アプリケーションノート

VIAVI Solutions

通信の未来に備える：量子安全技術の台頭

組織が量子アルゴリズムや量子アーキテクチャを理論モデルやラボ環境から現実世界の安全な環境に移行させることができるようにするためのセキュリティフレームワークや検証ツールを紹介。

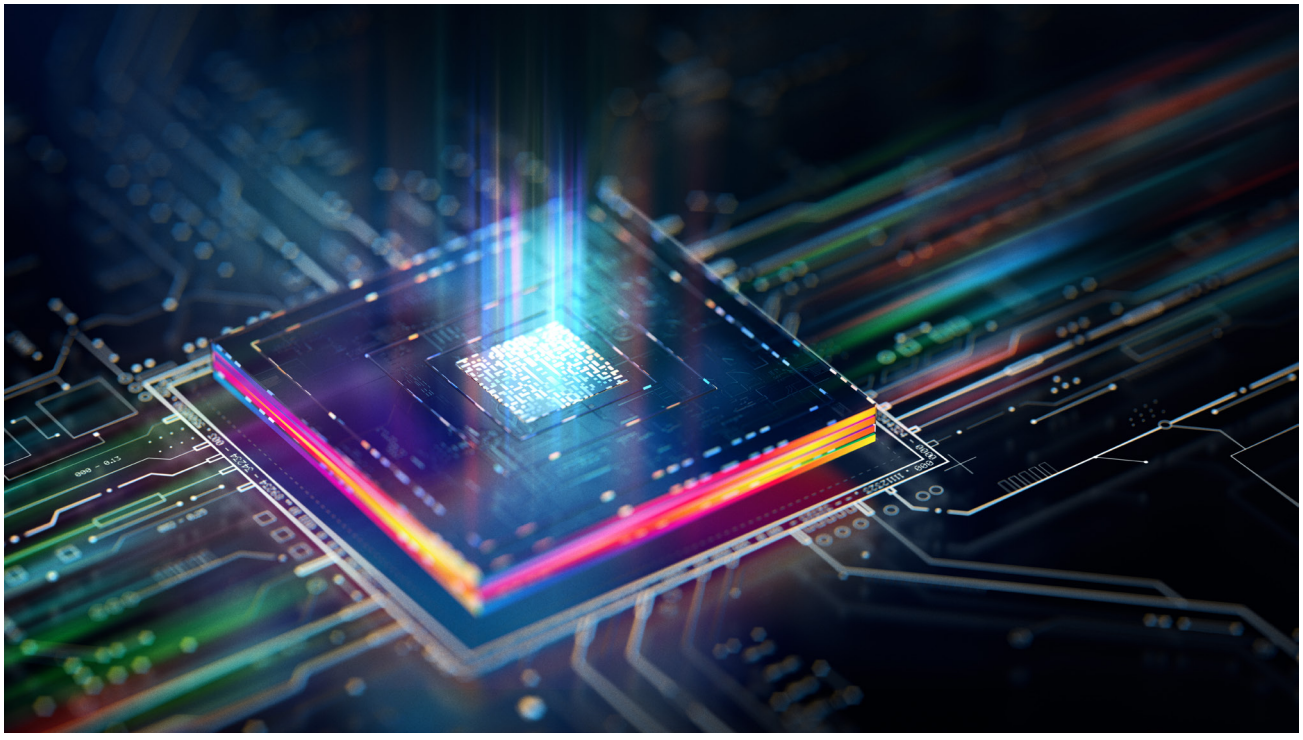
目次

量子安全通信はもはや遠い目標ではありません。すでに起こりつつあります。量子鍵配送（QKD）、ポスト量子暗号（PQC）、End-to-End のハイブリッド QKD-PQC モデル、衛星ベースの暗号と鍵管理、従来型システムと量子安全システムを組み合わせた過渡的なアーキテクチャなど、多様な技術のエコシステムがこの進歩を推進しています。これらの革新は、量子コンピューティングの破壊的なインパクトを踏まえ、安全な通信に関する私たちの理解を根本から変革しつつあります。

これらの技術が発展する中、アーキテクチャと展開するシステムに最大限のレジリエンスとセキュリティ、効率性、現実世界での信頼性を確保することが極めて重要になっています。これは、量子テクノロジーと物理インフラが交差する光レイヤーにおいて特に重要です。多くの場合、量子科学、特に量子光学を、実験用のセットアップから信頼性の高い、フィールドですぐに使えるソリューションに変えることが課題です。

この移行には、標準化と適合性の実現がきわめて重要です。加えて、インフラ、特に安全な量子伝送を支える光システムに対する深い理解も必要です。光学技術は単なる部品ではありません。それは量子安全通信を構成する土台のひとつです。

成功には、量子的なイノベーションとファイバーに関する深い専門知識を併せ持つ信頼できるパートナーが不可欠です。本稿では、量子安全技術を大規模に展開するための重要な要素について考察します。VIAVI は、光ファイバーにおける数十年にわたるリーダーシップと高度な量子研究を融合させ、この結節点で独自の地位を確立しています。システム、物理学、ラボでの検証において 30 年以上の経験を持つ VIAVI は、光子ベースの通信をラボから実用的な展開へと安全かつ効率的に移行させる方法について、独自の視点を提供しています。



1　はじめに

量子コンピューティング能力の爆発的な向上は、デジタルセキュリティの在り方を一変させようとしています。量子プロセッサーが実用化に近づくにつれ、今日の通信、金融システム、デジタル ID を保護する暗号基盤は存亡の危機に直面しています。しばしば Q デーと呼ばれる、この迫り来る節目は、量子コンピュータが RSA や楕円曲線暗号（ECC）などの広く使われている公開鍵暗号システムを解読できるようになり、世界中の暗号化されたデータの多くが復号化に対し脆弱になるポイントを示しています。

Q デーはまだ訪れていませんが、今こそ行動を起こすことが求められています。現在収集されるデータは、将来的に解読される可能性があり、これは「今収集し、後で解読する」と呼ばれる脅威です。これを受けて、政府、標準化団体、企業は、量子マシンの計算能力に耐える量子安全技術の導入に向けた取り組みを加速させています。

この進化には、標準化と適合性テストが不可欠です。厳密な検証を行わなければ、最も有望な量子安全ソリューションであっても、導入時に失敗する危険性があります。インフラ、特に光ファイバー、光子伝送、シグナルインテグリティに関する考慮事項は、正確に対処する必要があります。

しかし、理論を実践に移すことは極めて複雑な取り組みです。量子安全技術は、単に安全であるだけでなく、相互運用性、レジリエンス、移行性を持ち、実世界の環境で実現できる必要があります。これは、量子信号が送受信される光レイヤーや、量子鍵暗号化後のレイヤーにおいて特に重要です。多くの点で、課題は、量子技術、特に量子光学をラボからフィールドに移し、科学的な実験から運用可能なシステムに変えることです。

この点において、VIAVI の専門知識は不可欠になります。光ファイバー、システムエンジニアリング、ラボでの検証において 30 年以上のリーダーシップを持つ VIAVI は、量子への移行をサポートするユニークな位置にあります。当社の量子安全性テストスイートは、耐量子技術の機能性、コンプライアンス、パフォーマンス、レジリエンスを評価するための包括的なプラットフォームを提供します。既存のインフラに組み込むか、テストベッドに導入するかを問わず、VIAVI のソリューションにより、関係者は自信を持って量子安全システムを評価して導入できるようになります。

本稿では、量子安全通信の進化、それを推進する技術、そしてポスト量子世界への安全でシームレスな移行を保証するためのテストと検証の非常に重要な役割を考察します。

2　量子安全ネットワーク

2.1　必要とされる理由

デジタル暗号化は、携帯電話のような無線通信システムには欠かせない要素です。盗聴者は通話を盗聴してデータを抜き取ろうとしますが、データを暗号化すればこの脅威はなくなります。量子コンピュータの台頭により、現代の暗号化方法は破られるリスクがあります。量子コンピュータはまだ 5〜10 年先の話ですが、悪意のあるアクターは今データを不正に取得し、量子コンピュータが機能するようになったときに後で解読することができます。これは「今収集し、後で解読する（HNDL）」脅威として知られ、政府、軍、金融機関にとって重大な懸念事項となっています。この問題の解決策の 1 つは、量子コンピューティングや盗難情報の潜在的脅威から機密データを保護するために PQC を採用する方法です。

携帯電話の標準化団体である 3GPP は、将来の量子コンピュータ攻撃から防御するために、PQC アルゴリズムを組み込むように標準化を進化させています。3GPP は、標準化された PQC アルゴリズムについて、他の標準化団体（すなわち、米国国立標準技術研究所（NIST））に依存しています。量子コンピュータがもたらす可能性のある攻撃に対する懸念から、GSMA（Global System for Mobile Communications Association）は、ポスト量子対応への移行方法についてモバイル事業者に助言するため、ポスト量子通信ネットワークタスクフォース（PQTN）を設立しました。

QKD の標準化は、相互運用性、セキュリティ保証、量子安全通信システムの世界的な採用を確実なものにする必要性から、10 年以上にわたって進められてきました。欧州電気通信標準化機構（ETSI）、国際電気通信連合（ITU-T）、ISO/IEC などの団体が主導して、QKD システムのフレームワーク、プロトコル、セキュリティ要件を定義してきました。

2.2　標準規格

QuIC（EU）、QIC（カナダ）、Q-STAR（日本）、QED-C（米国）、UKQuantum（英国）、KQIA（韓国）、NQSN（シンガポール）、QIIA（中国）など、それぞれの国や地域が量子技術に関連するフォーラムを設立しています。ただし、その動機や目標は異なる場合があります。例えば、米国は国家量子イニシアティブ法で、量子技術の研究、人材育成、産業革新を促進することを目指しています。中国は「量子技術ロードマップ」で暗号や材料科学など特定の応用分野で量子の優位性を目指し、研究、人材、インフラなど多面的なアプローチを採用しています。日本は、量子技術を誰もが利用できる社会を構築し、量子技術のグローバル化を推進するとともに、量子技術の応用によるビジネスチャンスの創出を支援することを目指しています。

欧州では、量子通信、量子コンピューティング、量子センシングに焦点を当てた基礎研究を重視し、量子ハードウェア、量子ソフトウェア、量子アルゴリズムに投資してエコシステムの強化を図ろうとしています。この取り組みにより、量子計算、量子センシング、量子通信の研究拠点を育成しています。

ITU-T SG11、SG13、および SG17 は、ETSI ISG QKD とともに、QKD および QKDN の標準化に取り組んできています。ISO/IEC/JTC1 は、QKD モジュールの評価方法をいくつか規定しています。GSMA は、電気通信業界における PQC とハイブリッドシナリオのガイドラインを提供しています。

NIST は PQC アルゴリズムの定義において主導的な役割を果たしており、すでに 2024 年 8 月に最初の 3 つのアルゴリズムを発表しています。CRYSTALS-Kyber、CRYSTALS-Dilithium、および SPHINCS+ アルゴリズムに基づくこれらの標準規格は、将来の量子コンピューティング機能に対する安全な通信とデータ保護を保証するように設計されています。NIST は PQC 規格を制定する米国の機関ですが、多くの国が NIST の勧告を採用する道を選んでいますが、一部の国は独自のバージョンを作成することを決定しています（すなわち、中国や韓国）。

ETSI、ITU-T、ISO/IEC は、QKD システムのフレームワーク、プロトコル、セキュリティ要件の定義を主導してきました。ETSI の QKD 業界仕様グループ（ISG-QKD）は特に影響力が大きく、QKD コンポーネント、ネットワークアーキテクチャ、従来型暗号システムとの統合に対応する技術レポートや仕様を策定しています。一方、ITU-T は QKD ネットワークアーキテクチャと鍵管理インターフェイスの標準化に取り組んでおり、グローバルな展開戦略の調和を目指しています。このような進展にもかかわらず、いくつかの極めて重要な課題が残っています。

第一に、異なるベンダーの QKD システム間の相互運用性はまだ限られており、大規模なマルチベンダー展開の妨げとなっています。第二に、特に QKD をポイントツーポイントリンクだけでなく、複雑なメッシュ型ネットワークに拡張する場合、拡張性が依然として懸念事項となっています。第三に、専用の光ファイバーや信頼できるノードの必要性など、コストやインフラ要件が普及の障壁となっています。さらに、QKD システムのセキュリティ認証と適合性テストはまだ発展途上にあり、実世界の条件下での性能とレジリエンスに関する普遍的に受け入れられたベンチマークはありません。最後に、QKD を既存のセキュリティインフラと統合し、新たなポスト量子暗号標準と整合させることは、技術的かつ戦略的な課題でもあります。

2.3 QKDとPQC

システムが使用するポスト量子鍵の配布に関しては、2 つの方法が計画されています。QKD と PQC です。QKD は量子力学の特性を利用して鍵が交換が行われ、干渉を検知すると新たな交換が起きるため、盗聴はほとんど不可能です。耐量子暗号技術が必要とされるユースケースは大きく異なるため、両方の技術が共存することになると考えられます。

QKD では、量子ビット（情報の量子単位）を使って、光学的手段（地上ファイバー、自由空間光学、衛星リンク）を介して暗号鍵を交換します。この方法では、量子力学の基本原理である量子もつれ（通常は光子）を利用しているため、暗号化に用いる鍵が盗聴者に傍受されれば必ず検知でき、事実上改ざんは不可能です。伝送への干渉が試みられると、その試みが通信プロトコルにより直ちに検出され、通信は即時に停止します。このような場合、機密データが送信される前に新しい鍵を送信することができます。

QKD はハードウェアベースであるためコストが高く、その最適な用途は、あらゆる状況下で機密性を維持する必要がある、機密性の高いアプリケーションです。このようなアプリケーションでは、関係者の所在は一定であり、コストは最大の関心事ではありません。QKD が最も効果的に使用できる市場は、失敗した場合にその代償が壊滅的なものになりかねない、政府、軍、金融サービスの特定の分野です。

一方、PQC はソフトウェアベースのアプローチで、QC 攻撃に脆弱な既存の鍵アルゴリズム（RSA、ECC など）の代わりに、新しい数学的問題に基づくアルゴリズムを使用します。これらのアルゴリズムを破ることが可能かどうかは予見できず、こんのため 100% の保証は得られません。しかし、QKD に比べ低コストのソリューションであり、今後主流になることが予想されます。

まとめると、QKD にも PQC にも長短があります。したがって、QKD と PQC の共存シナリオは、従来型セキュリティメカニズムと同様に、実際のネットワークや検証システムで検討する必要があります。

	QKD	PQC
機器	光ファイバーと専用のトランシーバー	ソフトウェアの交換
セキュリティ手法	量子力学的セキュリティ	計算セキュリティ
長所	スニッフィングが不可能	ソフトウェアによるアップグレードが容易
短所	距離が短い（100km 程度まで、衛星ベースの QKD で解決可能）、速度が遅い、コストが高い	100% 安全ではなく、パフォーマンスに懸念があり、移行に時間を要する
標準化	ITU-T（Y.3800/X.1700シリーズ）、ETSI	IETF、NIST
ユースケースの例	国家安全保障、専用線	大規模通信、インターネットバンキング、企業サイト

現実には、独自の QKD プロトコル、異なる PQC 実装、ばらばらな鍵管理システムなど、量子安全エコシステムは本質的に断片化しています。しかし、こうした技術の世界的なサプライチェーンを強化し、実装に異種混合のアプローチを提供することが、本質的かつ戦略的に必要なことです。

相互運用性テストと検証のフレームワークは、統合におけるリスクを減らし、エコシステムの発展と標準への準拠を加速するために不可欠です。それらは、個々のベンダーのラボでは提供できない、あるいは提供しようとしない公共的な利益を担っています。

2.4 産業への影響

ポスト量子への対応は、政府、金融、医療、軍事、通信など、あらゆる業界に影響します。個人、金融、政府のデータはすべて、デジタル転送中は暗号化される必要があります。ひとたび量子コンピュータが利用可能になれば、悪質なアクターはいつでもどこでも、どのようなシステム上でも量子コンピュータを利用することができるため、データを守るための競争は今始まっています。量子コンピュータが登場する前であっても、HNDL のリスクは存在し、データが今傍受され、量子解読が可能になるまで保存され、機密情報にアクセスできるようになる可能性があります。

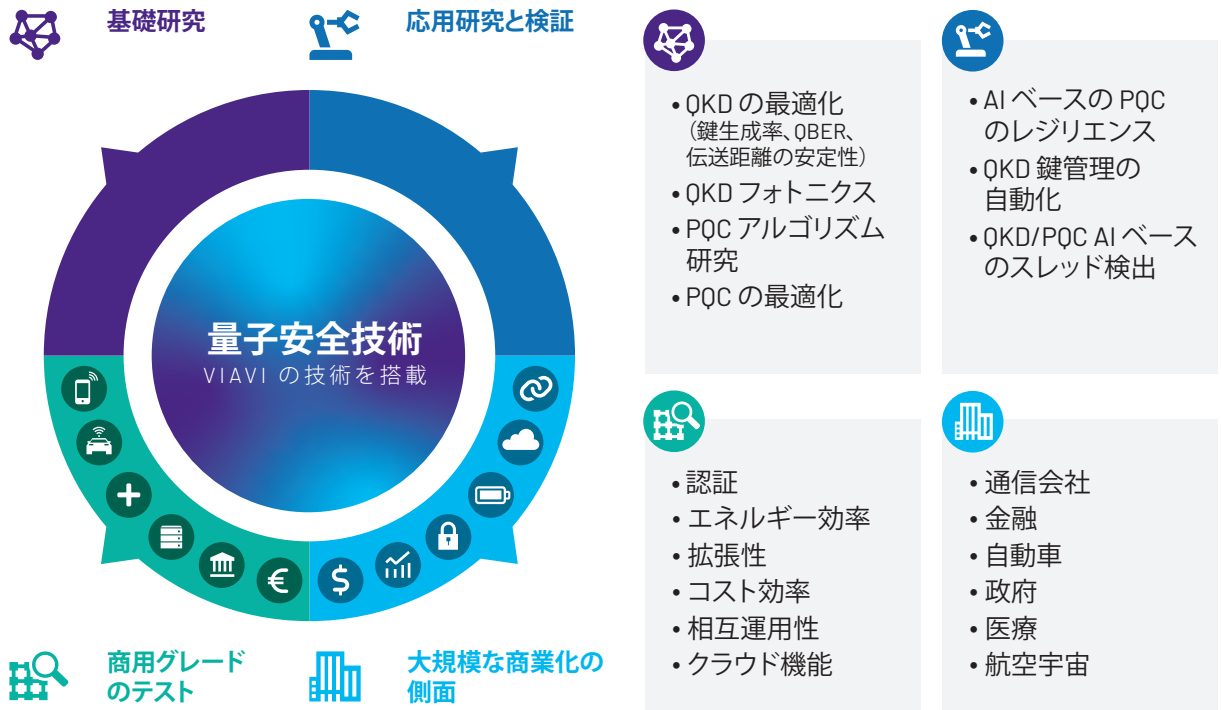
各業界は PQC への移行の道筋を個別に管理していますが、移行ロードマップなど多くの共通要素もあります。例えば、電気通信の管理団体である GSMA は、*「電気通信のユースケースのためのポスト量子暗号ガイドライン」*という報告書を発表しています。インド準備銀行は、「量子コンピューティング時代におけるインド銀行セクターのセキュリティ確保」と題したホワイトペーパーを発表しました。

しかし、規制認証、投資家の信頼確保、分野横断的な技術展開に不可欠な、信頼できる検証プラットフォームへの需要は、あらゆる業界で高まっています。このプラットフォームは、包括的なハイブリッド環境に対応し、以下を含む（ただしこれに限定されない）さまざまな検証シナリオを実行する必要があります。

- PQC の拡張性と QKD の情報理論的セキュリティを組み合わせたハイブリッドなシミュレーション
- 物理的な光子伝送からアプリケーションレベルのハンドシェイクプロトコルまでの階層化テスト
- 同期、フォールバックロジック、優先順位付け、キーリフレッシュ動作のための HKMS テスト
- ハイブリッドなレジリエンスのためのカオステスト：QKD リンクで問題が発生したり、PQC が劣化したりした場合の継続性の評価
- エッジメトロ、クラウド、衛星（非地上系ネットワーク（NTN）、自由空間光学、衛星ベースの QKD を含む）を横断するクラシック - 量子ハイブリッドネットワークをシミュレートするデジタルツイン環境
- パブリック対プライベート、コア対エッジなど、展開モデル間のコストパフォーマンスのベンチマーク

3　量子安全テストドメイン

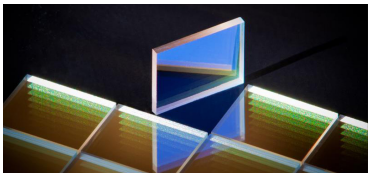
現在、量子安全ネットワークは移行段階にあり、ライフサイクル管理と大規模な商業化への取り組みを検討する必要が生じています。VIAVI はテストに関わるすべてのドメインをサポートしています。



1990.900.0725

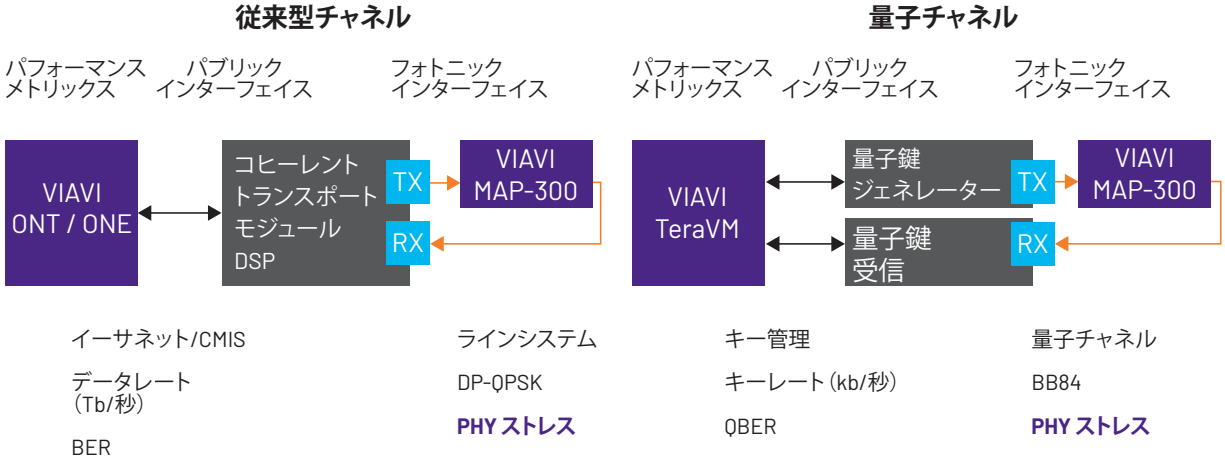
- 基礎研究：QKD 最適化、QKD フォトニクス、PQC アルゴリズム、PQC 最適化、量子セキュリティ、量子シミュレーション
- 応用研究と検証：QKD 鍵管理の自動化、QKD/PQC の AI ベースのスレッド検出、AI ベースの PQC レジリエンス（非 PQC プロトコルとのハイブリッドを含む）、ハイブリッドシステムの AI ベースのテスト自動化
- 商用グレードのテスト：認証、エネルギー効率、拡張性、コスト効率、相互運用性、クラウド機能
- 大規模な商業化の側面／要件：電気通信、金融、自動車、政府、医療、航空宇宙

本稿では、量子安全テストをサポートする VIAVI 製品群の各コンポーネントをコンテキストに即してレビューします。

量子安全ネットワーク機能	VIAVI 製品
QKD 鍵管理システムテスト	TeraVM セキュリティ
PQC パフォーマンステスト	TeraVM セキュリティ、VAMOS
量子チャネル評価	MAP-300 
ファイバー監視	ONMSi リモートファイバーテスト 
ファイバーセンシング	FTH-DTSS 
ネットワークの可観測性	NITRO® AIOps、ONMSi NITRO AIOps 
ファイバーインフラ/フィールド検証	OneAdvisor 800  INX 760 
運用効率	NITRO AIOps NITRO AIOps
ハイエンド光学製品	スペクトラムセンシングフィルター、光センサーフィルター 

次の図は、環境全体と VIAVI スイートの配置を示しています。

量子チャネルとクラシックチャネルの比較



量子チャネルと従来型チャネルのテストは、多くの点で同じです。
フォトニックインターフェイスの性質は大きく異なります。
ただし、どちらもエミュレートする必要のある光ファブリックで伝送されます。
光ストレッサーのレベルや種類は確実に変化します。

1991.900.0725

3.1 QKD システムのテストと監視

QKD システムには複数の基本的なテスト要件があります。それには、以下が含まれます。

- 実運用ネットワークに代表される広範なパワーおよびスペクトラム負荷シナリオをエミュレートする柔軟で再設定可能なフォトニックシステムを構築することによる QKD の障害対応。これは、新しい QKD システムやサブコンポーネントの性能や適用可能性を検証するために使用できます。
- ファイバーの種類、DWDM 信号（もしあれば）の大きさと位置、波長の追加や削除に伴う過渡的状態、P2P リンクの新しい光デバイス（光スイッチなど）の適合性に基づく QKD システムのレジリエンスの評価
- アンプからのインバンド/アウトバンドノイズ、ケーブルが動くことによる偏波状態の乱れ、アクティブな光素子（スイッチ、アッテネータ、波長スイッチ）からのディザや安定性、光コネクターによる単一または複数の反射イベントなど、制御されたさまざまな光ストレスを発生させる P2P リンクでのストレステスト
- サービスレイヤーへの ETSI GS QKD 014 コンプライアンステスト。QKD 鍵管理システムレイヤーは、レジリエンス、すなわち、IKEv2 (RFC8784) IPSec VPN トンネルを確立するためのポスト量子事前共有鍵（PPK）の取得に関して、L3 VPN アプリケーションレイヤーにどれだけ効率的にサービスを提供できるかどうかテストされます。これは、高度なポスト量子セキュリティのために VPN リンクで頻繁なキーローテーションが設定されている場合に、より重要となります。TeraVM の IKEv2 クライアントエミュレーションは、KMS/QKD レイヤーから PPK をフェッチする ETSI GS QKD 014 API をサポートしており、PPK 認証を使用したポスト量子安全 IKEv2 VPN トンネルで鍵が連続的にローテーションされる場合に、負荷がかかった状態で QoE をテストできます。
- ファイバーケーブルに対する温度や歪みなどの物理的攻撃のテスト、ならびに無許可の撤去作業

量子チャネル評価

テスト環境における量子チャネルの評価では、量子通信リンクが実環境またはシミュレートされた状況下で量子ビットの完全性をどれだけ維持できるかを測定します。これにより、導入の前にチャネルが安全な量子プロトコルをサポートしていることが保証されます。テスト環境における量子チャネルの評価には、量子通信リンクの挙動の特性評価も含まれ、通常は QKD や他の量子プロトコルへの適合性を評価します。

QKD の 2 つの主要なタイプは、離散変数 QKD（DV-QKD）と連続変数 QKD（CV-QKD）です。

- DV-QKD：単一光子の偏光や位相などの離散量子状態を用いて情報を符号化し、光子の到着時間を検出するために正確なクロック同期を必要とします。BB84 や E91 のようなプロトコルはこのカテゴリーに属します。検出器には単一光子検出器（APD、SNSPD など）が使用されます。
- CV-QKD：コヒーレントレーザー光の 4 値（振幅と位相）の連続変調を使用します。多くの場合、GG02 のようなガウス変調プロトコルに基づくホモダインまたはヘテロダイン検出によって情報が抽出されます。タイミングの精度要件はそれほど厳しくありませんが、位相基準の整合（ローカルのオシレーターの校正）が必要です。検出器には、ホモダイン検出器またはヘテロダイン検出器（従来型のフォトダイオード）が使用されます。

DV-QKD は長距離でより高いセキュリティ保証を提供しますが、ハードウェアが複雑になり、キーレートは低速になります。CV-QKDは、標準的な電気通信コンポーネントを使用する短距離、高レートのアプリケーションではより実用的です。テストアプローチは、ノイズ、同期、コンポーネントの校正に特に重点を置いて、それぞれの物理的特性とプロトコルの特性を考慮する必要があります。

テスト環境での量子チャネル評価のためのツールや方法には、単一光子検出器、量子光源、OTDR やその他の従来型の端面検査器、トモグラフィツール、ノイズ注入などのシミュレーターなどがあります。主要な測定値には、量子ビット誤り率（QBER）があり、送信された量子ビット（qubits）の誤り率を測定します。QBER が高くなると、ノイズや盗聴の可能性があります。その他の測定には、損失/減衰（dB/km）、コヒーレンス時間/偏波安定性、チャネル忠実度、タイミングジッターと同期などがあります。

テストには、光学テーブルや精密部品を使用した短距離テスト用の以下のラボベンチテストが含まれます。「現実世界」の距離（10km、50km など）でのシミュレーション、設置しファイバーに対するフィールドトライアル、衛星や空中でのテスト（自由空間光学系）。

量子安全の場合、チャネル評価は以下のような特定の側面に焦点を当てることができます。

- サイドチャネル攻撃に対する耐性：量子安全暗号の実装が、消費電力や電磁放射などの意図しない情報漏えいを悪用するサイドチャネル攻撃に対して脆弱でないことを保証するテスト
- 量子安全暗号化の検証：新たな脅威から重要インフラを守るため、各機関が量子安全暗号化手法を評価
- パフォーマンスと互換性のテスト：量子安全暗号ソリューションは、シームレスな移行を確実にするために、効率性と既存の IT システムとの統合についてテストされます。

これらの評価は、通信チャネルが将来の量子ベースのサイバー脅威に対して安全であることを保証することにより、量子時代に備えるのに役立ちます。

一般に、テスト用のセットアップは、ミスアライメント、温度ドリフト、検出器のダークカウントなどのエラーソースを低減するために最適化が繰り返され、QBER を安全なしきい値（BB84 QKD では通常 <11%）以下に抑えながらキーレートを最大化することを目標としています。

VIAVI のソリューション：MAP-300

量子テストでは、さまざまな量子実験条件を管理するために、スイッチ、波長管理ツール、エルビウム添加ファイバー増幅器（EDFA）、アッテネータで構成されるラボが必要です。QST は量子技術のトライアル/評価のためのネットワークを構築します。VIAVI MAP-300 は、リモートおよび自動化機能を備えた、高密度、かつ容易に再設定可能なモジュール式の光テストプラットフォームです。それは、コンピューティング、ネットワーキング、暗号化、および暗号技術における量子の限界を効果的に調査します。

MAP-300 は、実運用ネットワークに特徴的な広範なパワーおよびスペクトラム負荷シナリオをエミュレートする柔軟で再設定可能なフォトニックシステムを構築することで、QKD の障害に対応します。これは、新しい QKD システムやサブコンポーネントの性能や適用可能性を検証するために使用できます。また、QKD システムが以下の条件下でも動作可能であることを実証するのに必要な条件のマトリクスを定義する（標準化も）ための研究を行うことも考えられます。

- ファイバーの種類
- DWDM 信号（該当する場合）の大きさと位置
- 波長の追加ないし削除時の過渡的状態
- P2P リンクの新しい光デバイス（光スイッチなど）の適合性

制御された光ストレスの範囲を生成するための、QKD P2P リンクにおける全光学素子の作成と挿入

- アンプからのインバンドおよびアウトバンドノイズ
- ケーブルが動くことによる偏波状態の乱れ
- アクティブ光学素子（スイッチ、アッテネータ、波長スイッチ）によるディザまたは安定性
- 光コネクターによる単一または複数の反射イベント
- さまざまなレベルのノイズや外乱における QKD の誤り訂正メカニズムの開発に関する研究。現在の技術に関する研究とより良い方法の開発

ファイバー監視

ファイバー監視は、物理レイヤーの潜在的な攻撃を検出することで、量子安全通信において重要な役割を果たす可能性があります。例えば、ファイバーの盗聴は、QKD や他の量子安全プロトコルのセキュリティを危険にさらす恐れがあります。QKD は量子力学の基本的な性質に依存しています。具体的には、量子系を測定すると量子系が乱れるということです。しかし、攻撃者がファイバーを物理的に盗聴すれば、検知されずに信号を傍受しようとするかもしれません。

ファイバー傍受のシナリオでは、ファイバー監視は、信号損失の増加、後方散乱、または時間遅延などの異常を検出し、不正アクセスの試みを中央局舎に警告し、一般的に物理的な伝送媒体の完全性を維持するのに役立ちます。

ファイバー監視はまた、量子安全セキュリティ全体も強化します。QKD を使用しない場合でも、PQC アルゴリズムは安全な物理インフラに依存しています。誰かが受動的にファイバーを盗聴することができれば、暗号化されたデータを今日収集し、後で量子コンピュータ（HNDL）を使って解読する可能性があります。ファイバー監視はこのように、受動的な盗聴を阻止し、以下の手段で光通信ネットワークの完全性とセキュリティを確保することにより、量子安全暗号と物理レイヤーのセキュリティを補完する、防衛の第一線として機能します。

- 量子セキュア暗号化：ファイバー監視は、QKD と PQC を光ネットワークに統合することで、安全なデータ伝送を維持するのに役立ちます。これにより、量子時代のサイバー脅威から機密情報を確実に保護します。
- 超安全な量子通信：研究者は光ファイバーネットワークを使って量子情報を長距離伝送することに成功し、高価な極低温冷却を必要とせずに量子セキュアメッセージングの実現可能性を実証しました。[1]この進歩により、金融取引、医療データ、政府通信のセキュリティが強化されます。
- 量子暗号のための低レイテンシファイバー：量子暗号の効率を向上させるために、中空コアファイバーなどの新しい光ファイバー技術をテストしている組織もあります[2]。これらの技術革新は、量子セキュア暗号の適用可能な距離を拡大し、実世界での配備をより現実的なものにするのに役立ちます。

ファイバーセンシングを使ったり組み合わせることで、量子安全環境においてファイバー監視は、安全でレジリエンスのある通信ネットワークを確保することができます。

[1] https://techblog.comsoc.org/2025/05/03/ultra-secure-quantum-messages-sent-a-record-distance-over-a-fiber-optic-network/?copilot_analytics_

[2] https://www.luxquanta.com/luxquanta-collaborates-in-test-of-low-latency-fibre-in-data-centers-led-by-lyntia-n-71-en?copilot_analytics_

VIAVI のソリューション：ファイバーテストヘッド（FTH）を搭載した ONMSi 遠隔ファイバーテストシステム（RFTS）

ONMSi は、ネットワークの可視性をコアネットワークから PON まで更に宅内まで拡張する光ネットワーク監視システムで、あらゆる種類の光ネットワークで運用サポートとサービス品質（QoS）を改善します。ONMSi は、遠隔ファイバーテストシステムで、24 時間　365 日ファイバーネットワークをスキャンし、エンジニアをフィールドに派遣する必要なく、自動的に障害を検出し位置を特定します。業界トップの VIAVI 光学技術をベースに、光時間領域反射率計（OTDR）と光スイッチを統合したファイバーテストヘッド（FTH）は、データをベースラインと常に比較し、ファイバーに劣化があると、アラームを送信します。

ファイバーセンシング

ファイバーセンシングは、量子またはポスト量子セキュアネットワークの物理レイヤーに対するリアルタイムの侵入検知システムとして機能することにより、量子安全通信を強化することができます。最も単純に言えば、ファイバーセンシングは、光がファイバーに沿ってどのように反射または散乱するかを分析することによって、光ファイバーを分布型センサーに変えます。このセンシングは、レイリー散乱（振動や音響センシング用）、ブリルアン散乱（歪みや温度用）、ラマン散乱（温度プロファイリング用）によって実現され、これらのいずれの方法も長距離での微小な変化を検知できます。

ファイバーセンシングは、以下を提供することで、量子安全セキュリティをサポートします。

- QKD リンクの改ざん検知：QKD は、物理的な侵入が量子状態を乱すことを前提としています。ファイバーセンシングは、ファイバーを叩いたり、曲げたり、切断しようとする試みを重大なセキュリティ障害が発生する前に検出することで、別のレイヤーを追加します。例えば、誰かが光子を吸い上げるためにファイバーを曲げようとした場合、ファイバーセンシングは歪みや振動を検出し、警告を発することができます。
- 遅延盗聴の監視：PQC では、攻撃者は今ファイバーを盗聴して暗号化されたデータを保存し、後で量子コンピュータで復号化する可能性があります。ファイバーセンシングは、このような受動的な盗聴を検知するため、攻撃者が検知されずにいることが難しくなります。
- 状況認識の強化：ファイバーセンシングは、重要な量子安全インフラを脅かす可能性のある振動、環境妨害、無許可の工事を検出することができます。そうすることで、特に地下や露出した光ファイバー路にセキュリティ境界を提供します。

ファイバーセンシングは、物理的な攻撃を早期に警告し、リアルタイムで分散監視することで量子暗号を補完し、QKD と PQC の両方を物理レイヤーの脆弱性から保護することで、量子安全システムを強化します。そうすることで、潜在的な脅威に対してデータの完全性を維持しながら、安全で正確な測定を可能にし、量子安全環境において重要な役割を果たすことができます。例えば、エンタングルメントに依存することなく、長距離（すなわち、50km の光ファイバー）にわたって安全な量子リモートセンシング（SQRS）を提供したり、環境監視、災害対応、軍事監視のためのファイバーベースの量子センシングにより、確実に送信データの機密を維持し盗聴を防止したりできます。

これらの進歩は、量子セキュアアプリケーションにおけるファイバーセンシングの可能性が高まっていることを際立たせ、よりレジリエンスのあるスケーラブルな量子技術への道を開くものです。

VIAVI のソリューション：FTH-DTSS

VIAVI のファイバーテストヘッドの分布型温度と歪みセンシング（FTH-DTSS）は、市場で最も多用途の光ファイバーセンシングソリューションを使用して、パワーケーブル、パイプライン、通信ケーブルの温度と歪みを監視します。FTH-DTSS は、NITRO ファイバーセンシングソリューションの一部で、ファイバーケーブルとファイバー対応資産を継続的に監視します。これは光ファイバーケーブルを用いて、資産内や周辺環境で発生する温度や歪みを継続的にリアルタイムで監視します。そして、異常があれば即座に検出し、その位置を特定できます。FTH-DTSS の機能のいくつか次のような特徴をもっています。

- 高精度と信頼性が求められる業界向け。当社の革新的テクノロジーは、非常に長い光ファイバーケーブルに沿って温度と歪みを絶対測定するための分布型温度と歪みセンシング（DTSS）を提供し、さまざまなアプリケーションに不可欠なツールとなっています。
- 重要インフラ（電力供給）、パイプライン（石油、ガス、水など）、通信ネットワーク（データセンターインターコネクト（DCI））、その他多様なアプリケーションで異常の検出が可能
- プロアクティブな監視による温度と歪みの変化の追跡。この情報は、運用効率と応答性を向上させ、潜在的な損傷や故障を軽減するために取るべき先制的/プロアクティブなアクションを可能にする目的に利用できます。

3.2 PQC パフォーマンスのテスト

既存の暗号化アルゴリズムをポスト量子アルゴリズムに移行する際に注目されるのが、暗号鍵が大幅に長くなることの影響です。さらに、モバイルシステムのさまざまなコンポーネントで PQC を採用すると、特に無線帯域幅が制限されているユーザー端末では、性能やアーキテクチャに影響が出る可能性があります。地上波ネットワーク（TN）と NTN の両方を、PQC 対応の設定で徹底的にテストすることが不可欠です。以下は、電気通信業界からの懸念の声です。

会社名	PQC 移行に関する懸念
SKT	異なるメーカーの機器間、通信事業者間、国間での量子暗号ネットワークの統合的な運用と制御を可能するための、Q-SDN や QKDN Federation などの量子暗号ネットワーク統合技術の開発
Vodafone	Vodafone と IBM は、Vodafone のオールインワンデジタルセキュリティサービスである Vodafone Secure Net に IBM Quantum Safe 技術を統合するために協力することを発表しました。この概念実証は、PQC 規格を実装することで、将来の量子コンピューティングの脅威からスマートフォンユーザーを保護することを目的としています。
ソフトバンク	暗号化プロトコルがデータ伝送インフラに導入されると、通信に大きな負荷がかかり、レイテンシの問題が発生するため、品質が低下し、スループットが低下します。

会社名	PQC 移行に関する懸念
5G Americas	性能と相互運用性に潜在的な問題が予想されるため、徹底的なテストが必要です。
インド通信省	新しい PQC アルゴリズムは運用上重く、組織の主要業務に影響を与える可能性があります。新製品や更新された製品を継続的にテストし、その性能を監視することが不可欠です。
通信業界向けの GSMA ガイドライン	パフォーマンスへの影響を最小限に抑えるには、導入先で、特定のポスト量子暗号アルゴリズムの実行可能性を評価するテストを行うことが欠かせません。
インド準備銀行	懸念される要因としては、パフォーマンスのオーバーヘッドや複雑な実装があり、大規模なテストが必要になると考えられます。
BIS	新しい暗号の実装は、既存のインフラ内で正しく機能し、パフォーマンスレベルを維持し、システムの完全性を損なわないことを確認するために、徹底的にテストされる必要があります。

TeraVM PQC Performance テストソリューションは、VIAVI RAN2Core テストスイートのコンポーネントです。例えば、TM500（UE エミュレータ）に統合された PQC テストは、TN、NTN、IoT などの PQC を備えた多数の UE をエミュレートし、大規模なネットワークテストを可能にします。これにより、衛星ドメインを含む量子安全ネットワークデジタルツインが可能になります。

VIAVI のソリューション：TeraVM セキュリティ

システムが PQC に対応でき、パフォーマンスの観点から影響を受けないことを確認する最善の方法は、テストすることです。このテストで VIAVI TeraVM が活躍します。

TeraVM はソフトウェアテストツールです。VPN がトラフィックを処理し、マルウェアをフィルタリングする間、ユーザーとトラフィックをエミュレートし、VPN ヘッドエンドに限界までストレスを与え、ユーザーのパフォーマンスを測定することで、20 年以上にわたって VPN のパフォーマンスをテストしてきた実績があります。VPN テストを PQC テストに拡張するのは、この既存のソフトウェアツールに拡張機能を追加することにすぎません。VPN トンネルを PQC 標準アルゴリズムで暗号化します。これは、鍵サイズのバリエーション、リキーラウンド、ハイブリッド鍵など、追加の KPI を測定する必要があることを意味します。

多くの企業の IT 部門は、新機能を全社に展開する前にテストを行います。このためには、少人数のテスト担当者が世界中からログインして、新機能をテストします。このアプローチは、ほとんどのアップグレードやバグ修正には有効ですが、追加の計算オーバーヘッドを伴う変更には不十分です。米国だけでも、従業員数が 1,000 人を超える企業は 1 万社以上存在し、PQC への円滑な移行には大規模テストが不可欠です。

TeraVM は、数万人の従業員とその拠点（リモート、VPN、オンサイト、マネージドデバイスなど）をエミュレートし、コラボレーションツール、ビデオ会議、プライベートアプリケーションアクセスなど、オフィスのトラフィックをエミュレートすることができます。TeraVM は、実際のトラフィックで従業員数を段階的に増やしながら、レイテンシやスループット、MoS スコアといった KPI を同時に監視できるため、実運用に確信を持てるようになります。

PQC テスト

PQC プロトコルの実装は、ネットワークのパフォーマンスオーバーヘッドを増大させ、エンドユーザのエクスペリエンスに影響を及ぼします。PQC ベースのシステムを含め、暗号システムの開発と導入にはテストが不可欠です。PQC は、量子コンピュータの脅威に対して安全なアルゴリズムを作成することを目的としています。テストは、PQC のいくつかの重要な分野で役立ちます：

- セキュリティ保証
  - セキュリティ耐性テストは、PQC アルゴリズムの暗号攻撃に対する耐性を検証します。このテストは、従来型アルゴリズムや量子アルゴリズムを利用しているアルゴリズムを含め、レジリエンスを評価するための、さまざまなシナリオの下でのアルゴリズムのテストで構成されています。
- パフォーマンス評価
  - 計算効率テストは PQC アルゴリズムの計算効率を評価します。これには、暗号化/復号化速度、鍵生成速度、システム全体のパフォーマンスの測定が含まれます。PQC アルゴリズムの効率を確保することは、実用的なアプリケーションに広く採用する上で極めて重要です。
- 相互運用性テスト
  - 既存システムとの統合：暗号システムは、多くの場合、確立されたインフラやプロトコルとの相互運用を必要とします。PQC アルゴリズムを多様なシステムにシームレスに統合し、互換性の問題を回避することを保証するためには、テストが不可欠です。
- 標準化コンプライアンス
  - 規格準拠：このテストにより、PQC アルゴリズムの確立された暗号規格へのコンプライアンスが確認され、プラットフォーム間の相互運用性と一貫性のある実装が促進されます。

VIAVI はまた、VPN テストで培った長年の経験を活かし、悪意ある攻撃者による「今保存し、後で復号化する」リスクを防ぐことを目的とした PQC アルゴリズムの検証にも対応することができます。それには、以下が含まれます。

- ポスト量子 (PQ) VPN ハイブリッドテスト：ハイブリッドキーを使用した IKEv2 ピアリングのテスト
  - PQ VPN ハイブリッドのレスポンダーではなく、イニシエーターのテスト：両方が PQ VPN キーをサポートしていない場合、従来型の IKEv2 トンネルが確立されるようにします。
  - 不一致の PQC KEM が選択された場合のテスト：イニシエーターとレスポンダー間のネゴシエーションで一致する暗号が見つからない場合、テストは失敗する必要があります。
  - PQ VPN トンネルのストレステスト：2 つの PQC サポートサイト間で長期間にわたって大容量データファイルを転送し、両側でファイル伝送が完了するようにします。
- IPSec VPN PQC アルゴリズムのサポート：
  - NIST 標準の KEM アルゴリズムおよびいくつかのポスト量子アルゴリズムに対応しています。

VIAVI Automation Management and Orchestration System（VAMOS）

VAMOS は、TeraVM セキュリティを含む VIAVI ワイヤレステスト製品のテストキャンペーン、ケース、実行を自動化するクラウドベースの統合プラットフォームです。カスタマイズ可能なワークスペースと構成により、VAMOS はテストワークフロー全体を合理化し、チームやラボの所在地横断的なリソース利用を促進します。

共有ツールのテストベッドと個別のサンドボックスは、幅広いテストニーズに対応し、一方、ロバスト解析とレポート作成機能はテストの精度と信頼性を向上させます。

AI/ML、ラボ・アズ・ア・サービス（LaaS）を統合することで、VAMOS は運用コストを大幅に削減し、手作業を最小限に抑え、障害解析を加速します。その結果、市場投入までの時間が短縮され、品質が向上し、予算を厳しく管理できるようになります。主なメリットは以下の通りです。

運用経費の削減

- インテリジェントオートメーションによる工数削減
- 最適化されたワークフローによる市場投入までの時間の短縮
- 正確で一貫性のあるテストによるサービス品質の向上

ラボの効率と効果の最大化

- ゼロタッチ自動化による End-to-End のテスト実行
- AI/ML の知見を活用した応答時間の短縮とエンジニアリングの専門知識の増大

どこでもテストの実行が可能

- グローバルスケジューリングレイヤーは、ラボ所在地の間でリソースのバランスをとります。
- 場所に依存しない実行によるテストのコスト最適化
- すぐに使えるスケジューリング機能による、ツールにとらわれないオープンな自動化フレームワーク

クラス最高のツール活用の実現

- 高度なツール選択とスリップスルー分析でフィールドレベルの問題の検出
- サイクルの早い段階で真の問題を特定するツールとプロセスを優先順位付け

COTS プラットフォームでのハードウェア/ソフトウェア分離の活用

- 多様なテストシナリオに対応する共有コンピュートリソース
- 使い捨てのオンデマンドサンドボックスにおける動的ソフトウェアツールのプロビジョニング
- 硬直的なアプライアンスに代わる、柔軟なハードウェアプラグインによる純粋なソフトウェアツールの優先

3.3 ハイブリッドシステムのテスト

量子ネットワークにおけるハイブリッドシステムは、QKD、量子中継器、PQC などの量子技術と従来型ネットワークコンポーネントを統合したものです。これらのシステムのテストには、機能性、性能、セキュリティ、環境要因などを含む多角的なアプローチが必要です。

テストベッドでの移行テスト
目標：サービスプロバイダーが必要とする移行シナリオをエミュレートする。

- QKD、PQC、従来型セキュリティ手法の共存シナリオ
- QKD、PQC、従来型セキュリティ手法のフォールバックシナリオ

機能テスト
目標：従来型コンポーネントと量子コンポーネントが、意図したとおりに連携することを確認する。

- 量子-従来型インターフェイステスト：量子信号と従来型システム間のタイミングと同期の検証、QKD 制御プロトコルのテスト
- プロトコルスタックの検証：QKD と IPsec、TLS、または PQC との統合の確認

パフォーマンステスト
目標：スループット、レイテンシ、エラー率、セッション数、セッション確立時間を測定して最適化する。

- 主要メトリックス：量子ビット誤り率（QBER）、セキュアキーレート（bps）、レイテンシとジッター、セッション数、セッション確立時間
- ユースケース：ハイブリッド暗号化シナリオにおける安全な鍵の生成と消費の測定

セキュリティテスト
目標：量子安全暗号とハイブリッド暗号のレジリエンスを検証する。

- PNS、中間者、サイドチャネルなどの攻撃のシミュレーション
- PQC への安全なフォールバックの検証
- 量子乱数生成器（QRNG）のエントロピー品質のテスト

環境および物理レイヤーのテスト
目標：実環境下での堅牢なパフォーマンスを保証する。

- 損失、分散、偏光効果を測定するファイバーテスト
- DWDM における量子トラフィックと従来型トラフィックの共存
- 自由空間光学系（衛星リンクなど）の大気テスト

テストベッドでの統合テスト
目標：実運用のような環境をエミュレートする。

- ライブファイバーリンクとエミュレートされた量子ノードの組み合わせ
- 国内または民間の量子テストベッドでの展開

AIOps と監視の統合
目標：ハイブリッドネットワークの監視と適応に AI/ML を使用する。

- 古典的メトリックスと量子メトリックスの両方のリアルタイム分析
- 改ざんや劣化に対する異常検知の使用
- ハイブリッドリンクの健全性のリアルタイムの可視化およびアラーム表示

テスト分野	従来型コンポーネント	量子コンポーネント	ツール/アプローチ
移行	以下のコンポーネントの組み合わせ	以下のコンポーネントの組み合わせ	以下のコンポーネントの組み合わせ
機能	ネットワークスタック、ルーティング	QKD、QRNG	プロトコルアナライザ、QKD コンソール
パフォーマンス	帯域幅、ジッター	QBER、鍵生成率	ファイバーテスター、NetSquid、QuISP
セキュリティ	ファイアウォール、VPN、PQC	量子攻撃シミュレーション	ペンテスト、サイドチャネルツール
物理レイヤー	DWDM、ファイバー、RF	光子伝送	OTDR、ファイバーセンシング、偏波ツール
統合と監視	オーケストレーション、AIOps	キー使用状態、障害検出	NMS、AIOps ダッシュボード、VIAVI NITRO

以前のセクションで提供した VIAVI テストソリューションを活用することで、移行を含む複数のハイブリッドシナリオをテストすることができます。

4　その他の考慮事項

AIOps

IT 運用のための人工知能（AIOps）は、セキュリティの強化、脅威検出の自動化、データ転送の最適化のために、すでに量子安全環境で適用されています。AIOps は、量子暗号システムやポスト量子暗号システムを支えるインフラをプロアクティブに管理し、セキュリティを確保することで、量子安全保障を強化することができます。AIOps は常に進化していますが、基礎的なレベルで複数の利点があります。

1. 脅威検知と異常対応：量子安全システムは、暗号技術だけでなく、安全で安定した運用にも依存しています。AIOps は、盗聴、ファイバー盗聴、中間者攻撃を示す場合があるデータフローの異常な挙動を検出できます。また、QKD システムのログを分析し、量子ビット誤り率（QBER）の急上昇、予期せぬ信号の減衰、疑わしいデバイスの再認証などの異常を検出することもできます。AIOps は、通常の業務動作に基づいてトレーニングされた機械学習モデルを使用することでこれを行い、異常値を迅速に検出するのに役立ちます。

2. インフラ監視の自動化：多くの場合、量子安全システムには、低レイテンシで安定した環境が必要となります。AIOps は、量子ネットワークやハイブリッドネットワークのレイテンシ、ジッター、パケットロスを監視することで、この維持を支援します。リアルタイムで提供される AI の知見に基づいてルーティングやスイッチングを最適化し、量子鍵交換やポスト量子暗号化プロトコルに影響を与える可能性のある劣化に自動的に対応します。

3. 適応型セキュリティ態勢：量子安全の実装には、ハイブリッドシステム（従来型の暗号＋量子/ポスト量子暗号）が含まれる場合があります。AIOps は、認識された脅威レベルに基づいて暗号化強度や使用プロトコルを動的に調整し、観察されたシステムパフォーマンスとリスクレベルに基づいて量子安全アルゴリズムの展開を推奨します。

4. 暗号ドリフトとコンプライアンス管理: AIOps は従来の非準拠の暗号ライブラリの使用状況を追跡できるため、非量子安全アルゴリズム（RSA や ECC など）の使用を検出してフラグを立て、PQC ライブラリ（CRYSTALS-Kyber、Falcon など）を使用した自動置換を提案することができます。

AIOps には量子安全環境においていくつかの重要な応用があります。中でも重要なのは、ネットワークトラフィックを監視して悪意のある活動を検知し、潜在的な量子時代のサイバー脅威が機密データを侵害する前に対応する、脅威検知と対策です。また、暗号インフラの評価や、ポスト量子暗号規格への移行の自動化（したがって、長期的なセキュリティの確保）にも利用できます。

要約すると、AIOps は、スタック全体で脅威や異常を検出し、QKD や PQC の展開のためにオペレーションの整合性を確保し、自動暗号化調整を含む動的な防御を可能にし、量子安全規格への準拠を監視することで、量子安全システムを強化します。

VIAVI のソリューション：NITRO® AIOps

VIAVI は、マルチベンダー、マルチテクノロジー、マルチドメイン環境をシームレスに統合する包括的ソリューションとして、高度な End-to-End のトップダウンインテリジェントエンジンである NITRO AIOps を提供しています。NITRO AIOps の AI 機能は、NOC の複雑さを簡素化し、オペレーションを合理化するユニークな機会を提供します。NITRO AIOps には、以下のような多くのメリットがあります。

- TCO の削減：AI と予知保全を活用することで、NITRO AIOps はコストのかかるダウンタイムを効果的に低減します。リソース割り当て、キャパシティプランニング、最適化における高度な AIOps 機能は、コスト管理をさらに強化し、最も複雑なシナリオでも持続可能なネットワーク運用を促進します。
- 運用費の削減：NITRO AIOps は、自動化によってネットワーク管理、トラブルシューティング、サービス保証を向上させ、ゼロタッチ運用の可能性を最大限に引き出し、運用効率を高めます。
- デジタルトランスフォーメーション - 5G の収益化：NITRO AIOps は、リアルタイム分析と予知保全によってネットワークのデジタルトランスフォーメーションを可能にし、ユーザーに影響を与える前に問題を特定します。その自己修復機能はパフォーマンスを最適化し、ピーク負荷時でもシームレスなユーザー体験を保証します。

量子ネットワークにおけるファイバーのフィールドテスト

量子ネットワークは、通信に極めて壊れやすい量子状態を利用しているため、量子ネットワークにおいてはファイバーのフィールドテストが極めて重要です。ファイバーインフラにわずかな欠陥や不整合があっても、量子信号が乱れたり、完全に破壊されたりする可能性があります。

ファイバーを介した量子安全ネットワークは物理レイヤーの状態に非常に敏感で、ファイバーが高品質であることに依存しています。フィールドテストにより、ファイバーが安全な量子鍵交換をサポートしていることが保証されます。

ハイブリッドネットワークでは、量子安全の多くの導入先、従来型のデータとともに既存の通信ファイバーが使用されることになります。フィールドテストでは、ファイバーが量子トラフィックと従来型トラフィックの両方を処理できること、ノイズや干渉を受けずに安全に動作すること、ファイバーが量子安全展開要件に準拠していることが検証されます。

ファイバーフィールドテストは、量子鍵伝送のための信号の完全性を保証し、セキュリティに極めて重要な低エラーレートを維持するのに役立ち、量子証明暗号化を危険にさらす可能性のある脆弱性を検出するため、量子安全ネットワーキング（特に QKD）には不可欠です。

VIAVI のソリューション：OneAdvisor 800

VIAVI OneAdvisor 800 は、多種多様な有線および無線ネットワークを維持するために必要な、進化するネットワークテストのニーズを簡素化できるように設計されています。OneAdvisor 800 のモジュール式設計により、ネットワーク作業者は、3 つのカテゴリー（ワイヤレス、トランスポート、ファイバー）に大きく分類される多数のテストシナリオ間で簡単に切り替えることができます。

OneAdvisor 800 は、作業者に機器の使用方法を案内するアシスタントアプリとの直感的なタッチジェスチャー方式のユーザーインターフェースを提供します。幅広いモジュールと性能により、あらゆるネットワークアプリケーションに対応し、高速でエラーのないテストが可能です。また、新しい WDM サービス（CWDM、DWDM、MWDM、LWDM）のターンアップと検証を行い、高速のサービスアクティベーション、OSA プラスイーサネット/BERT テストのための将来要件にも対応できます。統合されたレポート作成により、管理すべきテスト結果の量を 50% 削減できます。

ファイバーテスト機能には、光コネクター検査、OTDR および PON-OTDR、FiberComplete PRO™ 双方向 IL/ORL および OTDR（TruBIDIR）、DWDM OTDR、光スペクトラムテスト、海底ケーブルの認定およびトラブルシューティングのための高度な分散テスト、高速 DWDM 地上トランスポートネットワーク、4G/5G 用無線アクセスネットワーク（バックホール、ミッドホール、フロントホール）、データセンター、データセンターキャンパスおよび相互接続（DCI）テスト、FTTH/PON ネットワークテスト（あらゆる標準、アンバランス/タップまたはインデックストポロジー）、DAA、リモート PHY、C-RAN 用 DWDM アクセスネットワーク、エンタープライズ/LAN などがあります。

トランスポートテストにおいて、OneAdvisor 800 にはいくつかの利点があります。

- **便利なポータブル型。**入手可能な最小の 400G/800G テストデバイスの 1 つ
- **比類のない冷却性能。**400G/800G ポータブル型でクラス最高 – ZR プラガブルを容易に冷却可能
- **優れたバッテリー寿命。**複数のバッテリーに拡張可能で、電源接続なしでも数時間使用可能
- **幅広いテストカバレッジ。**モジュール方式により、回線レートとプロトコル全体にわたってオールインワンのソリューションを提供
- **柔軟性。**光ファイバー信号テスト（OTDR、OSA）およびイーサネットレート（800、400、200、100、50、40、25、10、1）テストを提供
- **複数の光トランシーバーに対応。**QSFP-DD800/QSFP-DD/QSFPx、OSFP800/OSFP、SFP-DD/SFPx に対応、コヒーレント光トランシーバーに完全に対応

VIAVI のソリューション：INX™ 760

INX 760 はフィールド作業者にとって究極のツールであり、汚れのないファイバー接続を確保する上で比類のない効率を提供してくれます。25 年以上にわたる先駆的なイノベーションと専門知識の集大成として、次世代のファイバー端面検査と解析の頂点となるものです。端面検査は、多くのフィールド作業者にとって標準的な作業となっていますが、汚染は依然として光ネットワークの問題の最大の原因となっています。新しいコネクタータイプの出現、フィールドで使用されるコネクターの量の増加、新しいファイバー作業者の増加により、業界はすでに変曲点を迎えています。

光セキュリティとパフォーマンス

本稿では量子ネットワークの課題と関連する VIAVI テストソリューションの概要を紹介しましたが、VIAVI はまた、量子ネットワーク用のスペクトラムセンシングフィルターや光センサーフィルターなど、業界トップの独自の光コーティングも提供しています。1948 年に Optical Coating Laboratory（OCLI）として設立された VIAVI の光セキュリティおよびパフォーマンス（OSP）事業は、75 年にわたってカスタムおプティクスのイノベーションリーダーであり続けています。高性能オプティクスの進歩における信頼できるアドバイザーおよび長期的なパートナーとして、当社はプレミアムソリューションと比類のないカスタマーサービス体験をお届けしています。VIAVI は、エンジニアリング、研究、応用知識において強力なルーツを持ち、単純なものから複雑なものまで、光学に関する課題に対応する上で、VIAVI に勝るサプライヤーはありません。プロトタイプから生産に至るまで、当社の専門知識、技術、プロセスはお客様に競争上の優位性をもたらします。

OSP フィルターテクノロジーは、必要とされるあらゆるスケールで、光信号を可能な限り低い干渉と最高の忠実度で抽出できるように支援し、利用可能な最高精度で設計された構造を実現します。

5　まとめ

量子コンピューティングの進歩に伴い、従来の暗号化手法は脆弱性を増しています。これに対処するため、VIAVI は PQC の実装を評価するための先駆的なクラウド対応プラットフォームである TeraVM セキュリティテストを開発しました。このソリューションは、米国 NIST によって義務付けられているアルゴリズムに対応し、耐量子セキュリティフレームワークに移行するのを支援します。さらに VIAVI は、量子チャネル評価用の MAP-300、ファイバー監視とセンシング用の ONMSi と FTH-DTSS、ファイバーネットワーク敷設、トラブルシューティング、メンテナンス用のあらゆるフィールドテスターを提供しています。

〒163-1107
東京都新宿区西新宿6-22-1
新宿スクエアタワー7F

電 話：03-5339-6886
FAX: 03-5339-6889
Email: support.japan@viavisolutions.com

futureproofcomms-quantum-an-xpf-nse-ja
30194555 900 0825

viavisolutions.jp