VIAVI Solutions

UNSTOPPABLE
SCALE UP. SCALE OUT.

MPLS Japan 2026 発表資料

耐量子暗号(PQC)と量子鍵配送(QKD)の適用に求められるネットワークアーキテクチャを知ろう

26 Oct, 2026

VIAVIソリューションズ株式会社
Akihiro NAKAMURA
HSE & Security Sales Manager, Japan
Akihiro.Nakamura@viavisolutions.com

Outline

- 自己紹介
- 量子コンピューティングが暗号と通信に及ぼす脅威
- QKDとPQCの比較
- QKDとPQCのハイブリッドネットワーク
- PQC Test Results
- VIAVI QST1000のご紹介
- QST Hub
- まとめ

©2026 VIAVI Solutions Inc.

自己紹介

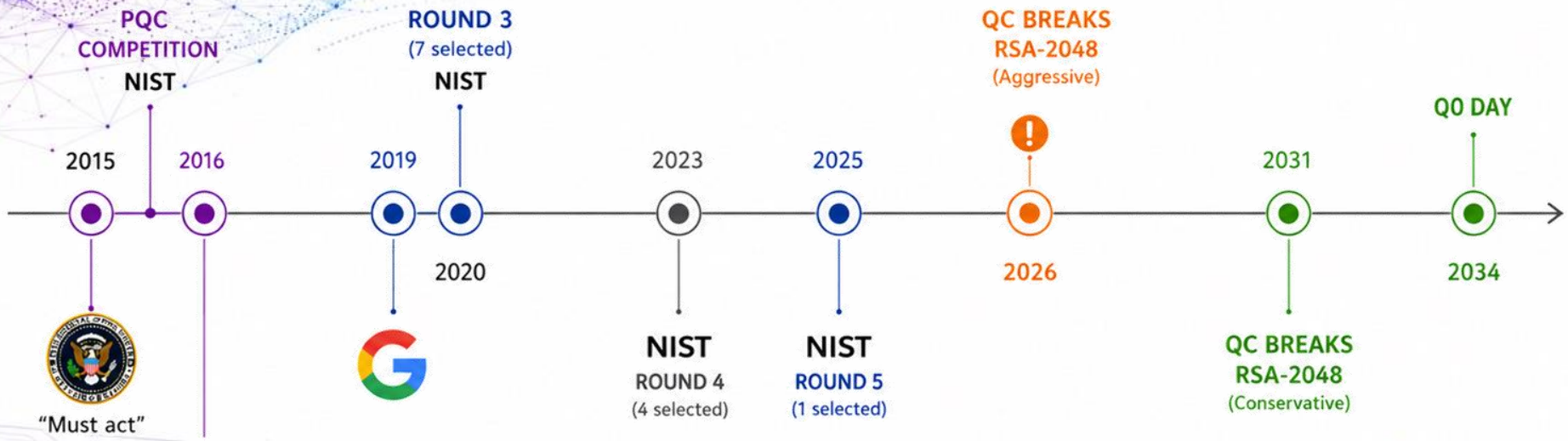


- 2001年3月　大学卒業
- 2001年4月　測定器専門商社
- 2017年4月　Spirent Japan
- 2025年10月~　現職

- 新製品の立ち上げや市場開拓、コミュニティ・学会にも積極的に参加
- 好きなスポーツ：野球（審判）、ゴルフ
- MPLS Japan 2010ごろ？から参加中
  - MPLS Japan 2024　Testing AI Datacenter Fabric

©2026 VIAVI Solutions Inc.

The Quantum Computing Threat to Cryptography and Communications



NATIONAL SECURITY THREAT | RSA VULNERABILITY | GAME OVER

2015–2016
NIST launches PQC competition.
"Must act."

2019–2020
Round 3 (7 selected)
PQC finalists announced.

2023
Round 4
(4 selected)

2025
Round 5
(1 selected)

2026
QC breaks RSA-2048
(Aggressive scenario)

2031
QC breaks RSA-2048
(Conservative scenario)

2034
QO Day
(Game Over)

© 2026 VIAVI Solutions Inc.

QUANTUM SAFETY:
COMPARISON AND KEY SCOPE

	QKD — QUANTUM KEY DISTRIBUTION	PQC — POST-QUANTUM CRYPTOGRAPHY
Equipment	Dedicated optical fiber + specialized transceiver hardware	Software replacement — runs on existing infrastructure, no new hardware needed
Security Pros	**Quantum-mechanical security** — eavesdropping is physically impossible	**Computational security** — easy software upgrade, massively scalable
Cons	Limited to **~100km** and point-to-point; slow key rate; satellite QKD needed for longer reach	**Not 100% provably secure;** performance overhead; needs migration
Standardization	ITU-T Y.3800 / X.1700 series • ETSI ISG QKD	IETF • NIST • GSMA
Use Cases	National security • government agencies • dedicated high-value links	Massive communications — internet banking • enterprise • telecom core

Key Insight: Both technologies have pros and cons — **hybrid QKD + PQC** co-existence validation (functional • migration • scalability) is the key to commercialization.

© 2026 VIAVI Solutions Inc.

QKDとPQCの比較

	QKD	PQC
NWアーキテクチャ	専用の光ファイバーNW or 波長、衛星	既存のIPNW
違い	OTNsec, MACsec, IPsecで使う**安全な秘密鍵を生成・配送するための量子通信**	従来の公開鍵暗号に代わる**次世代の数理暗号**であり、量子力学の性質（量子暗号）を使うわけではない
誰が使うのか？	金融、政府・防衛、ゲノムデータ etc.	広く全般（デフォルトになる想定）
導入ハードル	++++	+
導入コスト	+++	+
安全性	+++++	++++（従来と比べて）
導入時の懸念事項	距離制限とポイントツーポイントによるスケーラビリティ制限	パフォーマンス（従来と比べて）
事前検証例	伝送路の光特性、信号の耐性評価	RSA vs PQC
	鍵生成速度、相互運用性評価	End-to-Endのパフォーマンス検証、相互運用性評価

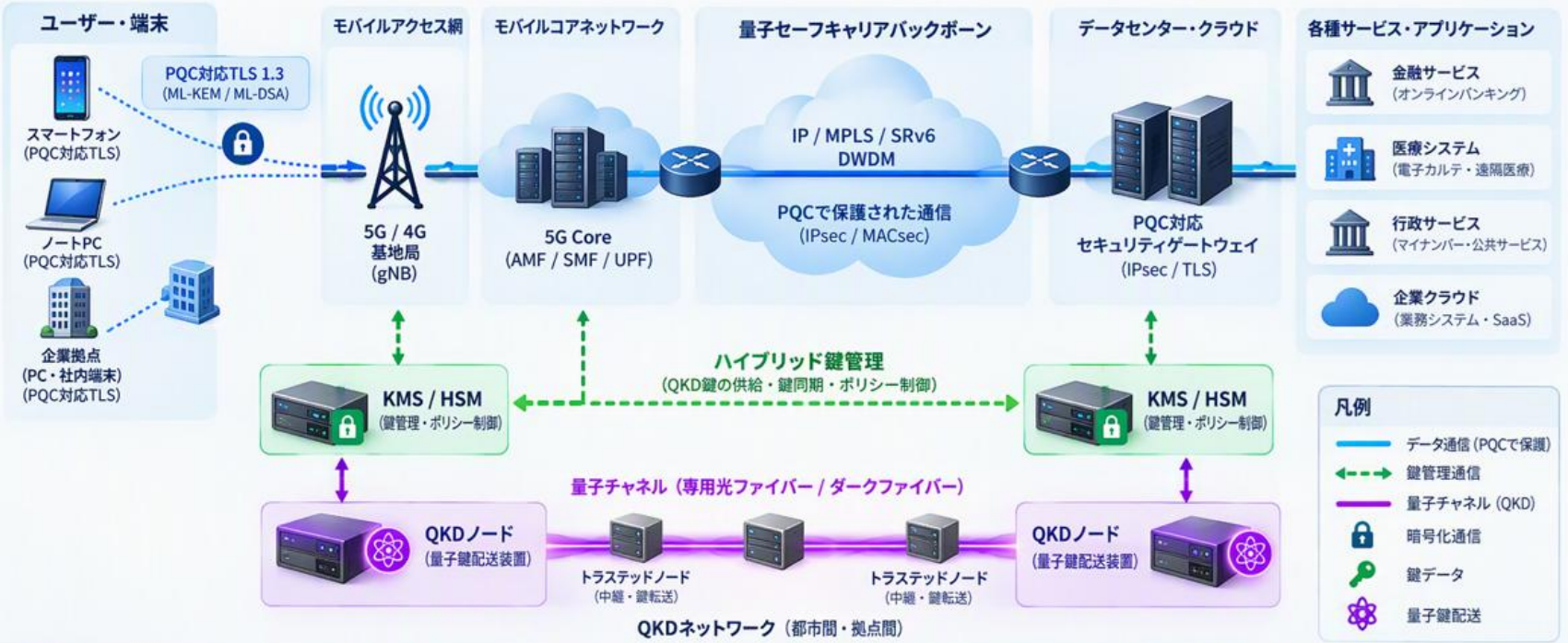
それぞれの特長を活かしたハイブリッドネットワークが推奨される

©2026 VIAVI Solutions Inc.

QKD + PQC ハイブリッドによるエンドツーエンド量子セーフモバイルネットワーク

スマートフォンからクラウドまで、量子時代に備えた安全な通信基盤

画像生成：
Microsoft Copilot



1. ユーザー通信の保護

- スマートフォン / PC は PQC対応TLS 1.3 を利用（ML-KEM / ML-DSA など）
- 既存のアプリやサービスを安全に利用可能

2. キャリア網の強化

- モバイルコアからバックボーンまで PQC対応のIPsec / MACsec
- QKDで生成した鍵とPQCの鍵を組み合わせたハイブリッド鍵管理

3. QKDによる鍵供給

- 専用光ファイバー網で量子鍵を配送
- トラステッドノードで広域接続
- 鍵はKMS/HSMで統合管理

4. 安全で持続可能な社会へ

- 金融・医療・行政・企業など あらゆるサービスを量子時代でも安全に
- モバイルからクラウドまで シームレスな量子セーフ通信を実現

UNSTOPPABLE

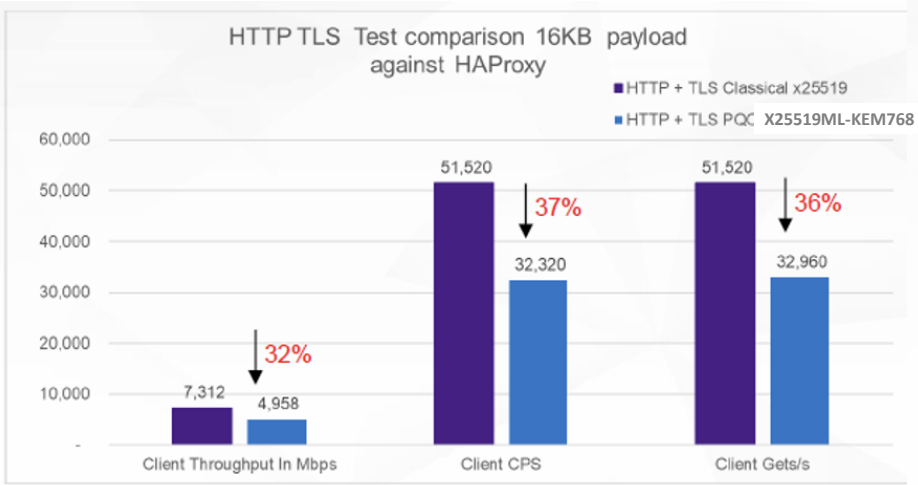
SCALE UP. **SCALE OUT.**

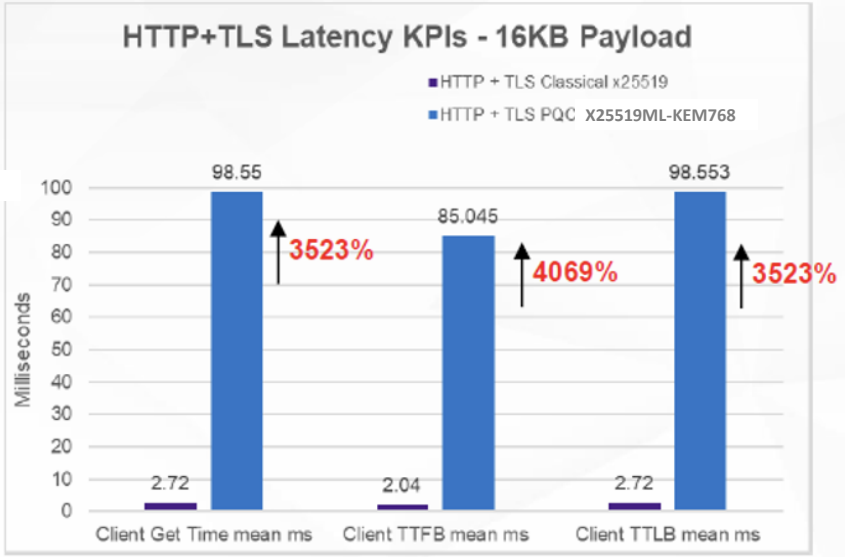


Comprehensive testing leads to a secure network.

PQC Test Results

TLS PQC Performance & Latency Impacts



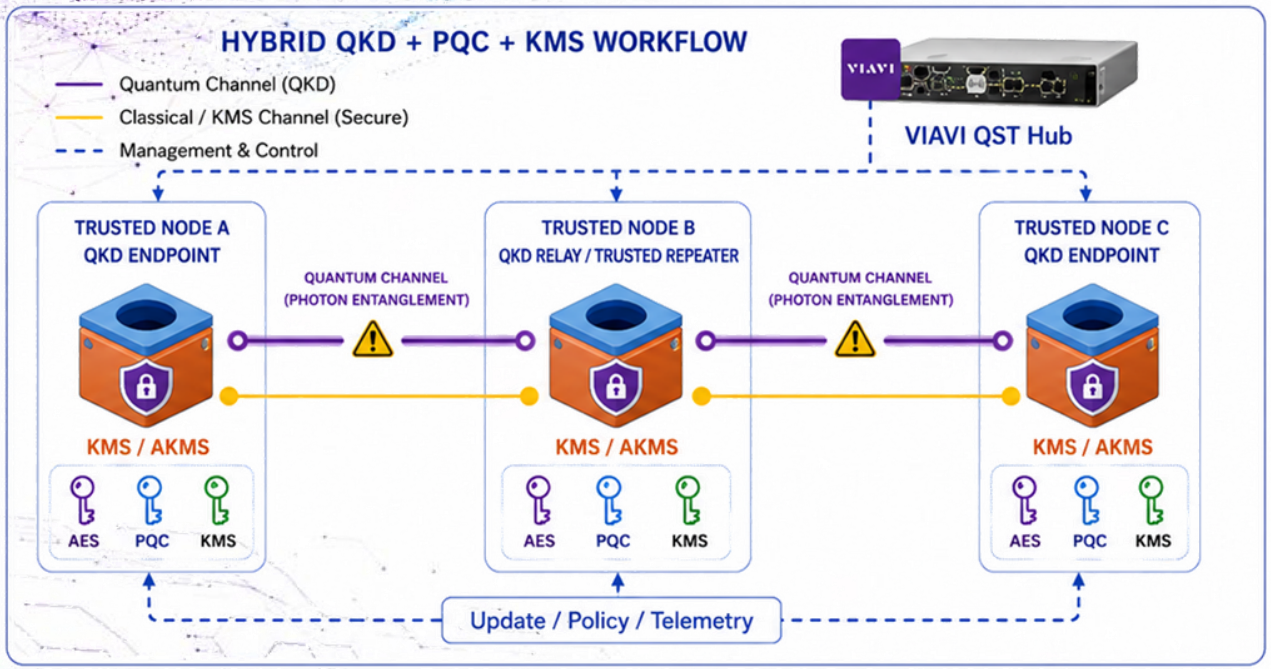


App	Metric	Impact	Business Implication
TLS/HTTPS PQC	Connection Rate CPS	-37%	Need 59% more HW capacity
TLS/HTTPS PQC	Time to First Byte	+4,069%(42x)	User experience: 2ms to 85ms
IKEv2 VPN PQC	Tunnel Establishment Rate	-75%	Need 4x more VPN concentrator capacity

©2026 VIAVI Solutions Inc.

QST1000: Hybrid QKD, PQC, & KMS Deployment

Unified AI-based End-to-End Quantum-Safe Validation, Testing, and Certification



END-TO-END QUANTUM-SAFE WORKFLOW
Validation: key generation → distribution → management → consumption. Validates hybrid architectures combining PQC, QKD, and classical cryptography.

PATENTED HYBRID KEY INTEGRATION TESTING
Ensures seamless fallback, key-mixing, and hybrid-KDF operational behavior.

MULTI-VENDOR, MULTI-PROTOCOL INTEROPERABILITY
Supports all leading PQC candidates (NIST Round 3), QKD vendor APIs, KMS/AKMS protocols.

REALISTIC NETWORK EMULATION & IMPAIRMENTS
Model real-world conditions: loss, latency, jitter, decoherence, noise and failures.

AUTOMATED COMPLIANCE & SECURITY STRESS TESTING & BENCHMARKING
Continuous testing for performance, resilience, and compliance with NIST, ETSI, and industry best practices.

- Hybrid Security QKD + PQC + KMS Protection
- Seamless Fallback & Key Mixing Assurance
- Broad Interoperability Across Vendors & Protocols
- Real-World Validation with Impairments & Emulation
- Automation & Operational Efficiency
- Compliance & Certification Readiness

© 2026 VIAVI Solutions Inc.

QST1000: AI-powered Quantum Safe Test Suite

VIAVI QST1000



- AI-powered natural language interface
- AI-powered orchestration & multi-layer hybrid test
- AI-powered test scenario creation & analysis
- New test scenarios (e.g., HSM: Hardware Security Modules, Smartcard)

CyberFlood/TeraVM



Cyber attack with real application

PQC/Classical performance

TeraVM



KMS (Key Management System)

MAP-300



Photonics Test & Measurement

QKD/KMS/PQC architecture in ITU-T

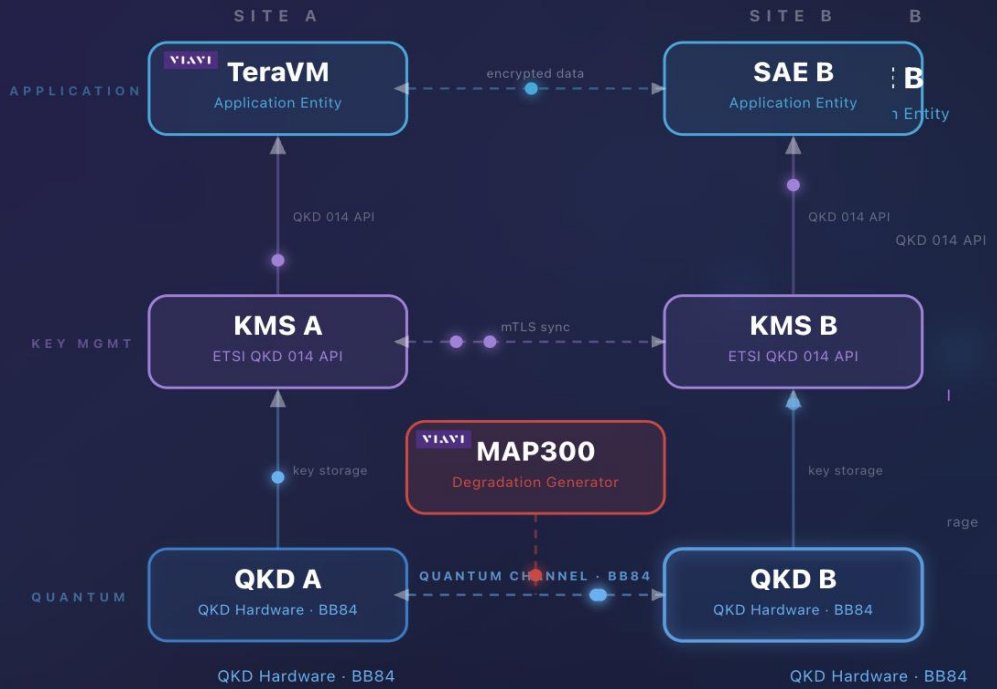


©2026 VIAVI Solutions Inc.

QKD Degradation vs IPSec Performance

Test configuration, architecture, and reports for the QKD Degradation vs IPSec Performance test scenario within Hybrid Tests.

ARCHITECTURE



CONFIGURATION

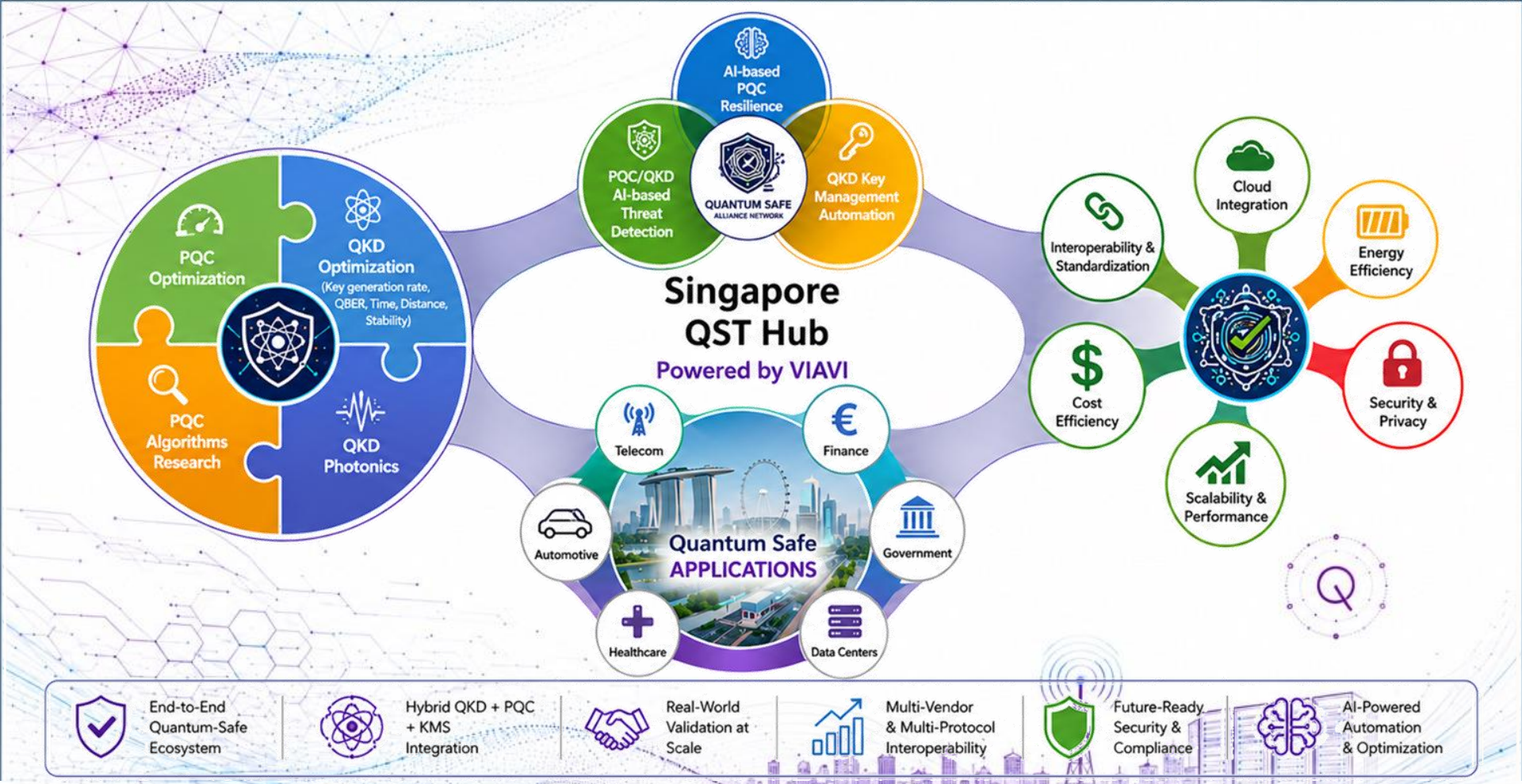
QKD Physical Layer	KMS Configuration	IPSec / IKEv2	PQC Layer	Test Parameters
6 PARAMETERS · VIEW ▸	5 PARAMETERS · VIEW ▸	8 PARAMETERS · VIEW ▸	5 PARAMETERS · VIEW ▸	3 TEST CASES · VIEW ▸

QKD Test by MAP300

QKD Network Link Performance & Channel Quality — QBER, Frequency Stability, Secret Key Rate

TC#01	TC#02	TC#03	TC#04	TC#05
Multi-Path Interference (MPI)	**Signal Power Conditions**	**Polarization State Effects**	**Quantum Source Power Monitoring**	**Light Injection & DoS Attacks**
DWDM noise injection via WSS to measure QBER degradation and Secret Key Rate under classical channel interference	Variable attenuation to emulate fiber span loss and power disruption scenarios	Manual and random ΔSOP emulation to test QKD system tolerance to fiber vibration and lightning-strike events	Highly sensitive detection with OPMSCOPE to log quantum light source power trends and characterize mode behavior	Tunable laser seeding attacks and optical pumping to emulate eavesdropper scenarios and evaluate QKD resilience

©2026 VIAVI Solutions Inc.



© 2026 VIAVI Solutions Inc.

VALOR: USA Quantum-Safe 6G Lab & QST Hub

Full Quantum-Safe Testing Hub for 6G Wireless Communications & Applications

VALOR™

PHOENIX, ARIZONA, USA

Advancing a Quantum-Safe Future for America

FUNDED BY

NTIA

National Telecommunications & Information Administration
U.S. Department of Commerce



FULL QUANTUM-SAFE TESTING HUB (QST HUB)

AI-BASED PQC RESILIENCE
AI/ML for network detection, resilience and autonomous optimization

PQC / QKD THREAT DETECTION
Real-time monitoring and quantum threats across 6G layers

PQC OPTIMIZATION & ALGORITHMS
PQC, QKD & PQ KMS optimization for 6G performance

QUANTUM SAFE 6G NETWORKS
Secure. Resilient. Future-Ready.
6G

QKD KEY MANAGEMENT AUTOMATION
Automated, scalable and policy-driven quantum-safe key management

INTEROPERABILITY & STANDARDIZATION
Multi-vendor, multi-protocol interoperability and compliance (NIST, 3GPP, ETSI)

REALISTIC 6G NETWORK EMULATION
AI-driven emulation of 6G RAN, core, edge and backhaul networks

TEST • VALIDATE • ASSURE

- Security Assurance
- Performance Benchmarking
- Compliance Certification
- Operational Readiness

QUANTUM-SAFE 6G APPLICATIONS & INDUSTRIES

- Robotics & Autonomous Systems
- Finance & Banking
- Defense & Government
- Critical Infrastructure
- Ports & Logistics
- Energy & Utilities
- Data Centers & Cloud
- Telecommunications & 6G Operators
- Smart Cities & IoT

END-TO-END QUANTUM-SAFE 6G CAPABILITIES

Research & Innovation → Simulation & Modeling → Testing & Validation → Interoperability & Integration → Deployment Readiness → Continuous Assurance & Monitoring

OUR MISSION

Build, test and validate quantum-safe 6G technologies and ecosystems that secure America's communications, industries and future.



- End-to-End Quantum-Safe Ecosystem
- Hybrid QKD + PQC + KMS Integration
- Real-World Validation at Scale
- Multi-Vendor & Multi-Protocol Interoperability
- Future-Ready Security & Compliance
- AI-Powered Automation & Optimization

VIAVI © 2026 VIAVI Solutions Inc.

まとめ

- 最低限、PQCへ移行しましょう！
- QKDとPQCの特徴を活かしたハイブリッドな量子セーフネットワークがデータをより安全に守る。
- 新しい技術、取り組みは十分な事前検証により安心して導入できる。

©2026 VIAVI Solutions Inc.

VIAVI Solutions



viavisolutions.com