である痕跡が消えない。一方 ML-DSA 側では、ctx が Composite Algorithm の Label に設定されているため、ctx=""の通常の ML-DSA.Verify では検証に失敗する。
  この動作により、ML-DSA／従来方式いずれの署名も、単独署名として独立に再利用することができず、Hybrid Signature Spectrums が定義する弱分離困難性を満たしている。
- 強分離困難性
  draft-ietf-lamps-pq-composite-sigs-14 では、攻撃者が composite 署名から片側の署名を取り出し、異なるメッセージに対してその署名を単独署名として再利用し、対応する verifier に受理させることを難しくする仕組みが備わっている。ML-DSA 側は前述の ctx (=Composite Label) により ML-DSA 単独検証では成功しないため、限定的とはいえ強分離困難性を満たす。
  さらに X.509 では、署名対象に署名アルゴリズムの Label (＝Composite であることを示す識別子) が含まれるため、片側署名のみを残しても X.509 の検証処理で Composite として署名されているはずと判断され、検証が失敗する。
  また、draft-ietf-lamps-pq-composite-sigs-14 の Section 9.3 で規定される composite と単独署名の文脈で鍵を使い回さないという要件により、強分離困難性が実運用上さらに強化されることとなる。以上により、draft-ietf-lamps-pq-composite-sigs-14 は Hybrid Signature Spectrums の強分離困難性に対応する仕組みを備えている。

5.3 ハイブリッド鍵共有と前方／後方互換性

既存の公開鍵暗号による鍵共有プロトコルでは、DH 鍵共有などを用いて当事者間で共有秘密 (shared secret) を共有し、共有秘密と付加情報を鍵導出関数 (Key Derivation Function: KDF) に入力して通信の暗号化等に用いる鍵素材 (keying material もしくは derived keying material) を生成する。ハイブリッド鍵共有では、既存の公開鍵暗号による鍵共有を用いて共有された共有秘密 ss_T と、PQC の KEM を用いて共有された共有秘密 ss_{PQ} の両方を KDF に入力する。ハイブリッド構成を想定した KDF の使い方を鍵結合器 (key combiner) と呼ぶ。

5.3.1 NIST SP 800-56C Rev. [2]の KDF とハイブリッド KEM

NIST SP 800-56C Rev.2 [9]では、鍵共有処理により得られる共有秘密 Z から、鍵生成関数 (KDF) を用いて暗号処理に用いる鍵素材 (Derived Keying Material) を生成する手順が定義されている。

従来、共有秘密はNIST SP 800-56A, Bで共有された値を指していたが、NIST SP 800-56C Rev.2において、上記の共有秘密Zと「その他の方法」で共有された補助的な共有秘密Tを連結したZ’=Z||Tを共有秘密としてKDFの入力とする方法を規定した。この「その他の方法」としてPQC方式のKEMを用いることで、PQ/TハイブリッドKEM（鍵共有）を構成することができる。

5.3.2 NIST SP 800-227と鍵結合器

NIST SP 800-227 [4]は、ハイブリッドKEMを規定する文書であり、その概要は4.2.1節で説明した通りである。[4]第5章では、ECDHなど既存の鍵共有方法からKEMを構成する方法を与えている。また、 [4]4.6.3節において、複数のKEMで得た共有秘密から鍵素材を生成する鍵結合器を規定した。二つのKEM KEM1, KEM2の共有秘密をK1, K2とするとき、鍵結合器Key_Combineは

K ← Key_Combine(K1, K2)

で与えられる。また、鍵結合器はKEM1, KEM2のパラメータp1, p2、公開鍵をek1, ek2、暗号文をc1, c2などを補助入力として入力しても良い。Key_Combineを実現する方法として、NIST SP 800-56C Rev.2に記載の鍵導出方法（Key Derivation Method: KDM）およびNIST SP 800-133に記載の鍵導出関数が挙げられている。[4]はKDMやKDFに複数の共有秘密を入力する具体的なエンコード方法を規定していないが、一例として共有秘密をK=K1||K2と連結する方法を挙げている。

5.3.3 ハイブリッド鍵共有と前方／後方互換性

図 5-1は、NISTが2024年3月に公開した講演資料 [25]からの引用である。この図のように、鍵合成器を使うハイブリッド鍵共有はすべての方式で共通であるが、その考え方にはいくつかのバリエーションが存在する。

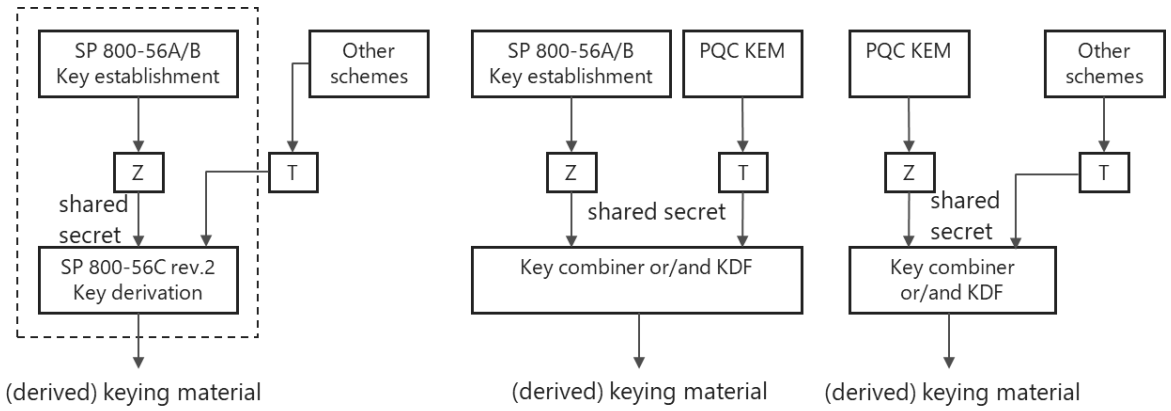


図 5-1 PQC暗号移行とKEMのハイブリッド構成［25］

まず、PQC方式のKEMや、KEMを用いた鍵共有プロトコルが標準化されていないPQC暗号移行の初期段階では、NIST SP 800-56C Rev.2の方法を用いる。すなわち、PQC方式を「その他の鍵共有方法」として、既存の標準の枠組みの中でハイブリッド鍵共有を実現する（図左）。この段階では既存の公開鍵暗号が主であり、PQC方式は補助的な役割である。したがって、PQC方式の共有秘密が用いられない場合があり得る。すなわち、この方式は後方互換性を満たす設定を許すが、その場合にはPQ/TハイブリッドKEM秘匿性を満たさない。

図中央はPQC暗号移行の中間的な段階であり、NIST SP 800-227がこれに該当する。この段階では、既存の公開鍵暗号とPQC方式が同格として扱われており、鍵素材の生成に両方の共有秘密を使うことが必須となる。したがって、この方式はPQ/T ハイブリッド秘匿性を満たすが、前方／後方

互換性のいずれも満たさない。

最後に、図右はPQC暗号移行の最終段階であり、PQC方式が主となり、補助的に「その他の鍵共有方法」を用いる。この方式は、前方互換性を満たす使用が可能であり、その場合にはPQ/Tハイブリッド秘匿性を満たさない。

6. ハイブリッド構成の実装・運用に関する解説

本章では、PQC およびハイブリッド構成の実装に関する主要な OSS の整備状況と、実運用環境における実装・移行事例を紹介する。暗号ライブラリ、PKI、メール、ブラウザなど多様な事例で得られた知見を通じ、移行期におけるハイブリッド構成の位置付けと実務上の課題を把握する。

6.1 実装基盤としての OSS 動向

PQC および既存暗号方式とのハイブリッド構成を実運用へ導入するにあたり、標準仕様の策定と並行して、実装基盤となる暗号ライブラリの整備状況を把握することが重要である。本節では、ハイブリッド構成の実装・検証において利用されている主要なオープンソースソフトウェア（OSS）として、Open Quantum Safe（OQS）プロジェクト [26]およびその成果物、ならびに主要な暗号ライブラリの動向を整理する。

OQS プロジェクトは、PQC アルゴリズムの実装およびそれらを既存プロトコルやライブラリへ統合するための検証基盤を提供することを目的とした OSS プロジェクトである。OQS プロジェクトの中核となる liboqs [27]は、PQC KEM や署名アルゴリズムの実装を提供する暗号ライブラリであり、これらを他の暗号ライブラリやプロトコル実装から利用可能とする役割を担っている。また、OQS-OpenSSL [28]は OpenSSL に liboqs を統合した派生実装であり、TLS をはじめとする既存プロトコル上で PQC およびハイブリッド方式の挙動を検証するための実装基盤として位置付けられる。

表 6-1 暗号ライブラリと仕様の対応関係

凡例　○：実装対象、△：限定的に実装対象、―：非実装対象

仕様 / 名称	CRFG Hybrid KEMs	Composite KEM	Composite signature	TLS Hybrid
liboqs (PQC アルゴリズムの実装 (KEM・署名))	△[6]	―	―	―
OQS-OpenSSL (OpenSSL に liboqs を統合した派生実装)	―	△[7]	△[7]	○
Bouncy Castle (Java を中心とした暗号アルゴリズムおよびプロトコル実装)	―	○	○	―
wolfSSL (組込み・軽量環境向けの TLS／暗号ライブラリ実装)	△[8]	―	―	○

一方、OQS プロジェクト以外にも、用途や実装方針の異なる暗号ライブラリが存在する。Bouncy Castle [29]は Java を中心とした暗号アルゴリズムおよびプロトコル実装を提供するライブラリであり、特に PKI／X.509 環境におけるコンポジット KEM（Composite KEM）やコンポジット署名（Composite Signature）の実装を通じて、ハイブリッド構成の実装を進めている。また、wolfSSL

6 CFRG Hybrid KEMs 構成における PQC KEM の実装要素として利用。

7 検証目的での限定対応。

8 TLS ハイブリッド鍵共有の用途に限定。

[30]は組込み・軽量環境を主な対象とする TLS／暗号ライブラリであり、TLS 1.3 におけるハイブリッド鍵共有の実装を中心に、実装規模や性能制約を考慮した対応が行われている。

表 6-1 は、これら主要な暗号ライブラリについて、ハイブリッド構成に関連する代表的な仕様に対する実装上の関与の度合いを整理したものである。本表における「○」「△」「－」は、それぞれ当該仕様が実装対象であるか、限定的・検証目的での対応にとどまるか、あるいは実装対象外であるかを示している。なお、ここで整理する対応関係は、正式な準拠宣言や仕様バージョンとの厳密な対応関係を示すものではなく、各暗号ライブラリが実装・検証の観点からどの仕様に関与しているかを俯瞰的に示すことを目的としている。

6.2 システム実装・運用の実例

本節では、PKI Consortium が主催する PQC 最新動向の国際的なカンファレンスである PQC Conference [31] [32]で報告された実装・運用事例の中から、PQC およびハイブリッド構成を既存システムへ導入する過程で顕在化した課題と、それに対して採られた実装上・運用上の判断を紹介する。ここで紹介する事例は、単に標準仕様に準拠した実装を行うことを目的としたものではなく、既存システムとの互換性、性能や運用負荷、ベンダ対応状況といった現実的制約を踏まえ、段階的導入や暫定構成を採用している点に特徴がある。

また、Chrome は、PQC への早期対応を目的としてハイブリッド鍵共有の導入を進めており、その実装過程ではプロトコル更新だけでなく、ネットワーク機器との互換性や段階的展開といった実運用上の課題が顕在化した。本節では、Chrome における実装の変遷とそこから得られた知見を紹介する。

6.2.1 実運用を想定した PQC 移行および性能評価の事例

Michiel Marcus (TNO), “Real-World Post-Quantum Migrations: Lessons Learned and Performance Results” ― OQS を用いた OpenSSL ベースの暫定的ハイブリッド構成 ― [33]

課題

既存アプリケーションにおける暗号処理はコード全体に分散して実装されており、RSA や ECC といった特定アルゴリズムへの依存が強く、PQC への単純な置換が困難であった。加えて、利用するベンダ製品が PQC に未対応であるという制約の下で移行検討を進める必要があった。

対応・工夫

暗号アルゴリズムを抽象化する設計へと段階的に改修し、crypto-agility を確保した上で、PQC および既存暗号を組み合わせたハイブリッド構成を追加した。これにより、将来的なアルゴリズム変更にも対応可能な基盤を整備した。

運用上の判断

ベンダ製品の PQC 対応が未成熟である状況を前提に、OQS を用いた OpenSSL ベースのリバースプロキシを暫定的に配置し、アプリケーション本体を変更することなく評価・計測を可能とする構成を採用した。

知見

ハイブリッド構成による性能低下は当初想定より限定的であり、多くのケースで最大でも数十パーセント程度に留まることが確認された。一方で、暗号依存関係の整理と crypto-agility の確保が移行コストを大きく左右する重要な要因であることが明らかとなった。

6.2.2 Web PKI における段階的 PQC 導入の事例

Shane Kelly (DigiCert), “The Internet Is Ready for Some PQC Certificates” [34]

課題

Web PKI において証明書チェーン全体を純粋な PQC へ置き換えた場合、証明書サイズやハンドシェイク時の転送量が大幅に増加し、既存ブラウザやインターネット環境への影響が懸念された。

対応・工夫

PKI 全体を一括で置き換えるのではなく、エンドエンティティ（リーフ）証明書から段階的に PQC 署名を導入する構成を採用した。

運用上の判断

証明書の有効期間を短縮することで、失効や強制的な更替を伴わずにアルゴリズム移行を進められる運用モデルが提案された。

知見

ハイブリッド構成を用いることで、完全な PQC 化に伴うサイズ・性能影響を抑えつつ、実運用環境での検証と経験蓄積を同時に進められることが示された。

6.2.3 PKI 階層設計におけるハイブリッド活用の事例

Mike Ounsworth (Entrust), “Architecting PKI Hierarchies for Graceful PQ Migration” [20]

課題

PKI 階層ごとに求められるセキュリティ要件や性能要件が異なり、単一アルゴリズムによる統一が必ずしも合理的でなかった。

対応・工夫

複数証明書方式、Composite、代替公開鍵拡張など、用途に応じたハイブリッド手法を組み合わせる「ツールボックス型」の設計が採用された。

運用上の判断

TLS などの交渉型プロトコルと、S/MIME 等の非交渉型用途で異なる方式を使い分けることで、後方互換性と移行容易性の両立が図られた。

知見

ハイブリッドは単一の方式としてではなく、用途に応じた設計上の選択肢群として扱う必要があることが示された。

6.2.4 S/MIME 電子メールにおけるハイブリッド実装の事例

Jan Klaußner (Bundesdruckerei), “Hybrid PQC E-Mail Communication: Easing Migration Pain” [21]

課題

S/MIME 電子メールでは、既存クライアントが複数署名や複数証明書を前提としておらず、単純な並列方式ではユーザ体験や互換性に問題が生じた。

対応・工夫

Composite 方式や代替鍵方式を用いることで、証明書構造を大きく変えずに PQC と既存暗号を統

合する実装が試行された。

運用上の判断

メールクライアント側の変更を最小限に抑えるため、暗号ライブラリ層での対応を重視し、アプリケーション層の変更を回避した。

知見

ハイブリッド構成では、暗号方式の選択に加え、既存クライアントの期待するデータ構造との整合を考慮する必要があることが明らかとなった。

6.2.5 ブラウザにおけるハイブリッド実装の事例(Chrome)

背景

Chrome は 2023 年に X25519Kyber768 を TLS で導入し、耐量子計算機性の確保に向けたハイブリッド鍵共有の検証を開始した。これは TCP／QUIC 双方を対象とした初期展開であり、当時の Kyber は標準化前のドラフト段階であった [35]。

実装

Kyber の標準化後、Google は自社で管理する TLS 暗号ライブラリである BoringSSL に ML-KEM を実装し、TLS のハイブリッド KEM コードポイントを Kyber（0x6399）から ML-KEM（0x11EC）へ移行した。Chrome131 以降では ML-KEM への一本化が予定されている [36]。

互換性問題

ハイブリッド KEM により ClientHello のサイズが 1KB 以上増加し、通信経路上で TLS メッセージを検査・中継するネットワーク機器（middlebox）が大きなメッセージを処理できず動作不良が発生したことが報告されている [35]。

問題対応

こうした非互換を把握するため、Chrome は段階的展開を行い、ネットワーク経路機器との互換性を継続的に検証する運用方針を採った [35]。

知見

ブラウザのようにクライアント側が先行して PQC を導入すると、ネットワーク機器が追随できず互換性問題が顕在化する一方、段階的展開によりエコシステム全体の問題を早期に露出させ、改善を促進できることが示された [35]。

6.2.1 節から 6.2.4 節の事例に共通する点として、PQC 移行は単なる暗号アルゴリズムの置換ではなく、システム構成、アーキテクチャ、運用手順を含めた包括的な設計変更として捉える必要があることが示されている。さらに、6.2.5 節で示した Chrome の事例は、クライアント側が先行して PQC を導入した場合、ネットワーク機器との非互換が顕在化し得ること、そして段階的展開や検証体制がエコシステム全体の移行に重要な役割を果たすことを示している。これらの事例は総じて、ハイブリッド構成が、移行期間を現実的に支えるための実用的な選択肢として位置付けられていることを裏付けている。

7. PQC 移行に関わる標準化動向の調査結果

本章では、PQC 移行期におけるハイブリッド方式の取り扱いに着目し、国際的な標準化団体および関連組織における検討状況を整理する。調査対象の選定にあたっては、CRYPTREC が公表した「ハイブリッドモード[1]の技術動向調査」 [3]による調査報告書を参照しつつ、その後の標準化動向や産業界での議論を踏まえて補完を行い、2026 年 1 月時点で PQC 移行やハイブリッド方式に関して実質的な情報発信を行っている組織を対象としている。

具体的には、NIST、IETF、ETSI、ISO、IEEE といった標準仕様策定機関に加え、国家レベルの暗号利用方針を示す機関、産業分野における実務的整理を行う団体、ならびに研究成果や知見を共有する国際的なプロジェクトや連合体を含めて調査対象としている。本章で扱う組織には、狭義の国際標準策定機関に限らず、標準化活動を補完する立場の組織が含まれる。

調査では、「hybrid」「composite」「multi-algorithm」等の用語を手掛かりとして、各組織が公開する標準文書、技術仕様、ガイドライン等を対象に情報収集を行い、鍵生成、デジタル署名、証明書、通信プロトコルにおけるハイブリッド構成の設計方針や運用上の位置付けに着目した。7.1 節から 7.11 節にかけて各組織の動向を整理することで、PQC 移行期におけるハイブリッド方式の全体像を俯瞰的に把握することを目的とする。

表 7-1 調査対象組織の一覧

章・節番号	組織名	URL
7.1	National Institute of Standards and Technology (NIST)	https://www.nist.gov/
7.2	Internet Engineering Task Force (IETF)	https://www.ietf.org/
7.3	International Telecommunications Union (ITU)	https://www.itu.int/
7.4	European Telecommunications Standards Institute (ETSI)	https://www.etsi.org/
7.5	Institute of Electrical and Electronics Engineers (IEEE)	https://www.ieee.org/
7.6	International Organization for Standardization (ISO)	https://www.iso.org/
7.7	ANSI Accredited Standards Committee X9 (ASC X9)	https://x9.org/
7.8	National Security Agency (NSA)	https://www.nsa.gov/
7.9	Cloud Security Alliance (CSA)	https://cloudsecurityalliance.org/
7.10	PQCRYPTO	https://pqcrypto.eu.org/
7.11	Post-Quantum Cryptography Coalition (PQCC)	https://pqcc.org/

7.1 National Institute of Standards and Technology (NIST)

7.1.1 組織概要

米国国立標準技術研究所（National Institute of Standards and Technology: NIST）は、米国

商務省傘下の連邦機関として、計測標準、情報技術、サイバーセキュリティ分野における国家標準および技術ガイダンスを策定・公開している。暗号技術分野では、DES、AES、SHA シリーズをはじめとする基幹暗号標準を提供してきた実績を有し、その成果は米国政府のみならず国際的にも広く参照されている。NIST の暗号標準化の特徴は、アルゴリズム仕様にとどまらず、実装、運用、移行といった実務的観点を重視している点にある。標準は FIPS として制定される一方、Special Publication (SP) および Interagency Report (IR) を通じて、技術的背景や移行戦略、設計上の留意事項が体系的に補完されている。PQC についても、NIST は既存暗号資産を前提とした段階的移行問題として位置付け、従来暗号と PQC を併用するハイブリッド方式を移行期の重要な選択肢として明確に示している。

7.1.2 PQC およびハイブリッド構成に関する標準化動向

NIST における PQC 標準化は、2016 年に公開された Call for Proposals [37]を起点として開始された。量子コンピュータの将来的な実用化による現在の公開鍵暗号の破綻リスクを背景として、耐量子計算機性を有する新たな鍵共有方式と署名方式の公募と長期評価が実施されてきた。

PQC アルゴリズム選定と並行して、既存暗号から PQC への移行方法そのものが重要な検討対象とされており、NIST IR 8547 [22]では移行期における主要な選択肢が提示されている。同文書では、単一の PQC アルゴリズムへの移行だけでなく、PQC と量子コンピュータに対して脆弱な暗号を組み合わせるハイブリッドソリューションの役割とトレードオフが提示されている。

NIST IR 8547 では、ハイブリッドソリューションは「構成アルゴリズムの少なくとも一つが安全である場合に全体の安全性が維持される」方式として説明されており、将来のアルゴリズム安全性に関する不確実性に対応する手段と位置付けられている。また、既存暗号の継続利用要件がある場合の移行パスとしても利用される。一方で、実装やアーキテクチャの複雑化、運用コストの増大といったトレードオフが存在し、NIST はこれらを PQC への完全移行までの暫定的措置として位置付けている。

ハイブリッドソリューションに関連する具体的技術は以下のとおりである。

- Hybrid Key-Establishment Techniques
  - Hybrid Key-Establishment は複数の鍵共有方式を組み合わせた構成であり、本報告書では合成 (composite) に相当する。
  - NIST は NIST SP 800-56C Rev.2 に記載された汎用合成鍵共有の利用を許容している。Z’ = Z || T は shared secret として扱われ、NIST SP 800-56C Rev.2 の任意の鍵導出方式を Z’に適用して鍵素材を導出することができる。
    Z：NIST SP 800-56A または NIST SP 800-56B に従って生成された shared secret
    T：その他のスキームにより生成・配布される shared secret
  - NIST は NIST SP 800-56C Rev.2 を改訂し、Z が現在および将来の NIST 鍵共有規格に基づき生成されることを許容する予定。Z を生成できる方式として、NIST SP 800-56A、NIST SP 800-56B、FIPS 203 (ML KEM) 、将来の PQC KEM 標準が含まれる。
  - NIST は、鍵結合器 (Key Combiner) に関する追加ガイダンスを、今後公開予定の NIST SP 800-227 で提供する予定である。[9]
- Hybrid Digital Signature Techniques
  - Hybrid Digital Signature とは同一メッセージに対して 2 つ以上の署名を付与する方式 dual signatures である。本報告書の用語の定義では、合成(composite)に

[9] 引用元の NIST IR 8547(2024 年)の時点では未公開であったが、本報告書執筆時点では NIST SP 800-227(2025 年)として発行されている。

あたる。

- 検証時には、構成要素となるすべての署名が正しく検証される必要がある。
- dual signatures は、文書や電子メールなどのユーザデータ、あるいはデジタル証明書の署名に利用できる。
- NIST の既存標準およびガイドラインは、少なくとも 1 つの署名アルゴリズムが NIST 承認である限り、dual signatures の利用を許容している。

これら方針や仕様の実運用における妥当性は、NIST SP 1800-38C [38]において、TLS や X.509 等の既存プロトコルを対象とした相互運用性および性能評価として報告されており、NIST の PQC 移行戦略が理論にとどまらないことを裏付けている。

7.1.3 技術仕様におけるハイブリッド構成の詳細

本節では、NIST SP 800-227 Section 4.6「Multi-Algorithm KEMs and PQ/T Hybrids」 [4]に基づき、鍵共有におけるハイブリッド構成の設計思想および技術仕様を整理する。Section 4.6 では、複数の鍵カプセル化（Key Encapsulation Mechanisms: KEMs）を並行して用い、それぞれから得られる共有秘密を安全に合成する Multi-Algorithm KEM（Composite KEM）が定義されている。特に、耐量子計算機暗号（Post-Quantum: PQ）KEM と既存の（Traditional: T）KEM を組み合わせた構成は、PQ/T Hybrid として位置付けられている。Multi-Algorithm KEM の基本構造は、各 KEM による独立したカプセル化処理、複数の共有秘密の取得、そして鍵結合器(キーコンバイナ)による最終共有鍵への統合から構成される。合成後の共有鍵が、少なくとも共有鍵の生成に使用された一つの KEM が安全である限り安全性を維持することを目標としている。ただし、この性質は自動的に保証されるものではなく、キーコンバイナには NIST SP 800-56C Rev.2 で規定された承認済み鍵導出手法を用いることが要求されている。なお、Section 4.6 に示される Multi-Algorithm KEM の手法概要と構築方法に関しては、本報告書の 4.2 節に示しているため、本節では記載を割愛する。

また、Section 4.6 では Composite KEM のセキュリティ考慮事項として、複数方式を併用することによって実装やプロトコルが複雑化し、プロトコル内に追加の選択肢が生じることでダウングレード攻撃などのリスクが発生し得る点にも言及している。

NIST は、Multi-Algorithm KEM および PQ/T Hybrid を恒久的な解決策とは位置付けておらず、あくまで移行期における暫定的手段として利用し、長期的には単一の PQC 方式へ収束させることを想定している。

7.2 Internet Engineering Task Force (IETF)

IETF の各種 WG および IRTF の CFRG の状況は以下の通りである。本節では、RFC 若しくは WG Draft の文献を対象とする。

7.2.1 Transport Layer Security Working Group (TLS WG)

- WG 概要

  TLS WG は IETF においてインターネット上の安全な通信を実現する Transport Layer Security(TLS)の仕様策定を担うワーキンググループである。TLS 1.3(RFC 8446)を基盤に、暗号アルゴリズムの更改、拡張機能、運用上の相互運用性を継続的に整備している。耐量子計算機性への対応として、TLS 1.3 の鍵共有方式において複数の KEM を組み合わせて利用するハイブリッド KEM の設計を WG ドラフト（draft-ietf-tls-hybrid-design-16）で提示して

いる。

- PQC およびハイブリッド構成に関する標準化動向
  draft-ietf-tls-hybrid-design-16 では、TLS 1.3 の鍵共有方式として複数の KEM を組み合わせるハイブリッド KEM を定義している。主要な仕様は次の通りである。

  - NamedGroup の設計：
    NamedGroup に、複数の KEM から構成される順序付き組を定義し、ハイブリッド構成として登録する。例えば、従来の ECDH ベースの鍵共有と耐量子計算機性を備えた KEM を用いた鍵共有を組み合わせた構成を MyECDHMyPQKEM のような 1 つの NamedGroup として扱い、これを TLS 1.3 の既存 NamedGroup と同様に、ClientHello／ServerHello で提示・選択されるネゴシエーション対象として登録する形式が示されている。
  - key_share の構造：
    key_share の KeyShareEntry.key_exchange には、選択対象となる NamedGroup に含まれる各 KEM の公開鍵／暗号文を固定長で連結して格納する。これらは TLS 1.3 の ClientHello／ServerHello における supported_groups および key_share 拡張の交換を通じてネゴシエーションされ、サーバが特定の NamedGroup を選択することで、最終的に鍵共有方式が合意される。
  - shared_secret の連結と HKDF の扱い：
    各々の KEM を用いた鍵共有から得られた shared_secret は、前段で選択された NamedGroup に対応する key_share の値からそれぞれ導出され、これら複数の shared_secret を連結したものを TLS 1.3 の既存 HKDF 鍵スケジュールに入力する。

  また、運用上の論点として、ClientHello に関する通信量の増加、KEM 固有の失敗確率に伴うハンドシェイク再試行、IANA Supported Groups へのハイブリッド組登録、TLS を UDP 化したプロトコル Datagram TLS への適用可能性が挙げられている。
  なお、ハイブリッド化の目的は、暗号移行に伴う不確実性に備える設計目標として示されている一方で、本ドラフトでは formal security proof（数学的モデルに基づく安全性証明）を提供していない。本ドラフトは構成要素となる KEM の種類を限定せず、特定方式に依存しないハイブリッド構成を想定する。

- 技術仕様におけるハイブリッド構成の詳細
  TLS 1.3 におけるハイブリッド鍵共有の具体的な手順については、4.3.1 節において図示しているため、本節では詳細説明を割愛する。

7.2.2 Limited Additional Mechanisms for PKIX and SMIME Working Group (LAMPS WG)

- WG 概要
  LAMPS WG は、IETF において X.509 証明書、PKIX、S/MIME、CMS 等に関する拡張仕様を策定するワーキンググループであり、既存 PKI 基盤との後方互換性を維持しつつ、暗号技術の拡張・進化を可能とする仕組みの標準化を担っている。PQC 移行期においては、証明書形式やアルゴリズム識別子、鍵および署名の表現方法が既存 PKI 基盤に与える影響が大きいため、LAMPS WG は TLS 等の通信プロトコル層とは異なり、証明書・署名・鍵管理といった PKI レイヤーに焦点を当てた標準化を進めている。

- PQC およびハイブリッド構成に関する標準化動向
  LAMPS WG における PQC への対応は、証明書および PKIX データ構造において PQC 単独方式とハイブリッド方式の共存を可能にすることを基本方針として進められている。中心的な取り組みとして、PQC と従来暗号を組み合わせた合成方式（Composite）の標準化が挙げられ、署名および鍵カプセレーションの双方について Internet-Draft が策定されている。

合成署名については、「Composite ML-DSA for use in X.509 Public Key Infrastructure」（draft-ietf-lamps-pq-composite-sigs-14） [12]において、ML-DSA（FIPS 204）と既存署名アルゴリズム（RSA、ECDSA、EdDSA 等）を組み合わせた Composite 署名方式が定義されている。これは単一の AlgorithmIdentifier として扱える設計を採用しており、既存の PKI 実装や証明書検証ロジックを大きく変更することなく、PQ/T ハイブリッド署名を導入可能とする点に特徴がある。

鍵共有に関しても、「Composite ML-KEM for use in X.509 Public Key Infrastructure」（draft-ietf-lamps-pq-composite-kem-12） [11]において、ML-KEM（FIPS 203）と RSA-OAEP や ECDH を組み合わせた Composite KEM が定義されている。これらの仕様は RFC 9794 で整理された PQ/T ハイブリッドの設計思想を PKIX 環境に適用するものであり、移行期におけるリスク低減を主目的としている。

さらに、「A Mechanism for X.509 Certificate Discovery」（draft-ietf-lamps-certdiscovery-02） [18]により、複数証明書を関連付けて発見可能とする仕組みが提案されており、PQC 証明書と従来証明書の併用や段階的切り替えを支援する基盤技術として位置付けられる。

なお、具体的な仕様に関しては、本報告書の 4.2 節に示しているため、本章では記載を割愛する。

7.2.3 Messaging Layer Security Working Group（MLS WG）

- WG 概要

  MLS WG は、IETF においてエンドツーエンド暗号化（E2EE）を前提としたセキュアなグループメッセージング基盤の標準化を担う作業部会である。主成果物である RFC 9420（Messaging Layer Security: MLS）は、大規模かつ動的な参加者集合を想定した効率的な鍵更新および前方秘匿性を実現するプロトコルとして位置付けられている。MLS WG では、実運用を意識した拡張性や長期安全性の確保が重視されており、PQC を含む次世代暗号技術の段階的導入についても継続的に検討が進められている。

- PQC およびハイブリッド構成に関する標準化動向

  MLS WG における PQC 対応の検討は、量子計算機の進展を見据えた長期機密性確保への対応を背景として進められている。RFC 9420 自体は従来暗号を前提としているが、その拡張として、PQC アルゴリズムを直接適用する方式や、既存の暗号方式と PQC を組み合わせるハイブリッド方式が議論されている。特に、計算量や通信量の増大という PQC 固有の課題に対し、効率性と安全性のバランスを取る実装手法が重要視されている。参考文献である draft-ietf-mls-combiner-02 [15]は、従来 MLS セッションと PQC MLS セッションを組み合わせる償却型ハイブリッド手法を提案しており、MLS WG における PQC 適用方針を具体化する中核的文書と位置付けられる。

- 技術仕様におけるハイブリッド構成の詳細

  draft-ietf-mls-combiner-02 [15]では、Amortized Post-Quantum MLS（APQ-MLS）Combiner と呼ばれる方式が定義されている。draft-ietf-mls-combiner-02 で定義される仕様は以下のとおりである。また、図 7-1 は本仕様の構造を視覚的に示したものであり、APQ-MLS Combiner の実装および性能評価を提示した学術論文 [39]の図を引用している。

  - 本方式では、1 つの PQ MLS セッションと 1 つの従来 MLS セッションを並行して運用し、PQ セッションで生成される exporter secret を従来セッションに取り込むことで、従来セッションに PQ 保証を付与する仕組みである。
  - 図中で示される Partial Update は、従来セッションのみで行われる通常の鍵更新であり、PQ 演算を伴わない。一方、Full Update は PQ セッションの exporter secret を従来セッションに注入して鍵スケジュールを更新する処理であり、従来セッションが PQ 安全性を獲得する更新である。

- APQ-MLS では、Partial Update と Full Update を柔軟に組み合わせることで、PQ 演算の計算量やメッセージサイズの増大を抑えつつ、MLS に求められる頻繁な鍵更新要求に対応できるよう設計されている。

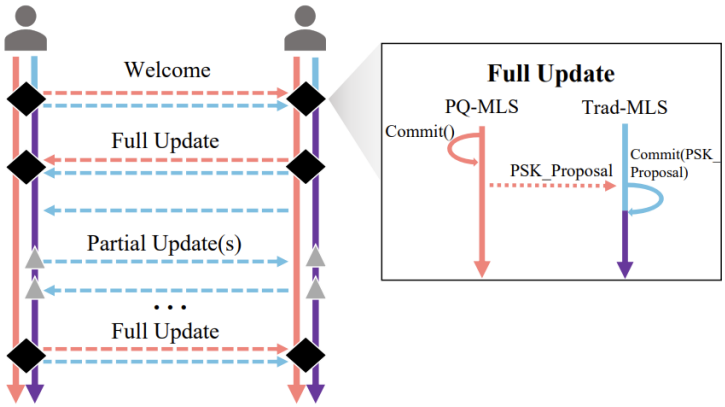


図 7-1 APQ combiner の概要 [39]。PQ MLS セッションの exporter secret を用いて、従来 MLS セッションに PQ 保証を注入する構造を示す。Partial Update は従来セッションのみで鍵更新を行い、Full Update は PQ セッションの秘密値を取り込み PQ 保証を付与する。

7.2.4 Post-Quantum Use in Protocols Working Group (PQUIP WG)

- WG 概要

  PQUIP WG は、IETF における PQC 移行期のプロトコル設計・運用指針を横断的に整理するために設置されたワーキンググループである。TLS、PKIX／LAMPS、IPsecME など個別 WG の仕様検討を補助する立場から、用語の標準化、ハイブリッド（PQ/T）方式に関する設計目標、セキュリティ特性、証明書モデルの整理などを担う。特に署名に関しては「ハイブリッド署名のスペクトラム」を提示し、非分離性（WNS／SNS）や同時検証（SV）などの概念を共有化することで、プロトコルや PKI における一貫した導入・検証を支援する。

- PQC およびハイブリッド構成に関する標準化動向

  PQUIP WG の中心成果として、PQ/T ハイブリッド方式の共通用語を定義する RFC 9794 [23]が 2025 年 6 月に発行された。同 RFC は、PQ/T ハイブリッド方式に関する用語体系を以下の 4 区分に基づき体系化している。各区分における具体的な定義内容は表 7-2 から表 7-5 に示すとおりである。

  - Primitives（暗号要素）：暗号方式の分類およびマルチアルゴリズム構成の基本概念を定義する。
  - Protocols（プロトコル）：ハイブリッド方式を取り扱うための鍵共有モデルやプロトコル構造を定義する。
  - Properties（性質）：PQ/T モードにおける秘匿性・認証性・相互運用性・後方／前方互換性などの成立条件を定義する。
  - Certificates（証明書モデル）：移行期の証明書構造や PQ/T 共存のための証明書モデルを定義する。

  併せて、インフォメーション目的の Internet-Draft「Hybrid signature spectrums」(draft-ietf-pquip-hybrid-signature-spectrums-07) [24]では、RFC 9794 で整理された PQ/T ハイブリッド方式の分類を署名分野に特化して拡張している。本ドラフトは以下の 6 区分から構成され、ハイブリッド署名の設計・検証に必要となる概念を体系的に示している。各区分における具体的な定義内容は**表 7-6** から表 7-11 に示すとおりである。

- Terminology（基本概念）：ハイブリッド署名方式、構成要素、攻撃モデル、アーティファクトなどの基礎語彙を整理する。
- Goals（設計目標）：ハイブリッド署名が満たすべき安全性・互換性・非分離性等の指標を示す。
- Non-Separability Spectrum（非分離性スペクトラム）：署名の分離困難性を段階的に分類し、強度の違いを示す。
- Artifacts(痕跡の種別と配置):message･certificate･signature･protocol／policy のどこにハイブリッド方式であることの痕跡を配置するかを分類する。
- Need for Approval Spectrum（承認要件の分類）：FIPS 140 を含む既存承認モジュールとの関係性を踏まえ、ハイブリッド方式が必要とする承認レベルを分類する。
- EUF-CMA Challenges（偽造困難性に関する課題）：コンポーネント偽造、鍵再利用、分離困難性との関係など、安全性分析における注意点やハイブリッド署名を構成する要素と攻撃モデルを整理する。

- RFC 9794 における用語の定義

表 7-2 Primitives(暗号要素) [23]

用語	定義
Traditional asymmetric cryptographic algorithm	整数因数分解･離散対数問題等に基づく既存の公開鍵暗号
Post-quantum asymmetric cryptographic algorithm	耐量子計算機性を持つ公開鍵暗号
Component asymmetric algorithm	マルチアルゴリズム方式において使用される単一の公開鍵暗号
Single-algorithm scheme	単一の公開鍵暗号アルゴリズムを使用する暗号方式
Multi-algorithm scheme	暗号操作(署名や鍵共有など)を行うために、複数の公開鍵暗号アルゴリズムを使用する暗号方式
PQ/T hybrid scheme	少なくとも 1 つの PQC と、少なくとも 1 つの既存の公開鍵暗号を構成要素とするマルチアルゴリズム方式

表 7-3 Protocols(プロトコル) [23]

用語	定義
PQ/T hybrid protocol	PQC と既存の暗号アルゴリズムを組み合わせたハイブリッド方式を利用するプロトコル
Composite key establishment	マルチアルゴリズム鍵共有方式を単一アルゴリズム方式の代替として組み込む方式
Non-composite key establishment	複数の鍵共有方式を、プロトコル内部でそれぞれ独立して実行する方式

表 7-4 Properties(性質) [23]

用語	定義
PQ/T hybrid confidentiality	PQ/T ハイブリッド構成に含まれる複数アルゴリズムのうち、少なくとも 1 つが機密性を保持している限り、全体として機密性が維持される性質
PQ/T hybrid authentication	PQ/T ハイブリッド署名に含まれる複数の署名方式のうち､少なくとも 1 つが署名の安全性を保持している限り、全体として認証が成立する性質
PQ/T hybrid interoperability	通信当事者がサポートするアルゴリズム集合に、少なくとも 1 つの共通構成要素が存在する場合に、プロトコルとして相互運用を維持できる性質
Backwards compatibility	従来方式しか扱えない検証者であっても、ハイブリッド署名に含まれる従来方式の署名部分のみを検証して受理できる互換性の性質
Forwards compatibility	将来の PQC 完全対応環境において、ハイブリッド署名の PQC 署名部分のみ、あるいは両方を選択的に利用できる柔軟性を指す性質

表 7-5 Certificates(証明書モデル) [23]

用語	定義
PQ/T hybrid certificate	PQC の公開鍵と既存の暗号方式の公開鍵を含む単一証明書
Post-quantum certificate	PQC 署名アルゴリズムのみを含む証明書
Traditional certificate	既存の署名アルゴリズムのみを含む証明書
PQ/T hybrid certificate chain	各証明書が PQ/T 署名を用いる証明書チェーン(エンドエンティティ証明書からルート認証局証明書までの階層構造)
PQ/T parallel PKI	PQC 証明書チェーン(エンドエンティティ証明書からルート認証局証明書までの階層構造)と既存の証明書チェーン(エンドエンティティ証明書からルート認証局証明書までの階層構造)を並列利用

- Hybrid signature spectrums におけるハイブリッド署名の体系

表 7-6 Terminology(基本概念) [24]

項目	定義・内容
Hybrid signature scheme	2 つ以上の署名アルゴリズムから構成されるマルチアルゴリズム署名方式
Hybrid signature / Dual signature	ハイブリッド署名方式により生成された署名
Component signature scheme	ハイブリッド署名を構成する個々の署名アルゴリズム
Artifact	ハイブリッド署名であることを示す痕跡(署名を分離しても残り、ハイブリッド利用の意図や証拠となる情報)
Stripping attack	ハイブリッド署名から一部署名を除去し、単独署名として悪用する攻撃
Component message forgery attacks	ハイブリッド署名の構成要素となる署名だけを単独で偽造する攻撃

表 7-7 Goals(設計目標) [24]

項目	定義・内容
Hybrid authentication	いずれか 1 つの署名方式が安全であれば認証が成立する性質
Hybrid unforgeability	EUF-CMA などの署名安全性が、構成要素の 1 つでも保持されていれば維持される性質
Proof composability	ハイブリッド署名の安全性が構成署名方式の安全性に基づいて証明できる性質
Weak non-separability (WNS)	署名を分離してもハイブリッドの痕跡 (artifact) は残るが、残った署名が検証に成功する場合がある性質
Strong non-separability (SNS)	署名を分離した場合、残った署名は必ず検証に失敗する性質
Simultaneous verification	全ての署名構成要素が同時に検証されなければ成功しない性質
Backwards compatibility	従来方式しか扱えない検証者でも、従来部分のみ検証して受理できる性質
Hybrid generality	複数カテゴリの署名構造に適用可能な汎用性を持つ性質

表 7-8 Non-Separability Spectrum(非分離性スペクトラム) [24]

項目	定義・内容
No non-separability	署名を分離しても痕跡が残らず、ハイブリッドであ

	ることを検知できない性質
Weak non-separability	痕跡は残るものの、残存署名が単独署名として検証成功してしまう場合がある性質
Strong non-separability	痕跡が署名内部に存在し、分離すると必ず検証が失敗する性質
SNS + Simultaneous verification	署名が完全不可分で、全構成要素を同時に検証しない限り成功しない最強の非分離性

表 7-9 Artifacts(痕跡の種別と配置) [24]

項目	定義・内容
Artifact location in message	メッセージ内にハイブリッド署名であることを示す情報（ラベル等）を配置する方式
Artifact location in certificate	証明書内のフィールドに、ハイブリッド署名利用を示すメタ情報を埋め込む方式
Artifact location in signature	複数の署名要素が結合され、単独署名として切り離せない構造を署名内部に持たせる方式
Protocol / policy artifacts	プロトコル仕様やポリシー上で「ハイブリッド署名を要求する」という設定・規定を痕跡として扱う方式

表 7-10 Need for Approval Spectrum(承認要件の分類) [24]

項目	定義・内容
New algorithm	新しい署名アルゴリズムとして扱われ、個別承認（例：FIPS）が必要となる
No approved module	既存承認済みモジュールに依拠するが、実装変更が必要で追加承認の要否が不明確な状態
1-out-of-n approved	構成要素のうち少なくとも 1 つを承認済みモジュールとしてブラックボックス利用できる状態
All approved	全ての構成署名方式が承認済みモジュールとしてブラックボックス利用可能で、内部動作を変更せずに組み合わせられる状態

表 7-11 EUF-CMA Challenges(偽造困難性に関する課題) [24]

項目	定義・内容
Component forgery risk	ハイブリッド署名の構成要素署名が単独署名として偽造されるリスク
Key reuse restriction	鍵を使い回すことにより生じる偽造リスクを防ぐための鍵利用制限
SNS-based mitigation	Strong Non-Separability（SNS）により分離攻撃を不可能にし、コンポーネント偽造を根本的に防止する対策

7.2.5 Crypto Forum Research Group (CFRG)

- RG 概要
  CFRG は、IRTF (Internet Research Task Force) 配下に設置された暗号技術分野の研究グループであり、IETF におけるインターネットプロトコル標準化を暗号技術の観点から技術的に支援する役割を担っている。CFRG は自ら標準仕様 (Standards Track RFC) を策定する主体ではなく、暗号アルゴリズム、鍵生成方式、電子署名方式等に関する研究成果や設計上の検討結果を、Informational または Experimental RFC として公開する点に特徴がある。これらの成果は、TLS、COSE、JOSE 等の IETF ワーキンググループにおける仕様検討や、NIST や ETSI による PQC 移行方針の技術的検討において、重要な参照情報として位置付けられている。

- PQC およびハイブリッド構成に関する標準化動向
  PQC への移行期において、既存の公開鍵暗号と新たな PQC アルゴリズムを併用するハイブリッド方式は、安全性と実運用性の両立を図るための重要なアプローチとして位置付けられている。CFRG では、量子コンピュータによる攻撃および量子コンピュータではない従来型のコンピュータによる攻撃の双方に対する耐性を同時に確保する、AND セキュリティモデルを前提としたハイブリッド鍵共有方式 (ハイブリッド KEM) について、設計原則や安全性要件の整理が行われており、その代表的な成果として draft-irtf-cfrg-hybrid-kems-07 (Hybrid Key Encapsulation Mechanisms (KEMs)) [10]が公開されている。これらの検討では、アルゴリズム単体の安全性のみならず、コンバイナ (combiner) の構成、ダウングレード攻撃への耐性、ならびに実装および相互運用性への影響といった実運用上の論点が重視されている。

7.3 International Telecommunications Union (ITU)

7.3.1 組織概要

国際電気通信連合 (International Telecommunication Union: ITU) は、電気通信および情報通信技術 (ICT) 分野に関する国連専門機関であり、標準化部門である ITU-T が電気通信の技術・運用・料金に関する勧告 (Recommendation) を策定している。ITU-T では、ディレクトリサービスや PKI の枠組み (X.500 系列) やサイバーセキュリティ、量子通信 (X.1700 系列) など広範な勧告群を所掌し、国際的な相互運用性の確保に資する技術的枠組みを提供してきた。とりわけ X.509 勧告は、公開鍵基盤 (PKI) および権限管理基盤 (PMI) の枠組みを定義し、証明書、失効リスト、拡張、検証手順、ディレクトリスキーマに至るまでを包括的に規定する、ITU-T と ISO/IEC による共同規格 (ISO/IEC 9594-8) として位置付けられている [19]。

7.3.2 PQC およびハイブリッド構成に関する標準化動向

ITU-T における量子安全 (Quantum-safe) 関連の標準化は、PKI／PMI を担う X.500 系列 (X.509) に加え、量子鍵配送ネットワーク (QKDN) や量子安全通信を対象とする X.1700 系列を中心に展開されている。PQC 移行期におけるハイブリッドの取り扱いについて、ITU-T は暗号プロトコルそのものを定義するのではなく、勧告における拡張や技術報告を通じて、複数暗号アルゴリズムの併用を前提とした運用上の考慮事項を整理している。例えば X.509 第 9.8 節では、代替暗号アルゴリズムおよび代替デジタル署名に関する拡張が規定されており、第 6.2.3 節では暗号アルゴリズム移行に伴う一般的な考え方が示されている。

一方、通信プロトコルレベルにおけるハイブリッド鍵共有や QKD 併用の論点については、ITU-T 技術報告「Overview of hybrid approaches for key exchange with quantum key distribution (XSTR-HYB-QKD, 2022-05)」 [40]において整理されている。同報告は、ETSI TS 103 744、NIST SP 800-56C Rev.2、IETF RFC 8784 など既存の仕様・ガイダンスを俯瞰し、QKD によって生成された鍵を既存プロトコルに統合する際の概念的整理や課題を示している。これらの検討は、ITU-T 自身が詳細仕様を定めるというよりも、関連標準間の整合的な理解を促す位置付けにある。

7.3.3 技術仕様におけるハイブリッド構成の詳細

ITU-T 勧告において、暗号プロトコルとしてのハイブリッド鍵共有を直接定義した仕様は存在しない。一方で、X.509 勧告は移行期における複数アルゴリズム併用を想定した拡張を備えており、PKI／PMI の運用面から複数アルゴリズム併存を可能にする拡張を提供している。以下では、X.509 (2019 版／ISO/IEC 9594-8:2020) [19]を中心に、その位置付けを整理する。

X.509 第 9.8 節では、一つのアルゴリズムの証明書や失効リストにおいて代替の公開鍵アルゴリズムや代替のデジタル署名を拡張として付与できる枠組みが定義されている。これにより、既存の暗号方式のみを理解する環境と新方式(PQC 署名等)を処理できる環境が併存する環境においても、同一オブジェクトに複数アルゴリズムに関する情報を保持する運用が可能となる。具体的な構造に関しては、本報告書の 4.2 節に示しているため、本節では記載を割愛する。

7.4 European Telecommunications Standards Institute (ETSI)

7.4.1 組織概要

European Telecommunications Standards Institute (ETSI) は、欧州を拠点とする国際標準化機関であり、情報通信技術 (ICT) 分野における国際的な技術仕様およびガイドラインの策定を担っている。通信事業者、装置ベンダ、研究機関、行政機関等から構成され、3GPP 等の標準化活動を通じて通信基盤のセキュリティ標準化に重要な役割を果たしてきた。

ETSI における PQC への取り組みは、暗号アルゴリズムの選定そのものよりも、既存プロトコルやシステムにおける移行設計・運用設計に焦点を当てている点に特徴がある。特に、Technical Committee CYBER (TC CYBER) において、Quantum-Safe Cryptography (QSC) を主題とした文書群が体系的に整備されている。

7.4.2 PQC およびハイブリッド構成に関する標準化動向

ETSI における PQC の標準化動向は、暗号アルゴリズム単体の規定ではなく、PQC を既存通信システム・暗号基盤へどのように段階的に導入するかという移行設計に主眼が置かれている。量子計算機の実用化時期や PQC アルゴリズムの成熟度に不確実性が残る中で、ETSI は移行期における安全性・相互運用性・運用継続性の確保を標準化の中心課題として位置付けている。

そして、PQC を単独で導入する「完全移行モデル」だけでなく、既存の暗号方式と PQC を併用するハイブリッド方式を重要な選択肢として明確に位置付けている。ETSI TR 103 966 V1.1.1 (2024-10) [41]は、PQC 移行におけるハイブリッド方式の役割を概念的に整理した技術報告書であり、PQC アルゴリズムの成熟度への備え、後方互換性の確保、既存プロトコル制約への対応といった観点から、ハイブリッド方式が検討される理由を体系的に示している。

同 TR では、PQC そのものに関しても、既存の暗号方式と比較した公開鍵や暗号文などの鍵材料のサイズや計算コストの増大、プロトコルメッセージ拡張、実装の複雑化といった技術的特性が整理

されており、これらが移行時の障壁となり得る点が明示されている。ETSI は、こうした PQC 特有の課題を踏まえた上で、移行初期段階においてはハイブリッド方式が現実的なリスク低減策として機能することを示唆している。

実際の技術仕様としては、ETSI TS 103 744 V1.2.1 (2025-03) [16]が、耐量子計算機性を備えたハイブリッド鍵共有方式を規定している。本仕様では、従来型の ECDH による鍵共有と、FIPS 203 で標準化された ML-KEM による鍵共有を独立に実行し、それぞれから得られる複数の共有秘密を KDF により安全に結合するハイブリッド構成が定義されている。これは、PQC 単独方式へ完全移行する前段階として、既存の PKI との互換性を維持しながら耐量子計算機性を付加する設計方針を反映したものである。

さらに、ETSI TS 104 015 V1.1.1 (2025-02) [42]は、耐量子計算機性を備えたハイブリッド KEM およびアクセス制御を組み合わせた応用的仕様である。本仕様では、Computational Diffie-Hellman (CDH) に基づく従来型 KEM と Learning With Errors(LWE) に基づく PQ KEM(FIPS 203 で標準化された ML-KEM を含む)を組み合わせることで、少なくとも一方の暗号方式が安全であれば秘匿性が維持されるハイブリッド構造を前提としつつ、PQC への移行期における実運用要件（匿名性、属性ベース制御、トレーサビリティ）を暗号仕様レベルで実現している。

以上より ETSI の PQC 標準化動向は、PQC アルゴリズム単体の安全性評価にとどまらず、ハイブリッド方式を含む複数の移行シナリオを想定した実用指向の技術体系として整理されている点に特徴がある。これは、NIST や IETF で策定されるアルゴリズム・プロトコル標準を補完し、実システムへの PQC 導入を段階的に進めるための指針を提供する役割を ETSI が担っていることを示している。

7.4.3 技術仕様におけるハイブリッド構成の詳細

ETSI TS 103 744 V1.2.1 [16]は、耐量子計算機性ハイブリッド鍵共有に関する代表的な技術仕様であり、複数の鍵共有方式から得られる共有秘密を安全に合成するための構造を体系的に定義している。本仕様では、現在の暗号方式として ECDH を、PQC 方式として ML-KEM を用いる構成を想定し、両者を並列に実行することで複数の共有秘密を生成する点が特徴である。なお、図 7-2 から図 7-6 は、これらのハイブリッド鍵共有方式（連結／カスケード、および ephemeral/static keying variant）の構造を補足的に示す概念図であり、構造を視覚的に補足するために掲載している。

鍵共有メカニズムは 3 つの機能で構成される：

- KeyGen( )：秘密鍵 sk と公開鍵 P を生成する鍵生成関数。
- ResponseFunc(P)：共有秘密 k と応答値 R を生成する応答関数。ただし、処理に失敗した場合にはエラー指標⊥を返す。
- ReceiveFunc(sk, R)：秘密鍵 sk と応答値 R を受け取り、共有秘密 k を計算する関数。ただし、処理に失敗した場合にはエラー指標⊥を返す。

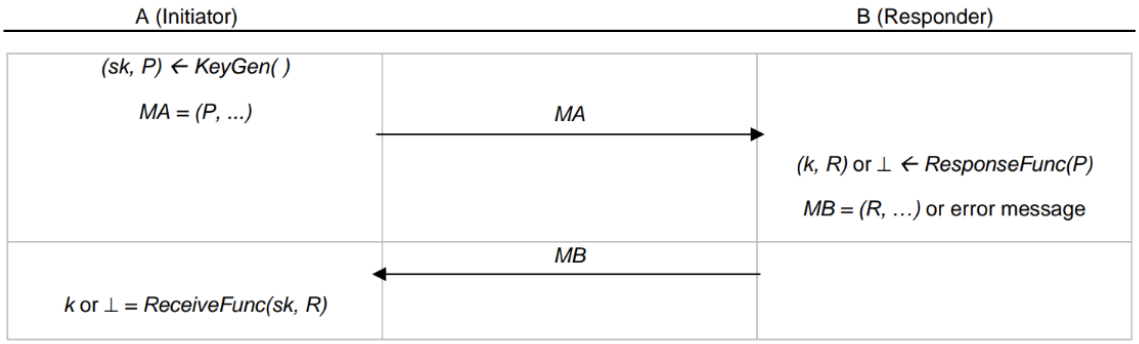


Figure 3: Key establishment abstraction

ResponseFunc がエラー指標を返した場合、レスポンダー(B)はエラーメッセージを応答し、プロセスを終了しなければならない。

イニシエータ(A)が B からエラーメッセージを受信した場合、または ReceiveFunc がエラー指標を返した場合、A はプロセスを終了しなければならない。

MA は、A から B へ送信されるオクテット列であり、1 つ以上の公開鍵の符号化を含む。必要に応じて、セッションネゴシエーション情報を含めることができる。

MB は、1 つ以上の応答値の符号化を含むオクテット文字列であり、同時にセッションネゴシエーション情報を含めることができる。

メッセージは不正な改変から保護されなければならない。メッセージは、送信者の身元に関連付けられた署名鍵によるデジタル署名を用いて保護され得る。この署名鍵は、信頼された第三者認証機関によって署名されたものである。

図 7-2 鍵共有方式の概要［16］

これらの共有秘密は単純に連結されるのではなく、CatKDF（Concatenate-based Key Derivation Function）および CasKDF（Cascade-based Key Derivation Function）と呼ばれる二種類の鍵導出関数を用いて統合される。CatKDF は複数の共有秘密を入力として KDF に与える方式であり、比較的実装が容易である一方、CasKDF は段階的に鍵導出を行うことで、より厳密なセキュリティ性質の保持を意図した方式である。本仕様では、これら二つの鍵導出方式について、ephemeral keying variant（セッション毎に新規生成する鍵を前提とする構成）と static keying variant（長期間保持される鍵を前提とする構成）の双方に対応するよう仕様化されており、利用環境やプロトコル要件に応じて適切な組み合わせを選択できるよう設計されている。

本条項は、ephemeral keying variant を用いた連結ハイブリッド鍵共有方式を規定する。Figure 3 の鍵共有方式の記述を拡張し、単一メッセージ内で公開鍵ペアと複数の応答値を交換する。ephemeral keying variant を用いた連結ハイブリッド鍵共有方式は Figure 4 に示す通り構築される。

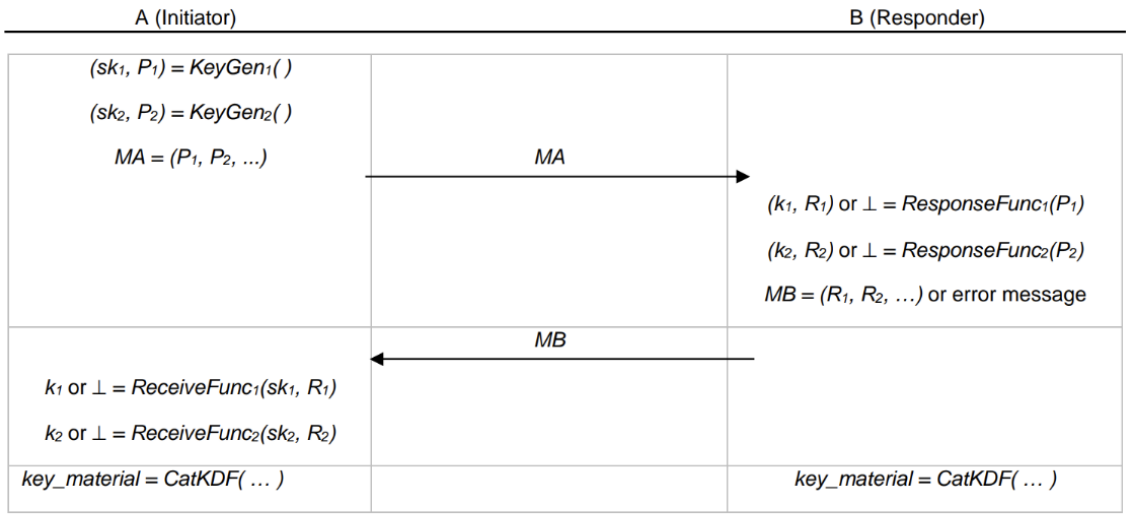


Figure 4: Concatenate hybrid key establishment - ephemeral

いずれかの ResponseFunc$_i$(i={1,2})がエラー指標を返した場合、B はエラーメッセージで応答し、プロセスを終了する。

A がエラーメッセージを受信した場合、A はプロセスを終了しなければならない。いずれかの ReceiveFunc$_i$(i={1,2})がエラー指標を返した場合、A はプロセスを終了しなければならない。

MA は、A から B へ送付された公開鍵 Pi の符号化を含むオクテット文字列とする。MA にはラベル用付加データなどのセッションネゴシエーション情報を含めることができる。

MB は、MB がエラーメッセージでない場合、応答値 Ri の符号化を含むオクテット文字列でなければならない。MB にはラベル用付加データなどのセッションネゴシエーション情報を含めることができる。

メッセージは不正な改変から保護されなければならない。メッセージは、送信者の身元に関連付けられた署名鍵を用いて、信頼できる第三者認証機関によって署名されたデジタル署名により保護することができる。

図 7-3 連結ハイブリッド鍵共有方式 - ephemeral keying variant [16]

本条項は、static keying variant を用いた連結ハイブリッド鍵共有方式を規定する。Figure 3 の鍵共有方式の記述を拡張し、単一メッセージにおいて、送信者(B)が受信者(A)が保持する静的な公開鍵(P_1, P_2)を信頼できる方法で取得するとともに、単一メッセージにおいて、複数の応答値 (R_1, R_2) を取得する。static keying variant を用いた連結ハイブリッド鍵共有方式は Figure 5 に示すように構築される。

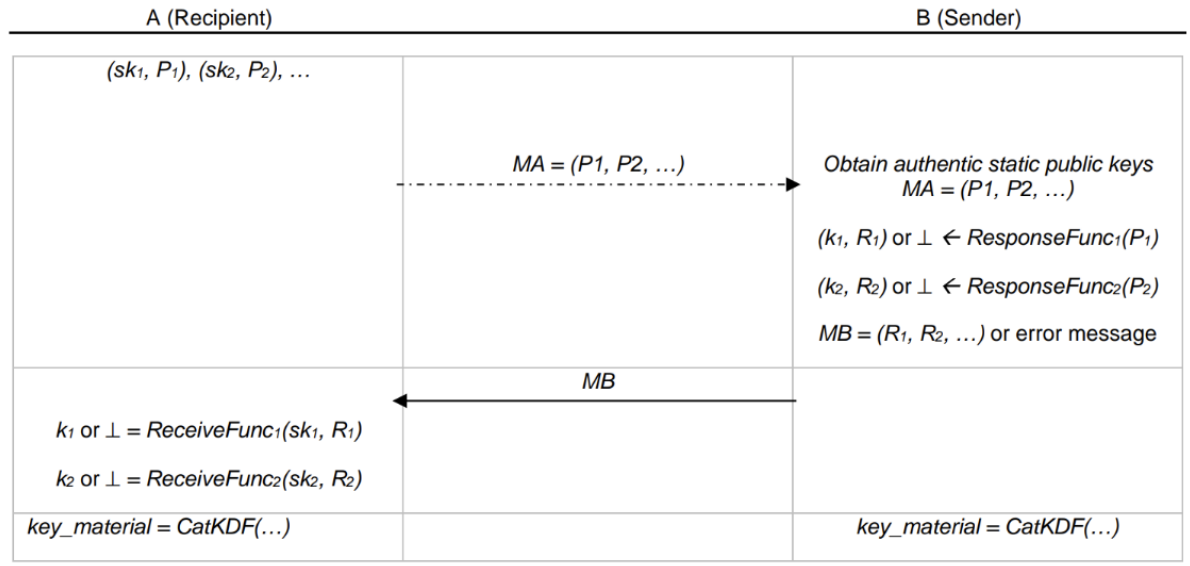


Figure 5: Concatenate hybrid key establishment - static

いずれかの $\mathrm{ResponseFunc}_i$(i={1,2})がエラー指標を返した場合、B はプロセスを終了する。いずれかの $\mathrm{ReceiveFunc}_i$(i={1,2})がエラー指標を返した場合、A はプロセスを終了する。

MA は、鍵共有の前または最中で、B が A の静的な公開鍵およびラベル用付加データ(label contribution values) などの追加値を信頼できる方法で取得していることを前提とする。

MB は、MB がエラーメッセージでない場合、応答値 R_i の符号化を含むオクテット文字列でなければならない。MB にはセッションネゴシエーション情報を含めることができる。2 つ以上の鍵共有方式が使用されている場合、MB には対応するすべての公開鍵と暗号文を含めなければならない。

メッセージは不正な改変から保護されなければならない。メッセージは、送信者の身元に関連付けられた署名鍵によるデジタル署名を用いて保護され得る。この署名鍵は信頼できる第三者認証機関によって署名される。

図 7-4 連結ハイブリッド鍵共有方式 - static keying variant [16]

本条項では、ephemeral keying variant を用いたカスケードハイブリッド鍵共有方式を規定する。Figure 3 の鍵共有方式の記述を拡張し、異なるメッセージ間で複数の公開鍵(MA_1, MA_2)を交換し、異なるメッセージ間で複数の応答値(MB_1, MB_2)を交換する。カスケードハイブリッド鍵共有方式は Figure 6 に示すように構築される。

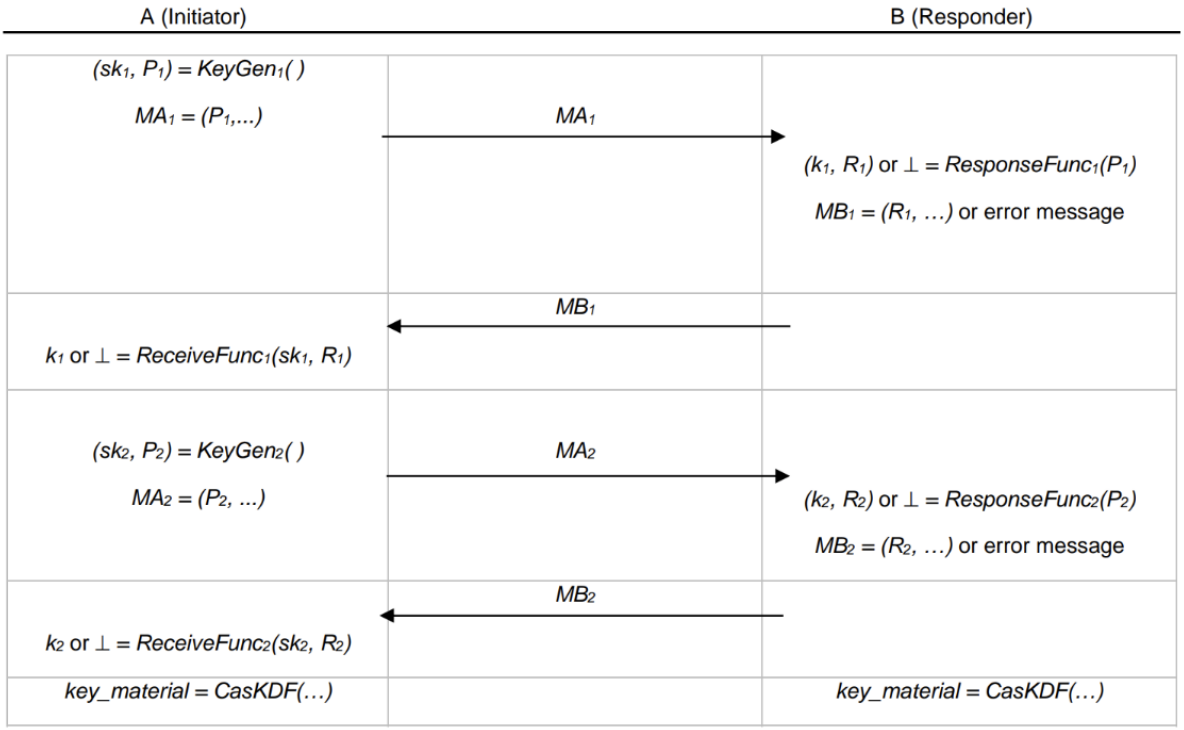


Figure 6: Cascade hybrid key establishment - ephemeral

いずれかの $ResponseFunc_i$(i={1,2})がエラーインジケータを返した場合、B はエラーメッセージを返し、プロセスを終了する。

A が B からエラーメッセージを受信した場合、A はプロセスを終了させるものとする。いずれかの $ReceiveFunc_i$(i={1,2})がエラーインジケータを返した場合、A はプロセスを終了する。

MA_i (i={1,2})は、A から B へ送付された公開鍵 P_i の符号化を含むオクテット文字列とする。MA_i (i={1,2})にはラベル用付加データなどのセッションネゴシエーション情報を含めることができる。

MB_i(i={1,2})は、応答値 R_i(i={1,2})の符号化を含むオクテット文字列とする。MB_i(i={1,2})にはラベル用付加データなどのセッションネゴシエーション情報を含めることができる。

メッセージは不正な改変から保護されなければならない。メッセージは、送信者の身元に関連付けられた署名鍵によるデジタル署名を用いて保護することができ、この署名鍵は信頼できる第三者認証機関によって署名される。

図 7-5 カスケードハイブリッド鍵共有方式- ephemeral keying variant [16]

本条項は、static keying variant を用いたカスケードハイブリッド鍵共有方式を規定する。Figure 7 に示すように構築される。

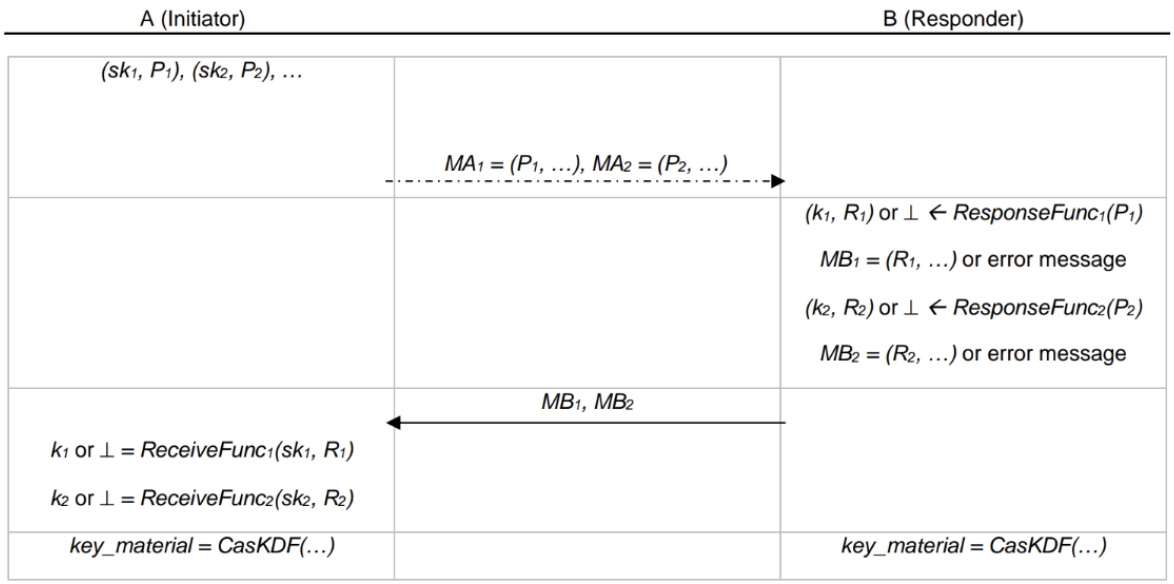


Figure 7: Cascade hybrid key establishment - static

いずれかの $ResponseFunc_i$ がエラー指標を返した場合、B はプロセスを終了する。いずれかの $ReceiveFunc_i$ がエラー指標を返した場合、A はプロセスを終了する。

MA_i(i={1,2})は、鍵共有前または鍵共有中で、B が A の静的な公開鍵およびラベル用付加データ(label contribution values) などの追加値を信頼できる方法で取得していることを前提とする。

MB_i(i={1,2})は、MB_i がエラーメッセージでない場合、応答値 Ri の符号化を含むオクテット文字列でなければならない。MB_i にはセッションネゴシエーション情報が含まれる場合がある。

メッセージは不正な改変から保護されなければならない。メッセージは、送信者の身元に関連付けられた署名鍵によるデジタル署名を用いて保護することができ、この署名鍵は信頼できる第三者認証機関によって署名される。

図 7-6 カスケードハイブリッド鍵共有方式- static keying variant [16]

重要な点として、ETSI TS 103 744 [16]は、ハイブリッド鍵共有方式の安全性が自動的に保証されるわけではないことを明示している。特定の構成では能動的攻撃に対して脆弱性が生じ得るため、鍵導出関数の選定、入力パラメータの整合性、プロトコルメッセージの完全性保護が不可欠であることが、セキュリティ考察として整理されている。これらは、PQC 単独方式に移行するまでの暫定的手法であるという位置付けとも整合している。

一方、ETSI TS 104 015 V1.1.1 [42]は、ハイブリッド方式を単なる通信路の鍵共有方式に留めず、より高度なデータ保護モデルへ拡張した技術仕様である。本仕様で定義される Hybrid Traceable KEM with Access Control (HTKEMAC) は、従来型 Non-Interactive Key Exchange(NIKE) と PQC KEM を組み合わせ、属性ベースのアクセス制御とトレーサビリティを同時に実現する構造を持つ。これにより、「誰が復号可能か」を暗号レベルで制御すると同時に、不正利用時には利用者を追跡可能とする設計が可能となる。

HTKEMAC では、暗号方式の選択をブラックボックス的に扱う構造が採用されており、将来的に PQC アルゴリズムが更新された場合でも、全体構造を維持したまま差し替え可能である点が意図されている。この点は、ETSI が PQC およびハイブリッド方式を恒久的解としてではなく、技術進展に応じて更新される移行期技術として捉えていることを反映している。

以上のように、ETSI の技術仕様におけるハイブリッド方式は、単なる防御的多重化ではなく、PQC

移行期における安全性・運用性・将来拡張性を同時に満たす設計指針として体系化されている。この点が、アルゴリズム中心の PQC 標準とは異なる ETSI 仕様の特徴である。

7.5 Institute of Electrical and Electronics Engineers (IEEE)

7.5.1 組織概要

Institute of Electrical and Electronics Engineers (IEEE) は、電気・電子・情報通信分野を中心とする国際的な専門家組織であり、標準化組織である IEEE Standards Association (IEEE SA) を通じて多数の技術標準を策定している。通信ネットワーク、無線通信、ネットワークセキュリティ分野においては、IEEE 802 シリーズをはじめとする規格群が広く利用されている。PQC への移行については、通信プロトコルおよびネットワーク基盤への適用を主な対象として検討が進められており、既存の暗号方式との相互運用性を維持しながら段階的に PQC を導入する観点から、ハイブリッド方式を含めた検討が行われている。

7.5.2 PQC およびハイブリッド構成に関する標準化動向

IEEE における PQC およびハイブリッド方式に関する標準化の検討は、主として通信プロトコルおよびネットワークセキュリティ分野を中心に進められている。無線 LAN 技術を対象とする IEEE 802.11 では、将来の量子計算機による暗号解読リスクを踏まえ、既存の公開鍵暗号方式と PQC 方式を併用する移行の中間時期の形態が検討対象となっている。IEEE 802.11 TGbt に提出された文書「Proposed Texts for Hybrid PQC」[17]では、認証フェーズで交換される管理フレームにおいて、従来の DH パラメータに加えて、ML-KEM のパラメータを格納可能とする拡張が提案されている。これは認証フレームというフレーム種別を変更するものではなく、同フレーム内に含めるパラメータ要素 (elements) を拡張する形でハイブリッド鍵共有を実現するものである。本提案では、既存の RSN (Robust Security Network) および AKM (Authentication and Key Management) の枠組みを保持しつつ、その拡張としてハイブリッド方式を導入する設計が示されている。これにより、PQC を利用しない既存端末との相互運用性を保ちながら、DH と ML-KEM の双方から得られる複数の鍵素材を KDF に投入してセッション鍵を生成する構成が整理されている。このような設計は、移行期において耐量子計算機性を確保しつつ、既存実装の構造や端末との実装互換性を維持することを目的としている。

一方、IEEE Standards Association において検討が進められている IEEE SA P1943 (Standard for Post-Quantum Network Security) [43]は、特定の通信プロトコルに限定せず、ネットワークセキュリティ全般を対象とした耐量子計算機化の枠組みを整理する標準である。P1943 では、鍵共有および認証における PQC の適用や、完全な PQC 移行に至るまでの過渡期におけるハイブリッド方式の位置付けが整理されている。これらの検討は、IEEE 802 系列規格における個別のプロトコル仕様検討を補完する位置付けとして整理されている。

7.5.3 技術仕様におけるハイブリッド構成の詳細

IEEE 802.11 Submission: Proposed Texts for Hybrid PQC [17]では、IEEE 802.11 における耐量子計算機化対応として、既存の鍵共有方式と PQC 方式を併用するハイブリッド構成が具体的な仕様変更案として示されている。本提案では、認証フェーズにおいて DH による共有秘密 DH_ss と ML-KEM による共有秘密 SS_pq を双方生成し、最終的にセッション鍵を導出する Hybrid Key Derivation が定義されている

この構成を無線 LAN のフレーム交換に統合するため、以下の 2 つの仕様拡張が提案されている。

(1) AKM Suite Selector の拡張：ハイブリッド構成を明示的に示す新しい AKM Suite を追加し、RSNE／RSNXE 内で交渉可能とする。

(2) RSN Extension (RSNXE) の拡張：ML-KEM のパラメータセット (ML-KEM-768/1024) および DH Group Identifier を広告するための新規フィールドが追加される。

さらに、従来の Diffie-Hellman Parameter element を拡張し、Diffie-Hellman and ML-KEM Parameter element として再定義することで、

- DH の有限体群識別子 (Finite Cyclic Group field)
- ML-KEM パラメータセット

の双方を格納し、両パラメータの組み合わせに対して Hybrid Parameter Identifier を割り当てる構造が示されている。これにより CNSA 2.0 で要請される ML-KEM-1024 や、IoT 端末向けの ML-KEM-768 を、DH と組み合わせて選択可能となる

また、認証および鍵導出処理の全体フローは 802.1X 認証および Fast Transition (FT) に対応する形で体系化されており、Hybrid PQC に対応した以下の手順が規定されている：

- DH 公開鍵の妥当性検証 (Finite Cyclic Group の整合性検証を含む)
- ML-KEM パラメータ検証 (RSNXE／Parameter element に基づく整合性確認)
- Hybrid Key Material の整合性確認 (DH_ss と SS_pq の生成可否チェック)

図 7-7 では、Authentication frame#1/#2 における DH_s_pub、MLKEM_s_pub の送信、AP による公開鍵検証、ML-KEM を用いたカプセル化の実行、STA による ML-KEM を用いたデカプセル化を例示する。

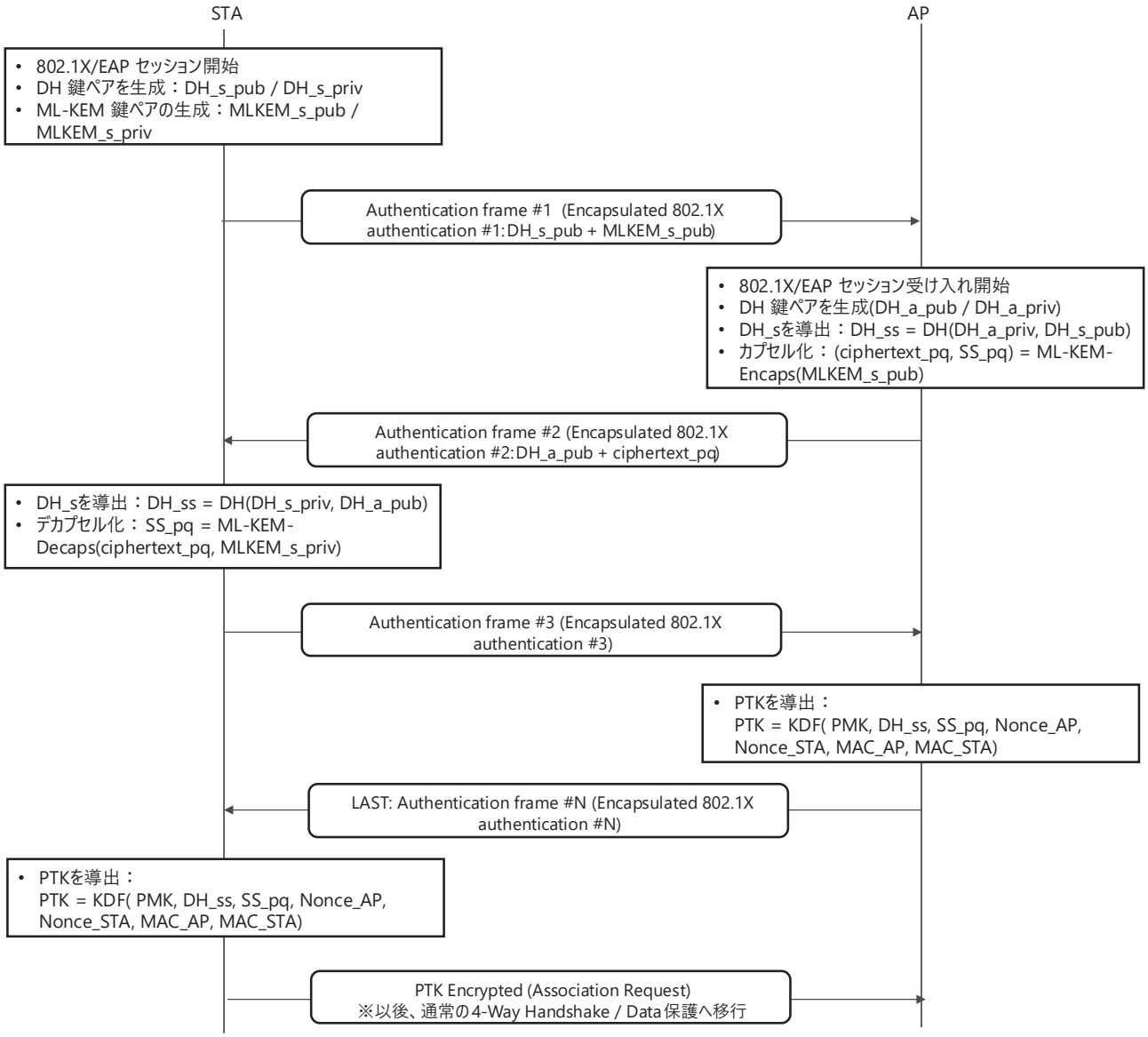


図 7-7 Hybrid PQC を適用した認証フレーム交換例。IEEE 802.11 Submission [17]の図を基にしつつ、原図では省略されている処理（EAP セットアップ、DH_ss／SS_pq の具体的導出、PTK 導出式など）を日本語で補足した再構成図である。

7.6 International Organization for Standardization (ISO)

7.6.1 組織概要

国際標準化機構（ISO）は、国際的な標準の策定を通じて、製品およびサービスの相互運用性や品質確保を目的とする国際標準化団体である。情報技術分野については、国際電気標準会議（IEC）との合同技術委員会である ISO/IEC JTC 1 が所管しており、暗号およびセキュリティ、プライバシ保護に関する標準化は、その下位分科会である SC 27（Information security, cybersecurity and privacy protection）が担当している。SC 27 の中でも、暗号アルゴリズム、鍵管理、デジタル署名などの暗号技術を扱うのが WG 2（Cryptography and Security Mechanisms）であり、ISO/IEC 18033（暗号アルゴリズム）、ISO/IEC 14888（デジタル署名）、ISO/IEC 11770（鍵管理）などの国際規格シリーズの策定および維持を行ってきた。PQC については、量子計算機の将来的な実用化を見据え、2015 年頃から検討が進められており、SC 27 Journal 等を通じて、標準化に向けた準備状況や基本的な考え方が共有されている。

7.6.2 PQC およびハイブリッド構成に関する標準化動向

ISO/IEC JTC 1/SC 27 における PQC の標準化は、新たな暗号方式を単独で規定するというよりも、既存の暗号標準体系の中に耐量子計算機性のある暗号方式を段階的に取り込む形で進められている。この取り組みの基盤整備として、SC 27/WG 2 により策定された Standing Document (SD8) がある。SD8 では、ハッシュベース署名、格子ベース暗号、符号ベース暗号、多変数暗号、イソジェニー暗号といった PQC メカニズムの主要な５つのカテゴリについて、基本概念、安全仮定、代表的方式例が整理されている。

SC 27 Journal (Vol.1, Issue 3, 2022) [44]に掲載された「Paving the Runway for Standardization of Post-Quantum Cryptography」では、量子計算機の進展が既存の公開鍵暗号方式に与える影響を整理するとともに、PQC 移行に向けた取り組みの方向性が示されている。本記事では、PQC メカニズムの主要なカテゴリや、それらに関連する安全性の前提、実装上の特性などを整理することが、今後の標準化活動に向けた基盤的なステップとして紹介されている。一方、TLS や X.509 証明書のような具体的なプロトコル仕様については、本稿では取り扱われておらず、SC 27 では暗号プリミティブの枠組み整理や基礎的事項の把握が中心的な役割として位置付けられている。

この方針に沿い、ISO においては、PQC と既存の暗号方式を併用するハイブリッド方式についても、具体的な構成や鍵・署名の組み合わせ方法を技術仕様として規定していない。これらは主として IETF や ETSI などの標準化機関において議論・仕様化が進められており、ISO/IEC SC 27 はリエゾンを通じてそれらの動向と整合を図りつつ、暗号プリミティブの枠組み整理や概念レベルでの整理を担う位置付けとなっている。

一方で、PQC メカニズムの一部については、既存規格の分冊として規格化が進められている。具体例として、ISO/IEC 14888-4 (Stateful hash-based mechanisms) があり、ハッシュベース署名を既存のデジタル署名の規格体系に取り込む取り組みが行われている。しかし、複数の暗号方式を同時に利用するハイブリッド構成そのものについては、ISO 規格として規範的な定義は与えられていない。

以上より、ISO における PQC およびハイブリッド方式への取り組みは、NIST、IETF、ETSI 等が策定する具体的な技術仕様や移行ガイダンスを補完する形で、国際標準としての暗号技術体系全体の整合性を確保する役割を担っていると整理できる。

7.7 ANSI Accredited Standards Committee X9 (ASC X9)

7.7.1 組織概要

ANSI Accredited Standards Committee X9 (ASC X9) は、米国金融サービス業界向けの標準を策定する ANSI 認定標準化団体であり、1974 年に設立された。銀行・証券・保険・決済事業者などの金融業界を対象に、決済処理、資金移動、証券決済、カード取引、クリアリングなどの金融業務に関わる、暗号技術、公開鍵基盤 (PKI)、データ保護、認証および情報セキュリティ管理に関する標準や指針を策定してきた。

ASC X9 は ISO/TC 68 (金融サービス) における米国の国内審議団体として国際標準化活動にも関与しており、国内標準と国際標準との整合性を考慮した活動を行っている点に特徴がある。中でも X9F 委員会は暗号および情報セキュリティ分野を担当し、金融業界が直面する実務的なセキュリティ課題に対応した文書を多数公表してきた。

近年は量子計算機の進展を受け、既存の暗号方式の長期的安全性に対するリスクへの対応を重要

な検討課題として位置付けている。特に金融分野では、長期的なデータ保護や業界横断的な相互運用性確保が不可欠であることから、PQC への移行に関する調査・検討を段階的に進めている。

7.7.2 PQC およびハイブリッド構成に関する標準化動向

ASC X9 における PQC への対応は、NIST が主導する PQC アルゴリズム標準化を技術的前提としつつ、金融業界における移行準備とリスク管理の観点から整理されている点に特徴がある。2025 年に公開された「Post-Quantum Cryptography Financial Readiness Needs Assessment」 [45]は、ASC X9F による Informative Report として、金融機関が PQC 移行に向けて検討すべき事項を体系的に整理した文書である。

同レポートでは、量子計算機の実用化時期に不確実性が残る一方で、公開鍵暗号の長期的安全性が将来的に損なわれる可能性を前提に、移行準備を早期に開始する必要性が指摘されている。特に金融分野では、取引データや顧客情報など長期にわたり保護すべき情報が多く、Harvest Now, Decrypt Later（HNDL）攻撃への対応が重要な検討課題として位置付けられている。

このような前提の下、ASC X9 は PQC 移行を単純なアルゴリズム置換としてではなく、組織全体の暗号使用状況を把握した上で段階的に進めるべき長期的プロセスとして整理している。具体的には、PKI、TLS、決済ネットワーク、外部委託先を含む暗号利用環境について、暗号資産の棚卸しおよびリスク評価を実施し、影響範囲や優先順位を明確にすることが出発点として示されている。

また、移行期間が長期化することを前提に、将来的な標準やアルゴリズムの変更に柔軟に対応可能なクリプトグラフィック・アジリティの確保が重要な要素として言及されている。特定の暗号方式や実装に強く依存した構成は、PQC 移行やその後の標準更新において運用上の制約となる可能性があるため、暗号ライフサイクル管理やアーキテクチャ設計の観点からの見直しが必要とされている。

さらに、PQC およびハイブリッド方式の導入に伴う実務的影響として、相互運用性、性能、証明書サイズの増大といった課題が整理されている。金融インフラでは、単一組織内にとどまらず業界全体での移行方針や実装方針の整合性を確保しつつ、他機関やベンダとの相互運用性を維持しながら移行を進める必要があるとされている。ASC X9 は、ハイブリッド方式を最終形として固定化するのではなく、PQC への完全移行までの移行期における現実的なリスク低減手段として位置付けている点に特徴がある。

7.8 National Security Agency (NSA)

7.8.1 組織概要

米国国家安全保障局（National Security Agency: NSA）は、米国政府における国家安全保障分野の通信・情報システムを担当する機関であり、暗号技術に関しては国家安全保障システム（National Security Systems: NSS）を対象とした標準化方針および運用ガイダンスを策定・提示する役割を担っている。NSA は、暗号アルゴリズムそのものを国際標準として策定する立場にはないものの、NIST が標準化する公開鍵暗号技術を前提として、NSS における利用要件、移行期限、運用上の制約条件を明確化する政策的・技術的指針を提示してきた点に特徴がある。従来は CNSA Suite 1.0 を通じて RSA や楕円曲線暗号を中心とした暗号スイートを規定してきたが、量子計算機の進展を背景として、PQC への移行を国家レベルで推進する方針を明確化している。

7.8.2 PQC およびハイブリッド構成に関する標準化動向

NSA における PQC 移行方針は、2022 年に公表された Commercial National Security Algorithm Suite 2.0（CNSA Suite 2.0） [46]により明確化された。同文書では、将来的に既存の暗号方式に対する解析能力を有する量子計算機（Cryptographically Relevant Quantum Computer: CRQC）が実用化されることを前提として、NSS において使用される公開鍵暗号を既存の RSA や ECDH／ECDSA から耐量子計算機性を有する方式へ移行する必要性が示されている。CNSA Suite 2.0 では、一般用途の公開鍵暗号として NIST が標準化を進める CRYSTALS-Kyber（鍵カプセル化方式）および CRYSTALS-Dilithium（電子署名方式）を将来の必須アルゴリズムとして位置付けている。

注目すべき点として、NSA は PQC への移行を単純な一括置換ではなく、既存の暗号方式と PQC を併用するハイブリッド構成を前提とした段階的移行として整理している。プロトコル標準や製品成熟度、相互運用性の制約によっては、一定期間ハイブリッド方式の利用が許容、あるいは必要となることを明示しており、ハイブリッド方式を恒久的解決策ではなく移行期の現実的対処として位置付けている点が特徴である。

さらに、CSfC（Commercial Solutions for Classified）プログラムにおいては、2025 年に公表された CSfC Post Quantum Cryptography Guidance Addendum [47]により、TLS、IPsec、EAP-TLS など具体的なプロトコル単位での PQC およびハイブリッド方式の適用方針が整理されている。同ガイダンスでは、既存の鍵共有方式と ML-KEM を組み合わせた構成や、Pre-Shared Key を併用した耐量子計算機性確保の考え方が示され、運用面の現実性を重視した段階的な移行方針が示されている。

7.9 Cloud Security Alliance (CSA)

7.9.1 組織概要

Cloud Security Alliance（CSA）は、クラウドコンピューティング環境におけるセキュリティの向上を目的として 2009 年に設立された国際的な非営利団体である。クラウドサービス利用者、クラウドプロバイダ、セキュリティベンダ、研究機関など幅広いステークホルダーが参加しており、クラウド特有のリスクや運用課題に対するベストプラクティスの整理と普及を主な活動目的としている。CSA はアルゴリズムやプロトコルの標準仕様を策定する標準化機関ではなく、クラウド利用の実務者を主対象としたガイドライン、リスク評価手法、統制フレームワークを提供する立場にある点が特徴である。代表的な成果物として、Cloud Controls Matrix（CCM）や各種セキュリティホワイトペーパーが挙げられる。近年は量子計算機の実用化を見据え、PQC に関する実務的ガイダンスの提供にも注力している。

7.9.2 PQC およびハイブリッド構成に関する標準化動向

CSA における PQC への取り組みは、アルゴリズムやプロトコルの仕様策定ではなく、クラウド利用者が直面するリスク評価および段階的移行判断を支援する実務ガイダンスの提示に主眼が置かれている。代表的な文書である「A Practitioner's Guide to Post-Quantum Cryptography (2025)」[48]では、量子計算機による将来的な既存の公開鍵暗号方式の解読リスク、とりわけ Harvest Now, Decrypt Later（HNDL）攻撃を背景として、クラウド環境における現実的な移行ステップが整理されている。CSA は、全面的な PQC 移行が短期間では困難である点を踏まえ、移行初期段階における有効なリスク低減策としてハイブリッド方式の活用を明確に位置付けている。具体的には、TLS 1.3、SSH、IPsec／VPN などの通信プロトコルを対象とし、既存の暗号方式と PQC アルゴリズムを組み合わせたハイブリッド鍵共有を優先的に導入すべき対象として挙げている。特に、TLS 1.3 における X25519 と ML-KEM（Kyber）を組み合わせたハイブリッド鍵共有は、移行期間中の代表的構成例として紹介されている。この方式では、複数の鍵素材を Combiner により結合し、いずれか一方の方式

が安全であればセッション鍵全体の機密性を維持できる設計思想が採用されている。また CSA は、証明書およびデジタル署名に関しても、Composite 証明書や Dual 署名といったハイブリッド署名モデルを検討することを推奨している。これらは既存の検証基盤との互換性を維持しつつ耐量子計算機性を段階的に導入するための現実的手法と位置付けられている一方、運用ポリシー不整合やダウングレード攻撃といった新たなリスクについても注意が必要であるとされている。総じて CSA は、NIST や IETF が策定する技術標準を前提としつつ、クラウド実運用の観点から PQC およびハイブリッド方式導入時の判断指針を補完する役割を果たしている。

7.10 PQCRYPTO

7.10.1 組織概要

PQCRYPTO は、欧州委員会 Horizon 2020（プロジェクト番号 ICT-645622）の支援を受け、2015 年 3 月から 2018 年にかけて実施された欧州主導の研究プロジェクトである。量子計算機の実用化によって既存の公開鍵暗号方式が破綻するリスクを背景に、長期的に安全な PQC の研究推進と国際標準化への橋渡しを主要目的とした。協調機関はアイントホーフェン工科大学（TU Eindhoven）であり、複数の欧州大学・研究機関が参画した。プロジェクトでは、候補暗号技術の整理・評価に加え、標準化団体との連携を担うワークパッケージ（WP5）が設けられ、ISO/IEC、ETSI、IEEE、IETF/IRTF 等の標準化活動への貢献と情報発信が体系的に進められた。プロジェクト自体は 2018 年に終了しているが、その知見と人的ネットワークは現在の PQC 標準化に継続的な影響を与えている。

7.10.2 PQC およびハイブリッド構成に関する標準化動向

PQCRYPTO は、個別技術仕様を策定する立場ではなく、PQC の標準化初期段階において、各標準化団体の活動を横断的に整理し、研究成果を標準化議論へ投入する役割を果たした。最終報告書（Deliverable D5.2）[49]では、ETSI、NIST、ANSI X9、IEEE、IETF/IRTF、ISO/IEC JTC 1/SC 27、ドイツ連邦情報セキュリティ庁（BSI）などにおける PQC 関連動向が体系的に整理されている。特に、ハッシュベース署名（XMSS、LMS）や格子暗号を中心とする PQC 候補技術の成熟状況、ならびに既存セキュリティ基盤との統合可能性が主要論点として扱われた。

ハイブリッド方式に関しては、量子計算機が直ちに実用化されない一方で「保存して後に解読（Harvest-then-Decrypt）」攻撃のリスクが顕在化しつつあるという問題意識の下、移行期における現実的な安全確保手段として位置付けられている。D5.2 では、IETF における TLS 1.3 向け耐量子計算機性を有する安全なハイブリッド鍵共有案や、ハイブリッド暗号方式におけるアルゴリズム選定指針などの検討状況が紹介されている。これらは、既存の暗号方式と PQC を併用し、複数の鍵素材や署名を構成する複数の要素(署名値・認証パス・付随パラメータなど)を組み合わせることで、少なくとも一方が安全であれば全体の安全性を維持する設計思想に基づくものであり、段階的移行と後方互換性の確保を両立する点に特徴がある。

また PQCRYPTO は、ETSI の Quantum-Safe Cryptography (QSC) ワークショップへの継続的参加や、ISO/IEC JTC 1/SC 27 (WG2) とのリエゾン確立を通じて、欧州を中心とした標準化議論に直接関与した。ISO/IEC では、WG2 における PQC の検討に対し「Initial recommendations of long-term secure post-quantum systems」を提供し、後続のスタンディングドキュメント (WG2/SD) 策定に寄与している。さらに、NIST の PQC 標準化プロセスに対しても、プロジェクト参加者が提案アルゴリズムの開発・評価・攻撃解析のいずれの側面でも関与し、グローバルな合意形成に影響を与えた。

以上のように PQCRYPTO は、PQC およびハイブリッド方式を「標準として定義する主体」ではなく、「研究成果を国際標準化活動へ橋渡しする触媒」として機能した点に特徴がある。2018 年のプ

ロジェクト終了後も、D5.2 で整理された標準化課題や設計観点は、ETSI 技術仕様、IETF RFC／インターネットドラフト、NIST SP／IR 等に引き継がれており、現在の PQC 移行戦略を理解する上で重要な歴史的参照点となっている。

7.11 Post-Quantum Cryptography Coalition (PQCC)

7.11.1 組織概要

Post-Quantum Cryptography Coalition (PQCC) は、量子計算機の実用化に伴う暗号リスクに対応することを目的として設立された、産学官横断の国際的アライアンスである。PQCC は特定の標準化機関とは異なり、アルゴリズムやプロトコルの規格制定を直接行う立場ではない。一方で、ソフトウェアベンダ、クラウド事業者、暗号ライブラリ開発者、研究者などが参加し、PQC 移行に関する実践的課題の整理、ユースケース分析、実装上の留意点の共有を行っている点に特徴がある。特に、OS イメージやライブラリといった既存のデジタル資産（ソフトウェア資産）が広範に展開されているソフトウェア流通・サプライチェーンを対象とし、PKI やコード署名(ソフトウェアの真正性証明)における量子コンピュータによる暗号解読リスク低減を重要テーマとして位置付けている。PQCC の議論は、将来の正式標準を先取りする形での設計判断や運用上の知見を提供する役割を担っており、NIST や IETF 等の標準化動向を実装・運用の観点から補完する存在といえる。

7.11.2 PQC およびハイブリッド構成に関する標準化動向

PQCC は、PQC の長期安全性に対する不確実性と、既存の PKI やソフトウェア署名基盤が直ちに全面刷新できない現実を踏まえ、移行期におけるハイブリッド方式の必要性を強調している。PQCC が公開している文書「Artifact Signing: Dual Post Quantum / Traditional Hybrid Signatures and Downgrades」[50]では、ソフトウェア配布物やアップデートファイルの署名 (Artifact Signing) を対象に、PQC と現在の暗号方式を併用するデュアル署名型ハイブリッド方式の設計意義とリスクが整理されている。同文書では、単一の PQC 署名への一足飛びの移行は現実的ではなく、既存検証基盤との互換性を維持しつつ耐量子計算機性を付加できる段階的移行が実務上不可欠であるとの立場が示されている。

具体的には、既存の署名方式（例：RSA／ECDSA）と PQC 署名（例：ML-DSA）を同一成果物に対して並列に付与するデュアル署名構成を採用し、検証側は両方、もしくは少なくとも一方を検証できる柔軟性を持つ設計が議論されている。これにより、PQC 対応が未整備なクライアント環境でも既存の署名方式による署名検証が可能となる一方、量子計算機出現後を想定した耐量子計算機性の検証経路も確保される。

ただし PQCC は、この柔軟性が逆にダウングレード攻撃や検証ポリシーの不整合を招く可能性があることを明示的に指摘している。具体的な失敗シナリオとしては、攻撃者が意図的に PQC 署名を除去し、脆弱となった既存署名のみを提示した場合に、検証者が（互換性維持のための設定により）それを正当なものとして受理してしまうケースが挙げられる。このように、検証ポリシーの設定が不適切であれば、PQC 署名が実質的に無視され、耐量子計算機性が失われるリスクがある。

そのため PQCC 文書では、ハイブリッド署名を導入する際には、技術仕様そのものよりも、検証ポリシー、署名優先順位、失効・更新時の運用ルールが安全性を左右すると整理している。この観点は、NIST や IETF が主にアルゴリズムや構成方式を定義しているのに対し、PQCC が運用面での失敗シナリオを具体的に提示している点に特徴がある。また、PQC アルゴリズム自体も標準確定直後は実装成熟度が十分でない可能性があるため、単独 PQC 署名への即時依存を避ける意味でも、移行期のハイブリッド方式はリスク分散手段として有効であると結論付けている。

8. 調査結果に関する考察

2020 年時点では、ハイブリッド構成は概念レベルに留まり、標準化活動は議論開始段階にあった。しかし、2025 年から 2026 年初頭にかけて、主要な標準化機関により以下の事実が確認される。

- NIST
  ML-KEM および ML-DSA を FIPS 203 および FIPS 204 として標準化。SP 800-227 で Multi-Algorithm KEM および PQ/T ハイブリッドの設計指針を提示。SP 800-56C Rev.2 で複数の共有秘密(Z, T)を連携した Z’＝Z || T を KDF の入力として扱う方法を規定。SP 1800-38C により TLS や X.509 を対象とした相互運用性評価を報告。
- IETF
  TLS WG が draft-ietf-tls-hybrid-design-16 で TLS 1.3 におけるハイブリッド鍵共有を定義。LAMPS WG が Composite KEM および Composite 署名の仕様を策定（draft-ietf-lamps-pq-composite-kem-12、draft-ietf-lamps-pq-composite-sigs-14）。PQUIP WG は RFC 9794 で PQ/T ハイブリッド方式に関わる用語を体系化し、Hybrid signature spectrums を提示。
- ETSI
  TS 103 744 でハイブリッド鍵共有および CatKDF／CasKDF による複数の共有秘密の統合方式を仕様化。TR 103 966 で移行設計上の考慮事項を整理。
- NSA
  CNSA Suite 2.0 で Kyber＋ECDH 構成を推奨。CSfC ガイダンスで TLS、IPsec におけるハイブリッド構成の適用方針を明示。
- その他の機関
  IEEE は 802.11 におけるハイブリッド鍵共有の提案を提示し、P1943 でネットワークセキュリティ全般の耐量子計算機化枠組みを検討。ISO/IEC は概念整理とリエゾン調整を担当し、具体的なハイブリッド仕様は定義していない。CSA はクラウド環境におけるハイブリッド導入ガイドを公表。PQCC はソフトウェア署名におけるデュアル署名モデルを提示。

2026 年 1 月時点で、ハイブリッド構成は主要標準化機関により技術仕様として確立され、TLS、X.509 などのプロトコルにおいて、具体的な実装指針が整備されている。

- TLS1.3 の例
  draft-ietf-tls-hybrid-design-16 により、複数 KEM の公開鍵・暗号文を連結して key_share に配置し、双方が得た shared_secret を HKDF で統合する手順が明確化され、ハイブリッド鍵共有が実装可能な形で定義されている。
- X.509／PKI の例
  LAMPS WG で策定された Composite KEM および Composite 署名、ITU で策定された代替署名拡張（Alternative Signature Algorithm）により、PQC 方式と従来方式を単一証明書内で合成また混成できる構造が仕様レベルで整備され、移行期の証明書運用における選択肢が確立された。
- ハイブリッド鍵共有方式（ETSI TS 103 744）の例
  ECDH＋ML-KEM のハイブリッド鍵共有方式、並びに CatKDF／CasKDF を用いた共有秘密の結合方法が規定され、プロトコル実装者が参照可能な手順として提示されている。

これらの具体的な整備により、ハイブリッド構成は単なる概念段階を超えて、既存プロトコル・証明書・運用基盤の中で「移行期に採用可能な実装構成」として体系的に確立されたと評価できる。

9. 参考文献

[1] CRYPTREC 暗号技術調査ワーキンググループ（耐量子計算機暗号），“CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）2024 年度版，” 3 2025. [オンライン]. Available: https://www.cryptrec.go.jp/report/cryptrec-gl-2007-2024.pdf.

[2] CRYPTREC 暗号技術調査ワーキンググループ（耐量子計算機暗号），“耐量子計算機暗号の研究動向調査報告書，” 3 2025. [オンライン]. Available: https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2024.pdf.

[3] レピダム，“ハイブリッドモードの技術動向調査，” 12 2020. [オンライン]. Available: https://www.cryptrec.go.jp/exreport/cryptrec-ex-3004-2020.pdf.

[4] NIST, “Mechanisms Recommendations for Key-Encapsulation Mechanisms,” 9 2025. [オンライン]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-227.pdf.

[5] デジタル庁・総務省・経済産業省，“電子政府における調達のための参照すべき暗号のリスト（CRYPTREC 暗号リスト），” 16 5 2023. [オンライン]. Available: https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022r1.pdf.

[6] K. Moriarty, B. Kaliski, J. Jonsson , A. Rusch, “PKCS #1: RSA Cryptography Specifications Version 2.2,” 11 2016. [オンライン]. Available: https://datatracker.ietf.org/doc/html/rfc8017.

[7] R. Housley , S. Turner, “Use of the RSA-KEM Algorithm in the Cryptographic Message Syntax (CMS),” 2 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/rfc9690/.

[8] PQCC, “Post-Quantum Cryptography (PQC) Migration Roadmap,” 5 2025. [オンライン]. Available: https://pqcc.org/wp-content/uploads/2025/05/PQC-Migration-Roadmap-PQCC-2.pdf.

[9] NIST, “NIST Special Publication 800-56C Recommendation for Key-Derivation Methods in Key-Establishment Schemes, ” 8 2020. [オンライン]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf.

[10] D. Connolly, R. Barnes , P. Grubbs, “Hybrid PQ/T Key Encapsulation Mechanisms,” 20 10 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-irtf-cfrg-hybrid-kems/07/.

[11] M. Ounsworth, J. Gray, M. Pala, J. Klaußner , S. Fluhrer, “Composite ML-KEM for use in X.509 Public Key Infrastructure, ” 7 1 2026. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/12/.

[12] M. Ounsworth, J. Gray, M. Pala, J. Klaußner , S. Fluhrer, “Composite ML-DSA for use in X.509 Public Key Infrastructure, ” 8 1 2026. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/14/.

[13] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” 7 3 2020. [オンライン]. Available: https://datatracker.ietf.org/doc/rfc8446/.

[14] D. Stebila, S. Fluhrer , S. Gueron, “Hybrid key exchange in TLS 1.3,” 18 11 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/16/.

[15] X. Tian, B. Hale, M. Mularczyk , Joël, “Amortized PQ MLS Combiner,” 4 11 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-mls-combiner/02/.

[16] ETSI, “ETSI TS 103 744 V1.2.1 CYBER; Quantum-Safe Cryptography (QSC); Quantum-safe Hybrid Key Establishment, ” 3 2025. [オンライン]. Available: https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.02.01_60/ts_103744v010201p.pdf.

[17] IEEE, “Proposed Texts for Hybrid PQC, ” 25 11 2025. [オンライン]. Available: https://mentor.ieee.org/802.11/dcn/25/11-25-2051-01-00bt-proposed-texts-for-hybrid-pqc.docx.

[18] T. Okubo, C. Bonnell, J. Gray, M. Ounsworth , J. Mandel, “A Mechanism for X.509 Certificate Discovery,” 19 11 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-lamps-certdiscovery/02/.

[19] ITU, “ITU-T Recommendations,” 10 2019. [オンライン]. Available: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509.

[20] M. Ounsworth, “ “Architecting PKI Hierarchies for Graceful Post-Quantum Migration,” presented at the PKI Consortium Post-Quantum Cryptography Conference 2025,” 1 2025. [オンライン]. Available: https://pkic.org/events/2025/pqc-conference-austin-us/WED_BREAKOUT_1200_Mike-Ounsworth_Architecting-PKI-Hierarchies-for-Graceful-PQ-Migration.pdf.

[21] J. Klaußner, “ “Hybrid PQC E-Mail Communication: Easing Migration Pain,” presented at the Post-Quantum Cryptography Conference 2025, ” 1 2025. [オンライン]. Available: https://pkic.org/events/2025/pqc-conference-austin-us/WED_BREAKOUT_1430_Jan-Klaussner_Hybrid-PQC-E-Mail-Communication-Easing-Migration-Pain.pdf.

[22] NIST, “NIST IR 8547 ipd Transition to Post-Quantum,” 11 2024. [オンライン]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf.

[23] F. D, M. P , B. Hale, “RFC 9794 Terminology for Post-Quantum Traditional Hybrid Schemes,” 13 6 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/rfc9794/.

[24] N. Bindel, B. Hale, D. Connolly , F. D, “Hybrid signature spectrums,” 17 9 2025. [オンライン]. Available: https://datatracker.ietf.org/doc/draft-ietf-pquip-hybrid-signature-spectrums/07/.

[25] L. Chen, “Cryptographic Agility and Transition R&D and Plans,” 21 3 2024. [オンライン]. Available: https://csrc.nist.gov/Presentations/2024/cryptographic-agility-and-transition-rd-and-plans.

[26] Open Quantum Safe Project, “Open Quantum Safe, ” [オンライン]. Available: https://openquantumsafe.org/.

[27] Open Quantum Safe Project, “liboqs: C library for post-quantum cryptography,” [オンライン]. Available: https://github.com/open-quantum-safe/liboqs.

[28] Open Quantum Safe Project, “ OQS-OpenSSL, ” [オンライン]. Available: https://github.com/open-quantum-safe/openssl.

[29] The Legion of the Bouncy Castle, “Bouncy Castle Crypto APIs,” [オンライン]. Available: https://www.bouncycastle.org/.

[30] wolfSSL Inc., “Hybrid Post-Quantum Key Exchange in wolfSSL,” [オンライン]. Available: https://www.wolfssl.com/hybrid-post-quantum-key-exchange-in-wolfssl-5-8-0/.

[31] PKI Consortium, “Post-Quantum Cryptography Conference,” 15-16 1 2025. [オンライン]. Available: https://pkic.org/events/2025/pqc-conference-austin-tx/.

[32] PKI Consortium, “Post-Quantum Cryptography Conference,” 28-30 10 2025. [オンライン]. Available: https://pkic.org/events/2025/pqc-conference-kuala-lumpur-my/.

[33] M. Marcus, “"Real-World Post-Quantum Migrations: Lessons Learned and Performance Results,” presented at the Post-Quantum Cryptography Conference 2025,” 10 2025. [オンライン]. Available: https://pkic.org/events/2025/pqc-conference-kuala-lumpur-my/THU_P_1400_michiel-marcus_real-world-post-quantum-migrations-lessons-learned-and-performance-results_merged.pdf.

[34] S. Kelly, “The Internet Is Ready for Some PQC Certificates,” presented at the Post-Quantum Cryptography Conference 2025, ” 10 2025. [オンライン]. Available: https://pkic.org/events/2025/pqc-conference-kuala-lumpur-my/WED_B_1130_shane-kelly_the-internet-is-ready-for-some-pqc-certificates_merged.pdf.

[35] S. Barker, “X25519Kyber768: Paving the Way for Post-Quantum Security,” 21 9 2024. [オンライン]. Available: https://expertbeacon.com/x25519kyber768-paving-the-way-for-post-quantum-security/.

[36] Google, “Protecting Chrome Traffic with Hybrid Kyber KEM,” 10 8 2023. [オンライン]. Available: https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html.

[37] NIST, “ Post-Quantum Cryptography, ” 3 1 2017. [オンライン]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/call-for-proposals.

[38] NIST, “ NIST SP 1800-38 Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography,” 19 12 2023. [オンライン]. Available: https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1).

[39] B. Halee, X. Tiane , L. Wang, “Benchmarking of the Amortized Post Quantum Combiner for MLS,” 8 1 2026. [オンライン]. Available: https://eprint.iacr.org/2026/034.pdf.

[40] ITU, “Overview of hybrid approaches for key exchange with quantum key distribution,” 20 5 2022. [オンライン]. Available: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2022-1-PDF-E.pdf.

[41] ETSI, “ETSI TR 103 966 V1.1.1 CYBER Security (CYBER);Quantum-Safe Cryptography (QSC); Deployment Considerations for Hybrid Schemes,” 10 2024. [オンライン]. Available: https://www.etsi.org/deliver/etsi_tr/103900_103999/103966/01.01.01_60/tr_103966v010101p.pdf.

[42] ETSI, “ETSI TS 104 015 V1.1.1 Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Efficient Quantum-Safe Hybrid Key Exchanges withHidden Access Policies,” 2 2025. [オンライン]. Available: https://www.etsi.org/deliver/etsi_ts/104000_104099/104015/01.01.01_60/ts_104015v010101p.pdf.

[43] IEEE, “ Standard for Post-Quantum Network Security, ” [オンライン]. Available:

https://standards.ieee.org/ieee/1943/10957/.

[44] L. CHEN, “PAVING THE RUNWAY FOR STANDARDIZATION OF POST-QUANTUM CRYPTOGRAPHY,” *SC27 Journal,* 第 巻 Vol 1, 第 Issue 3, pp. pp. 11-19, 2 2022.

[45] ASC X9, “New X9 Report Supplies Guidance on Migrating to Post-quantum Cryptography Safely and Cost-effectively,” 8 2025. [オンライン]. Available: https://x9.org/new-x9-report-migrating-to-post-quantum-cryptography/.

[46] NSA, “Announcing the Commercial National Security,” 9 2022. [オンライン]. Available: https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF.

[47] NSA, “CSfC Post Quantum Cryptography Guidance Addendum 1.0,” 4 4 2025. [オンライン]. Available: https://www.nsa.gov/Portals/75/documents/resources/everyone/csfc/capability-packages/CSfC%20Post%20Quantum%20Cryptography%20Guidance%20Addendum%201_0%20Draft%20_5.pdf.

[48] CSA, “A Practitioner’s Guide to Post-Quantum Cryptography,” 10 11 2025. [オンライン]. Available: https://cloudsecurityalliance.org/artifacts/a-practitioners-guide-to-post-quantum-cryptography.

[49] PQCRYPTO , “Post-Quantum Cryptography for Long-Term Security,” 9 4 2018. [オンライン]. Available: https://pqcrypto.eu.org/deliverables/d5.2-final.pdf.

[50] P. Kampanakis , D. V. Geest, “Artifact Signing: Dual, Post-Quantum/Traditional Hybrid Signatures and Downgrades,” 4 2025. [オンライン]. Available: https://pqcc.org/artifact-signing-dual-post-quantum-traditional-hybrid-signatures-and-downgrades/.