MPLS JAPAN 2026

PQC対応はなぜ必要なのか。

PQCに関する取り組みと対応方針について

Kazuhiro Kureishi
Solutions Engineer, Lead – Architecture and Solutions
Office of the CTO,
Cisco Systems G.K.

October 26, 2026

基盤となるセキュリティの上に構築される “Resilient infrastructure”



安全な利用、シンプルに（ベースラインのセキュリティ確保）

導入直後から適用されるセキュリティ設定と、リスクを未然に防ぐアラート機能

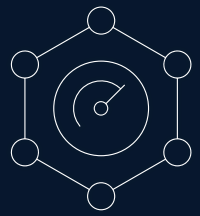
セキュリティ上の問題があるプロトコルを非推奨とし、その後廃止する



リアルタイム脅威対応（IDR：インフラストラクチャ向けのランタイム保護）

業務に支障をきたすことなく、脆弱性に対する即時の防御を実現

Live Protectは、ゼロデイ脆弱性に対して「シールド」を展開します



未来を見据えたレジリエンス (PQC)

転送中のデータおよびデバイスの完全性を確保するための耐量子計算機暗号(PQC)

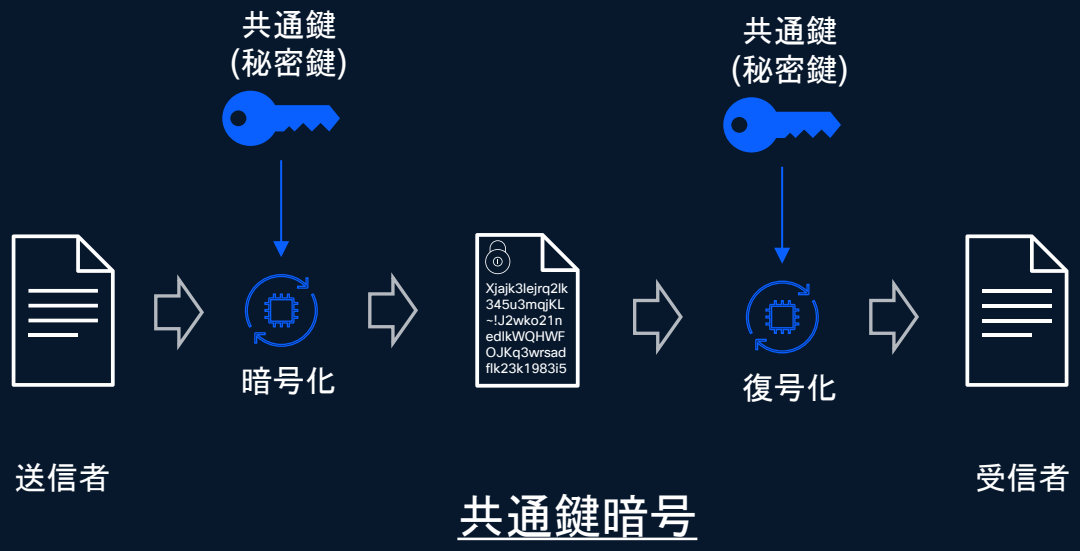
サポート対象のプラットフォーム全体にわたる通信と信頼の連鎖を保護します

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

共通鍵暗号と公開鍵暗号とは
(おさらい)

共通鍵暗号 / 公開鍵暗号 / ハイブリッド暗号

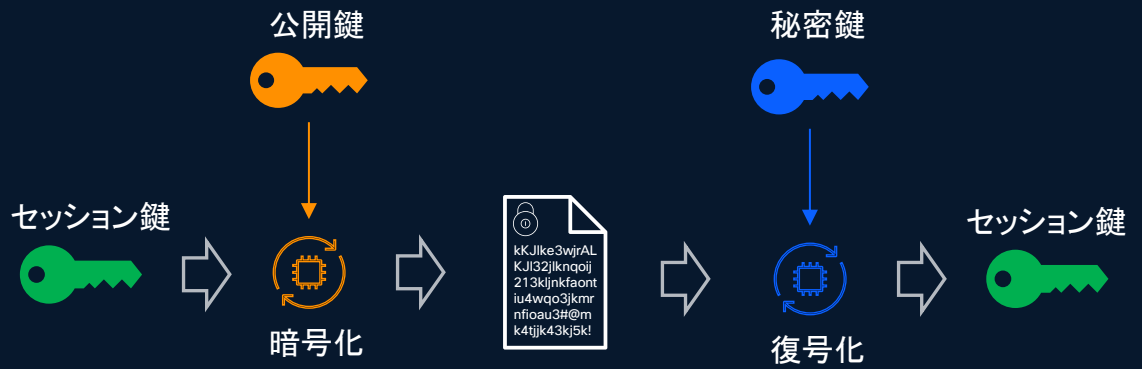


共通鍵暗号

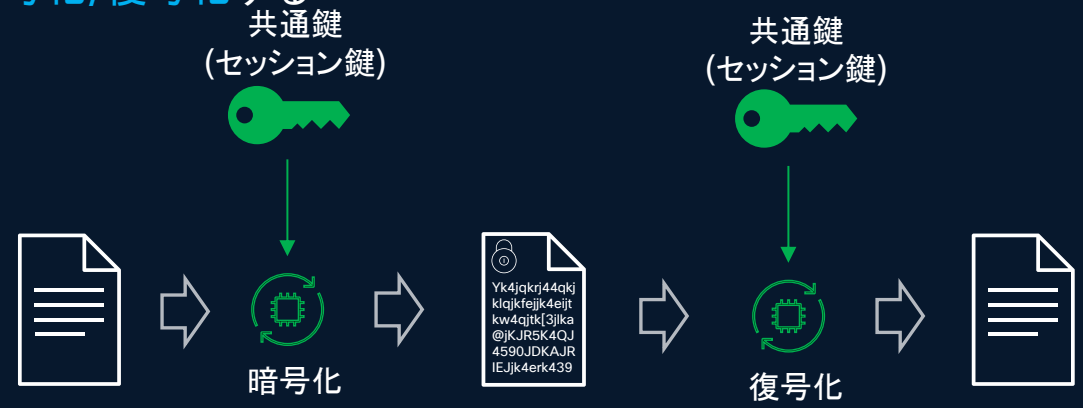


公開鍵暗号

①実トラフィックの暗号化/復号化で用いる共通鍵(セッション鍵)を公開鍵暗号で共有する



②共通鍵(セッション鍵)を用いて実トラフィックを共通鍵暗号で暗号化/復号化する



ハイブリッド暗号

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

※CRQC (Cryptographically Relevant Quantum Computer) とは、既存の公開鍵暗号を解読できる実用的な量子コンピュータ

共通鍵暗号 / 公開鍵暗号 / ハイブリッド暗号



共通鍵暗号

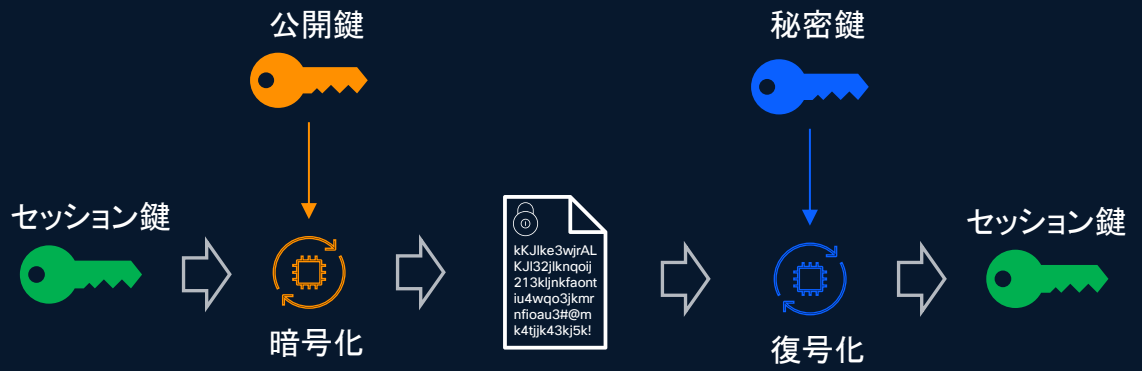


公開鍵暗号

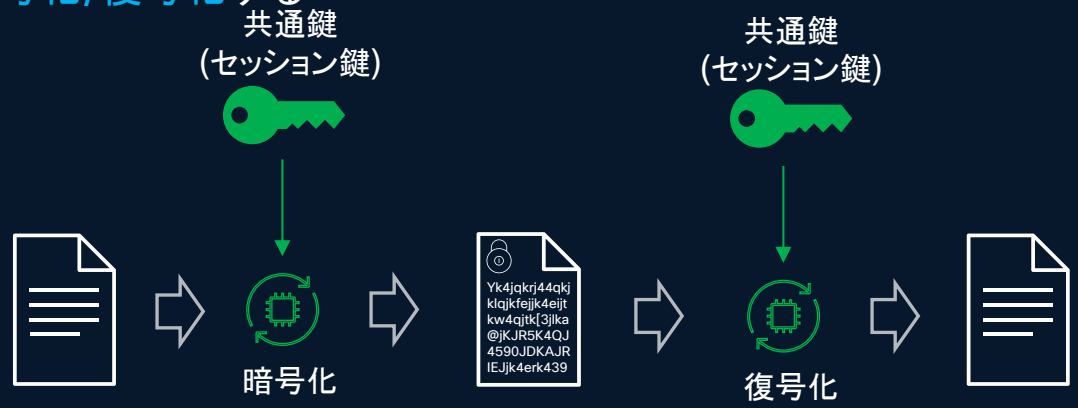
CRQCによって危殆化

CRQCによって危殆化

①実トラフィックの暗号化/復号化で用いる共通鍵(セッション鍵)を公開鍵暗号で共有する



②共通鍵(セッション鍵)を用いて実トラフィックを共通鍵暗号で暗号化/復号化する



ハイブリッド暗号

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

量子コンピュータの発展に伴う従来暗号の危殆化とPQC対応

PQC(耐量子計算機暗号)とは何か

Post Quantum Cryptography(PQC: 耐量子計算機暗号)



量子コンピュータの計算能力向上に耐え得る、
従来のコンピュータやネットワークの仕組みで動く暗号

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

なぜPQCが必要なのか

量子コンピュータは既存のコンピュータと同様に万能ではない

しかし、主に電子署名等で利用されている公開鍵暗号(RSA/DSA等)が量子コンピュータとShorのアルゴリズムを活用することで効率的に解くことが可能であると証明されている



つまり、量子コンピュータで計算規模と安定性が向上することで、
既存の非対称鍵暗号が脆弱になる(Q-dayを迎える)
＝ PQC対応が必要となる

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

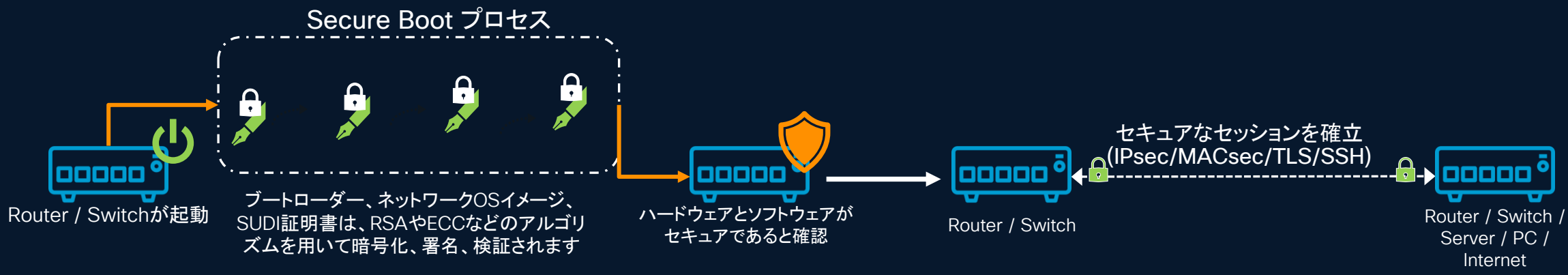
暗号化の種別と量子耐性

項目	公開鍵暗号（非対称鍵暗号）	共通鍵暗号（対称鍵暗号）
概要	公開鍵と秘密鍵のペアを使用。 鍵配送問題を解決。	同一の共通鍵を使用。鍵配送が課題。
IPsecでの役割	IKEv2： RSA/ECDSA 認証、DH/ECDH による鍵交換	IKEv2：PSK 認証 ESP：AESなどでデータ暗号化
計算の複雑さ	高い（複雑な数学計算、長い鍵長が必要）	低い（高速・ハードウェア最適化可能）
鍵の管理	秘密鍵のみ厳重管理、公開鍵は自由に共有可能	双方で同一鍵を安全に共有・保管する必要
主な用途	鍵交換、認証、署名、少量データ暗号化	大量データ暗号化、セッション暗号化
IPsecでの具体例	IKEv2フェーズ1：DH/ECDH、証明書認証	ESP：AES-GCM/CBC によるペイロード暗号化
PQC（量子耐性）	**危殆化**:ShorでRSA/ECDH/ECDSAが破壊	比較的安全: Groverで強度半減のみ （AES-256推奨）
NIST PQCでの扱い	**PQCへ移行が必要**	**継続利用可（AES-GCM 256推奨）**
主な実装	RSA (512,1024,2048bit), ElGamal, 楕円曲線	RC4, DES, 3DES, AES

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

現代のネットワークにおける暗号技術
ハードウェアからソフトウェアへ



セキュリティ機能	暗号	利用方法
ネットワークOSイメージおよびブートローダーイメージの署名/検証	**デジタル署名（公開鍵暗号を使用）**	システムソフトウェアの真正性と完全性を起動前に保証します
SUDI Certificates / TLS Certificates / Root CA Certificates	**デジタル証明書（デジタル署名と公開鍵暗号を使用）**	デバイス識別と認証を提供し、信頼チェーン（PKI）を有効化する
安全なトランスポートセッション/鍵交換	**公開鍵暗号& 共通鍵暗号**	**鍵交換のための公開鍵暗号、そして大量データのための共通鍵暗号**

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

ご参考: CRQCの台頭がもたらす2つの脅威と対応方法

脅威	緊急度：極めて高い Harvest Now, Decrypt Later (HNDL)	緊急度：高い Trust Now, Forge Later (TNFL)
攻撃手法	現在の通信内容を記録し、将来CRQCを使用して公開鍵から秘密鍵を生成する事で過去の記録内容を復号化する	将来的には、CRQCを利用して鍵を生成し、過去の署名等を偽造することが可能になる
何が脅威なのか	「機密性」が損なわれる + 今時点から情報が収集されている	「完全性」、「真正性」が損なわれる
対応方法	PQC対応のアルゴリズム、および、プロトコルへ移行する あるいは、PPK、サードパーティの鍵交換メカニズム、またはQKDを実装する	デジタル署名アルゴリズム、および、プロトコルをPQC対応のものに移行する

HNDL:
過去の通信記録に含まれる公開鍵を取り出して利用する

TNFL:
デジタル署名に紐づく公開鍵を利用する



HNDL:
生成された秘密鍵を利用して過去の通信内容の記録を復号化

TNFL:
生成された秘密鍵を利用してデジタル署名を偽装

※ CRQC（Cryptographically Relevant Quantum Computer）とは、既存の公開鍵暗号システムを破ることができる実用的な量子コンピュータ

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

なぜ今のタイミングでPQCなのか

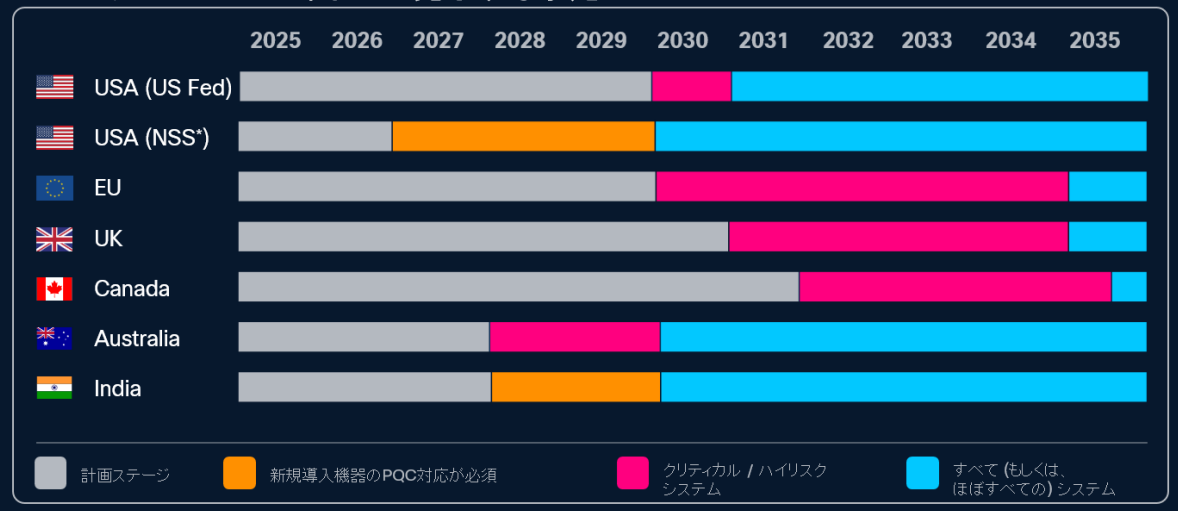
PQCの対応にはHW/SWのライフサイクルに沿った対応が
必要となるため、時間がかかる

“Harvest Now, Decrypt Later (HNDL)”への対応

各国のPQC対応が進む中で、日本もPQC関連の対応指針が
政府から示されるタイミングとなっている(2025年11月～2026年にかけて)

規制当局によるPQC移行のスケジュール

移行は段階的に計画、「高リスク」システムは早ければ2026年、
全システムは 2035 年までに完了する予定

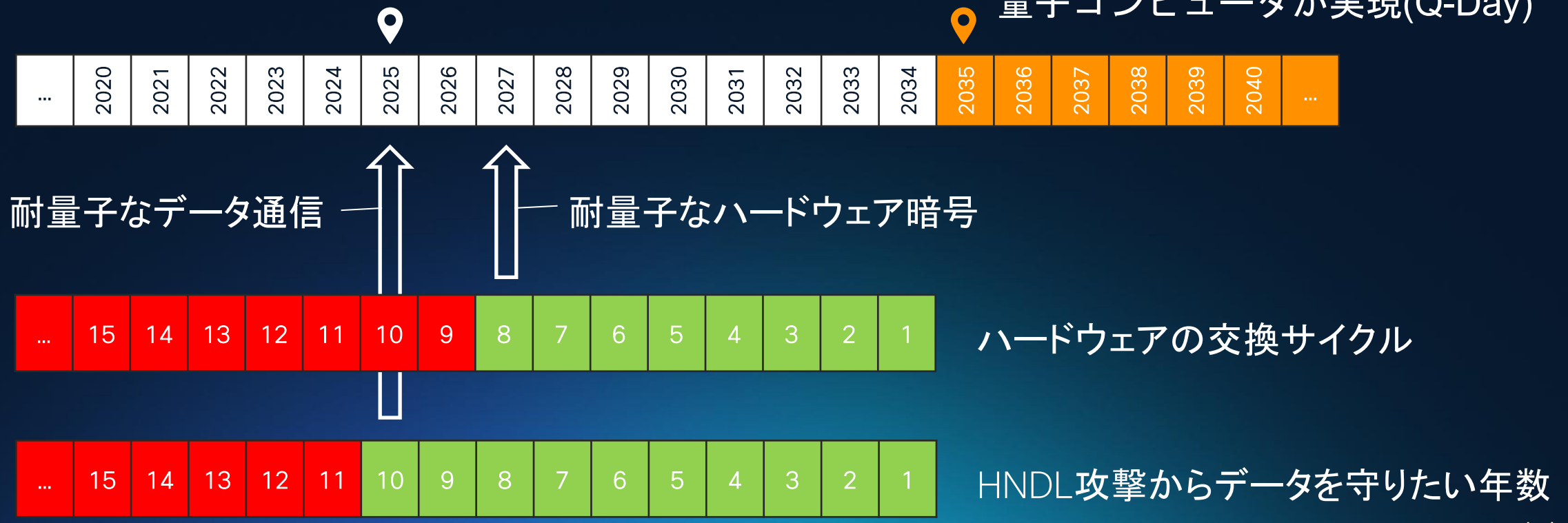


© 2026 Cisco and/or its affiliates. All rights reserved.

© 2026 Cisco and/or its affiliates. All rights reserved.

なぜ今からPQCへの移行を検討するべきなのか？

- ハードウェアの交換サイクル
- Harvest Now, Decrypt Later (HNDL) 攻撃



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

PQC関連の動向について

政府は公共部門、国家安全保障、重要インフラ向けにPQC移行のタイムラインを設定



2030年までに全ての国家安全保障システム (NSS) に対して

2030年までに義務付け

(新規調達システム：

2027年1月1日以降必須)



重要インフラに対して

2030年までに適用義務付け



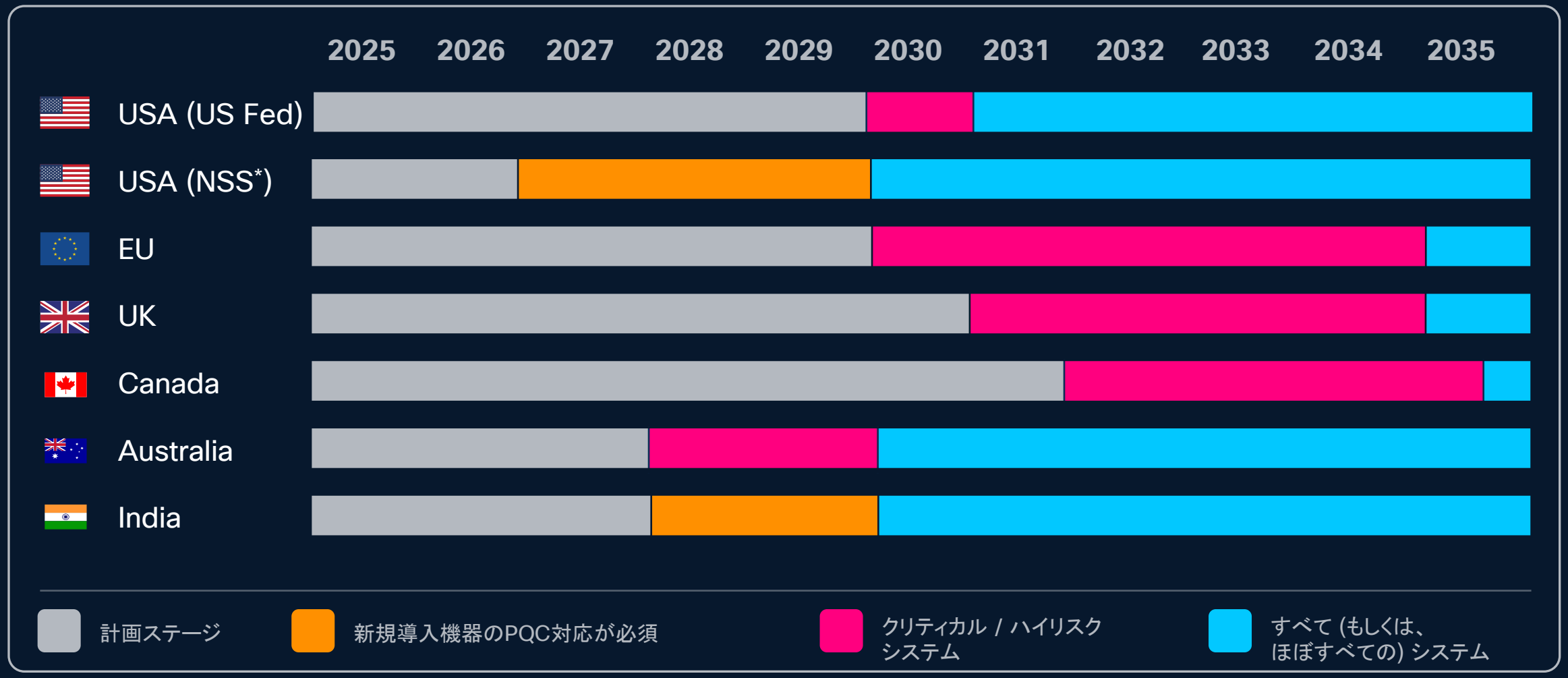
2026年以降
公共部門契約に組み込まれる

2030年までに義務付け

© 2026 Cisco and/or its affiliates. All rights reserved.

規制当局によるPQC移行のスケジュール

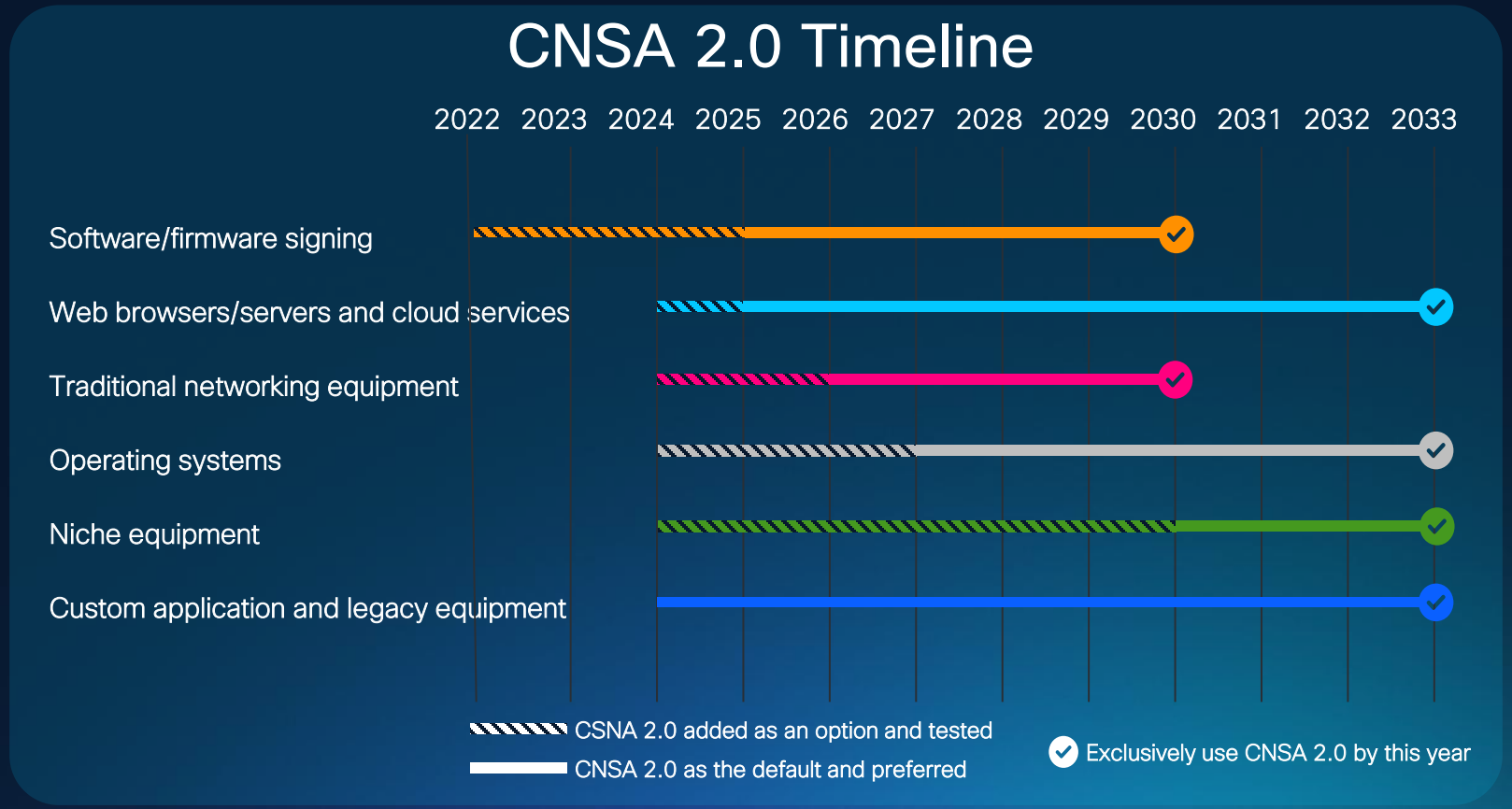
移行は段階的に計画、「高リスク」システムは早ければ2026年、全システムは 2035 年までに完了する予定



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

CiscoのPQC対応: 原則としてCNSA 2.0に準拠



PQC対応に関して署名およびクラウドサービスは、**2025** 年までに「デフォルトかつ推奨」となり、**2030**年までに義務化

–CNSA 2.0[1,2]

“2027年1月1日以降、US NSS向けの新規取得品は、特に記載がない限り、CNSA 2.0準拠であることが義務付けられる" [3]

–US NSA

1. Commercial National Security Algorithm Suite 2.0;
2. 2. Commercial Solutions for Classified program;
3. 3. US National Security Agency’s Committee on National Security Systems

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

Quantum Safety （耐量子安全性）のこの議論に関わるコア用語



Quantum-Safe

量子における脅威に対するセキュリティを提供するあらゆる手法。これにはシステムや実装が含まれる可能性がある。



Post-Quantum Cryptography (PQC) 耐量子計算機暗号

量子コンピューティングの将来の時代を見据えた公開鍵暗号アルゴリズム。**NIST**標準アルゴリズム（**FIPS 203, 204, 205**）がここに位置づけられる。**QKD**（量子鍵配送）は該当しない。



Hybrid (PQ/T)

Post-Quantum/Traditional (PQ/T) とは、従来の暗号アルゴリズム（**Diffie-Hellman**など）と**PQC**（耐量子計算機暗号）アルゴリズム（**ML-KEM**など）を組み合わせた手法を指す。両手法は並行して動作し、その出力が統合される。



Crypto Agility

クリプト・アジリティ（暗号化の俊敏性）とは、セキュリティと継続的な運用を維持しつつ、プロトコル、アプリケーション、ソフトウェア、ハードウェア、ファームウェア、インフラストラクチャにおける暗号アルゴリズムの置換と適応に必要な能力を指す。

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

標準化団体は、PQC（耐量子計算機暗号）アルゴリズム、実装、および統合に関する世界的な整合性を推進

NIST

National Institute of Standards and Technology （アメリカ合衆国）

2016年にPQアルゴリズムの定義を開始

Working Group (WG) にはアカデミア、および産業界の代表者が参加している

NISTアルゴリズムは地域を問わず一般的に受け入れられている

IETF

Internet Engineering Task Force

インターネットプロトコルの定義を担うグローバルコミュニティ

積極的に**NIST**アルゴリズムをセキュリティプロトコルへ変換

Others

ITU, 3GPP, WIFI Alliance, Trusted Computing Group, PKI Consortium, ETSI

（主に）**NIST**アルゴリズムの適応

© 2026 Cisco and/or its affiliates. All rights reserved.

NIST の PQCアルゴリズム(FIPS-203, 204, 205等)は、安全な通信、認証、およびシステムの信頼性の基盤を提供

ML-KEM (FIPS 203)	HQC (Draft)	ML-DSA (FIPS 204)	SLH-DSA (FIPS 205)	FN-DSA (FIPS 206) Draft	LMS/XMSS (NIST SP 800-208)
• Based on CRYSTALS-Kyber • Lattice-based • Secures the exchange of keys over untrusted medium	• Serves as a backup for ML-KEM to diversify outside lattices • Code-based (decoding random linear codes problem)	• Based on CRYSTALS-Dilithium • Lattice-based • Digital signature scheme for authenticity and integrity of data	• Based on SPHINCS+ • Stateless hash-based • Digital signature scheme for authenticity and integrity of data	• Based on FALCON • Lattice-based • Very compact digital signature scheme for authenticity and integrity of data	• Stateful hash-based signatures
Privacy / Confidentiality		Authentication / Integrity			

https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

NIST の PQC アルゴリズムを実装し拡張するには IETF 標準が必要、多くの標準はまだ未承認

プロトコルスタンダード (最も緊急性の高いセット)

IKEv2:

- RFC 9370 – Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2) – approved
- RFC 9242 – Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2) – approved
- Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2) – draft
- Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) using PQC - draft

TLS:

- RFC9953 - Hybrid key exchange in TLS 1.3 – approved
- ML-KEM Post-Quantum Key Agreement for TLS 1.3 – draft
- Use of ML-DSA in TLS 1.3 - draft

SSH:

- RFC 10042 - PQ/T Hybrid Key Exchange with ML-KEM in SSH - approved
- Module-Lattice Key Exchange in SSH – draft
- SSH Support of ML-DSA - draft

PKI:

- RFC 9881 - Internet X.509 Public Key Infrastructure: Algorithm Identifiers for ML-DSA – approved
- RFC 9935 - Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)– approved
- Composite Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for use in X.509 Public Key Infrastructure– draft

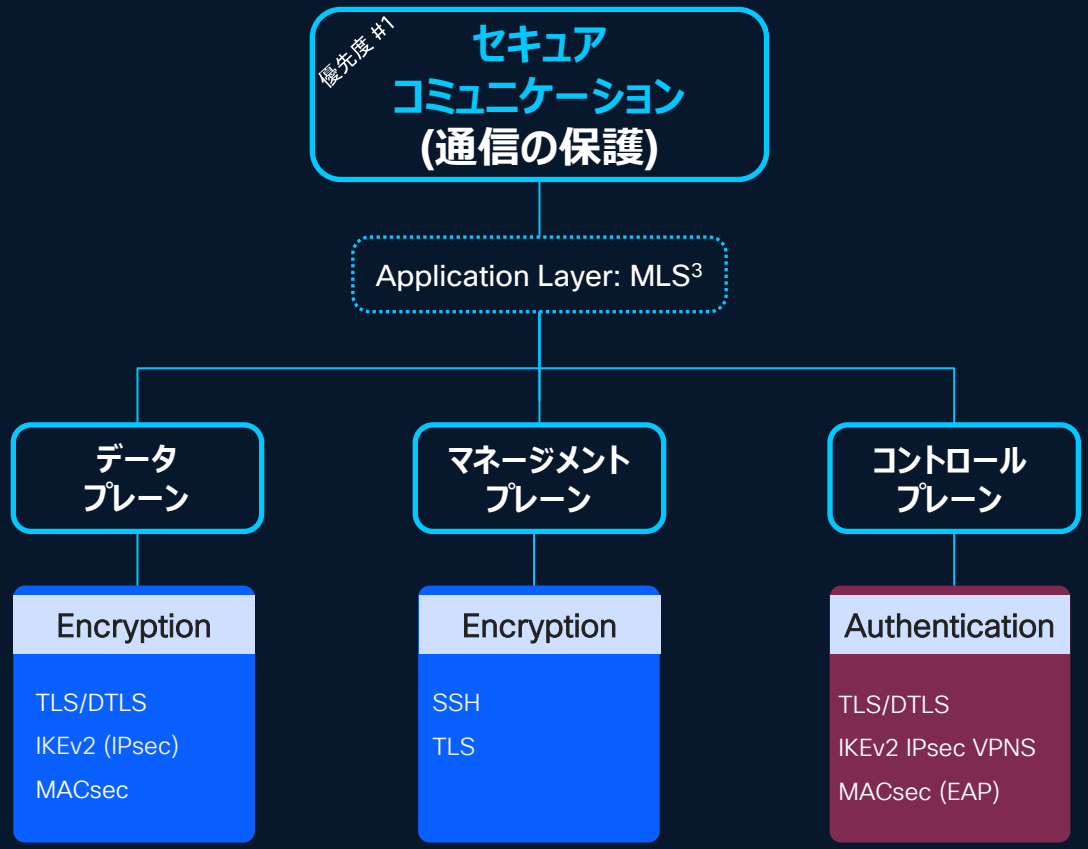
MLS:

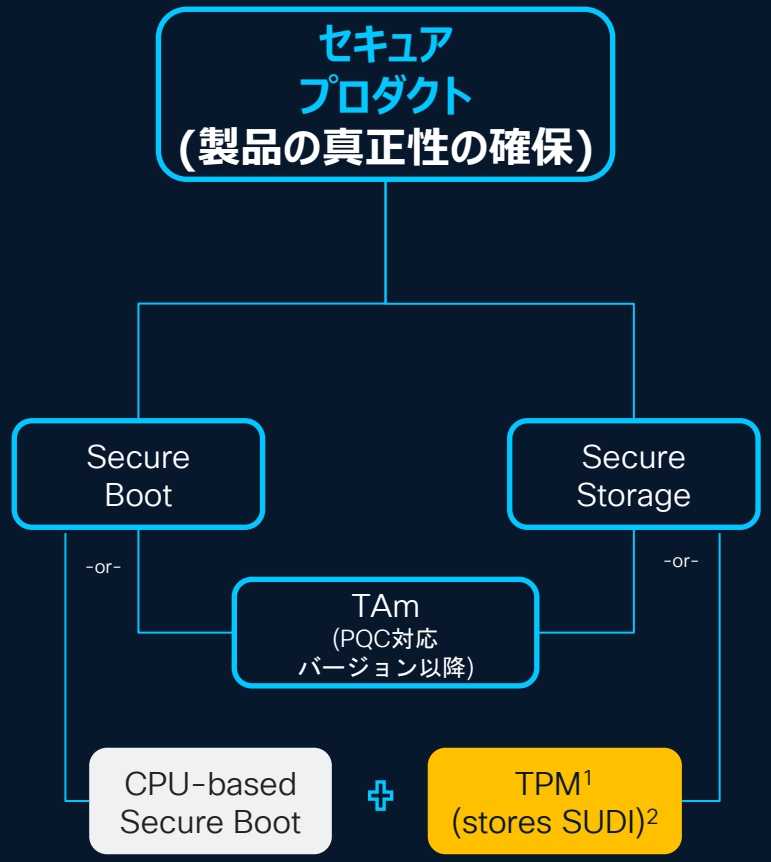
- ML-KEM and Hybrid Cipher Suites for Messaging Layer Security – early draft

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

Cisco の耐量子安全性への取り組みは、お客様の通信の保護と製品の真正性の確保に重点を置いている(CNSA2.0準拠)





Cisco TrustworthyのPQC対応

凡例

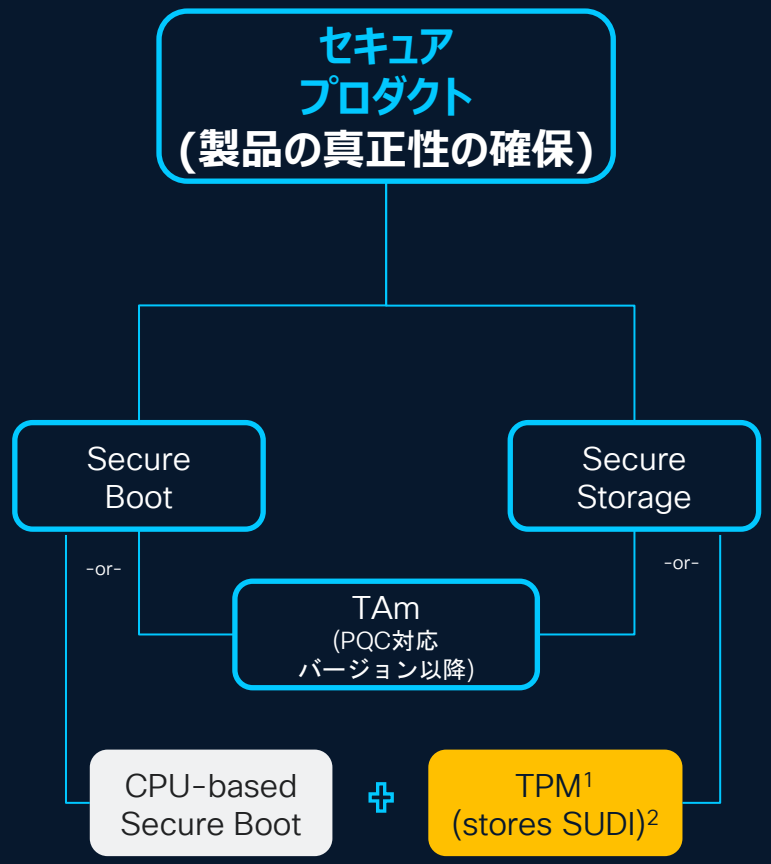
- 外部ベンダーに依存
- 標準化未完了
- Coming soon
- Available now

Note: External key management also available via SKIP or ETSI GS-QKD-014

1. Trusted Platform Module;
2. Secure Unique Device ID
3. MLS is applicable to Webex on the application layer

© 2026 Cisco and/or its affiliates. All rights reserved.

PQC対応のセキュアプロダクトの実現方法



Cisco TrustworthyのPQC対応

TAm(トラストアンカーモジュール)などの独自実装

- ✓Ciscoの独自実装 (Secure Boot と Secure Storageの機能を併せ持つ)
- ✓Cisco Trustworthyを実装する為にCisco Router / Switch 等に搭載
- ✓製品、および、出荷時期によりTAmのバージョンが異なる
- ✓TAmのバージョンは一部を例外として、原則として工場出荷後はアップグレードを行うことが出来ない
- ✓出荷時のTAmのバージョンにより、PQC対応のセキュアプロダクトの可否が異なる

CPUベースのSecure Boot + TPM (PQC対応版)

- ✓CPUによるSecure Boot と TPMによる Secure Storage で実現
- ✓TCGによりTPMの仕様が標準化されている
- ✓使用するTPMはPQC対応のものである必要がある
- ✓サーバや小型ネットワーク機器、IoT機器等で利用
- ✓OSについてもUEFI等のPQC対応についても考慮する必要がある

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

PQC対応の新しいプラットフォーム

Cisco Live 2025 US San Diegoで発表のプラットフォームから順次対応を開始

Cisco 8000 シリーズ Secure Router

PQC Capable

Small Branch	Medium Branch	Large Branch	Campus (XLarge)	Data Center (XLarge)
Cisco 8100-G2	Cisco 8200-G2	Cisco 8300-G2	Cisco 8400-G2	Cisco 8500-G2
IPsec: Up to 1.5 Gbps SD-WAN: Up to 1 Gbps Threat Protection: Up to 1 Gbps	IPsec: Up to 5 Gbps SD-WAN: Up to 4 Gbps Threat Protection: Up to 2.5 Gbps	IPsec: Up to 30 Gbps SD-WAN: Up to 12 Gbps Threat Protection: Up to 7 Gbps	IPsec: Up to 45 Gbps SD-WAN: Up to 22 Gbps Threat Protection: Up to 11 Gbps	IPSec: Up to 60 Gbps SD-WAN: Up to 23 Gbps IPSec Scale up to 10,000

C9610 Core Smart Switches

Generation 3 modular core

PQC Capable

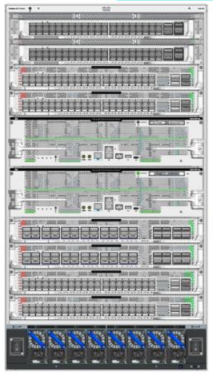
Gen 3 Supervisors

C9610-SUP3

C9610-SUP3XL

- 2M IPv4/1M IPv6
- 3.2 Tbps per slot
- 512K hosts or clients*
- 32G DDR4 memory
- 256K ACL entries*
- 8 core X86 CPU @2.0 Ghz

Gen 3 Chassis



C9610

- 8-line card slots (1.25 RU)
- 2 supervisor slots (dedicated) (2.5 RU)
- 51.2 Tbps System Bandwidth
- Four serviceable fan trays in rear side
- Blue Beacons (system/fan tray, sup, line cards)
- Modular power supplies

Gen 3 Line cards

C9610-LC-32CD

C9610-LC-40YL4CD

4x FAN Trays

With front to back airflow

*Hardware Capable

Cisco C9350 シリーズ Smart Switches

PQC Capable

Gigabit

Up to 1 GB

C9350-24P/48P
- 24/48x 1G/100M/10M copper
- 30W PoE+

C9350-24U/48U
- 24/48x 1G/100M/10M copper
- 60W UPoE

C9350-24T/48T
- 24/48x 1G/100M/10M copper
- Data only

MultiGig

Up to 10 GB (mGig)

C9350-48HX
- 48x 10G mGig
- 90W UPOE+

C9350-48TX
- 24/48x 10G mGig
- Data only

On-prem

Cloud management

Unified Product-Single SKU

C9350 only flexible Uplinks – Introducing 50G Uplinks in Access

Cisco C9350 Exclusive Modular uplinks

4x 100G | 2 x 100G | 8 x 25G or 4 x 50G

3 Slot Titanium PSU For Maximum Resiliency

New Titanium-rated power supplies

500W AC | 850W AC | 1600W AC

New Stack cables capable of 1.6T Stack Bandwidth

New StackWise® and StackPower cables

Stack Adapters | 50CM-1M-3M | 30CM-150CM

Front to Back and Back to Front Fan Airflow

New Modular Fans

© 2026 Cisco and/or its affiliates. All rights reserved.

セキュアコミュニケーション | 例: Cisco 8000 Series Secure Routers

ソフトウェア側のPQC実装により、各トランスポート暗号化のPQC対応を実現



IKEv2 IPsec

DMVPN

FlexVPN,
IKEv2 CLB

MACsec
EAP-TLS

SSH

IOS-XE Release 26.1.1 (2026年4月リリース済み)
ML-KEM（FIPS-203) が各プロトコルで利用可能となった

© 2026 Cisco and/or its affiliates. All rights reserved.

セキュアコミュニケーション / セキュアプロダクト: Cisco 8000 Series Secure Router PQC Readiness
IOS XE Release 26.1.1(2026/4リリース済み), 26.2.1(2026/9 リリース済み)

	Secure Routers (8600 and 8500 Series)	Secure Routers (8400 and 8300 Series)	Secure Routers (8200 Series)	Secure Routers (8100 Series)
Quantum-safe Communications				
IPsec: includes DMVPN, FlexVPN (ML-KEM for IKEv2)	26.1.1	26.1.1	26.1.1	26.1.1
IPsec: SD-WAN (ML-KEM for IKEv2)	26.2.1	26.2.1	26.2.1	26.2.1
MACsec (ML-KEM for EAP-TLS 1.3)	26.1.1	26.1.1	26.1.1	N/A
SSH (ML-KEM for key-exchange)	26.1.1	26.1.1	26.1.1	26.1.1
TLS 1.3 Infra (ML-KEM for key exchange)	26.1.1	26.1.1	26.1.1	26.1.1
TLS 1.3: SD-WAN (ML-KEM for key-exchange)	26.2.1	26.2.1	26.2.1	26.2.1
PKI for Site-to-Site VPNs (ML-DSA for authentication)	26.2.1	26.2.1	26.2.1	26.2.1
Quantum-safe Products				
LMS signed ROMMON	対応予定	対応予定	対応予定(一部機種は除く)	対応予定
ML-DSA signed IOS XE	対応予定	対応予定	対応予定(一部機種は除く)	対応予定

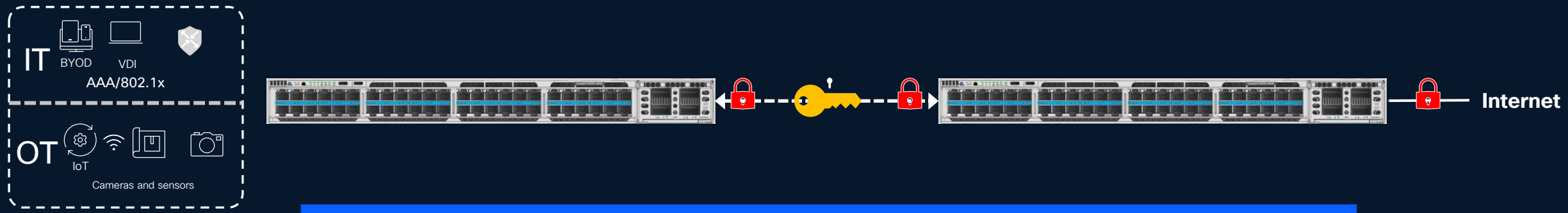
© 2026 Cisco and/or its affiliates. All rights reserved.

※「対応予定」につきましては、開発等の都合により変更となる可能性が御座います。

Cisco Public

セキュアコミュニケーション / セキュアプロダクト: Cisco 9000 Switching PQC Readiness

ソフトウェア側のPQC実装により、各トランスポート暗号化のPQC対応を実現



	IOS-XE for Switching	Supported Platform
Quantum-safe transport (PQC Secure Communication)		
MACsec (ML-KEM for EAP-TLS 1.3)	26.1.1 (2026/4リリース済み)	C9350, C9200-C9600
IPsec (ML-KEM for IKEv2)	26.2.1 (2026/9リリース済み)	C9350
SSH (ML-KEM for key exchange)	26.1.1 (2026/4リリース済み)	C9350, C9550,C9610, C9200-C9600
TLS 1.3* (ML-KEM for key exchange)	26.2.1 (2026/9リリース済み)	C9350, C9550, C9610
Quantum-safe secure boot (PQC Secure Boot)		
LMS signed ROMMON	対応予定	C9350, C9550, C9610
ML-DSA signed IOS XE	対応予定	C9350, C9550, C9610

© 2026 Cisco and/or its affiliates. All rights reserved.

※「対応予定」につきましては、開発等の都合により変更となる可能性が御座います。

Cisco Public

Cisco’s Quantum Resilience Framework

Ciscoは、量子レジリエンスの複数のレベルを明確に定義するフレームワークを開発

Quantum Resilience	Secure Communication	Secure Products	Description
Level 1 *Partial*	3rd-Party Key Management[1]	Secure Boot (LDWM)	出発点であり、最終状態ではありません。これは、組織がより完全なレベルの量子耐性に向けて前進するための基盤となります。
Level 2 *Core*	Confidentiality[2]	Secure Boot (LMS/XMSS, ML-DSA) Software/Firmware Integrity	転送中のデータのリスクと、保護を実施するプラットフォームの完全性の両方に対処すると同時に、顧客が自社のセキュリティ、相互運用性、およびコンプライアンスのニーズを反映した方法でPQCを採用できる柔軟性を提供
Level 3 *Extended*	Confidentiality[2] Authentication[3]	Secure Boot (LMS/XMSS, ML-DSA) Software/Firmware Integrity Hardware Identity[4]	Level2の領域に加えて、 PQC で署名されたセキュアな一意のデバイス識別子(SUDI)、および、アテステーション ID キー証明書(AIK) により、デバイスは自身の身元を暗号的に証明し、ライフサイクル全体を通じて改ざんされていないことを実証

CNSA 2.0 に準拠

1. 暗号の柔軟性を実現するポスト量子事前共有鍵（手動および動的）ならびに量子鍵配送（QKD）
2. 関連するプロトコルは製品によって異なるが、TLS、dTLS、IKEv2/IPsec、OpenPGP、MLS、X509、SSH、S/MIMEにおけるPQCアルゴリズムの実装が含まれる場合がある
3. 公開鍵インフラストラクチャおよび認証の大部分において、PQC標準は未定義のままである
4. 例：SUDI（単一一意デバイス識別子

注：レベル2およびレベル3はNIST標準のアルゴリズムを活用し、CNSA 2.0の要件に準拠している

Quantum Resilience Needs a Common Language. Here’s Where to Start
https://blogs.cisco.com/security/quantum-resilience-needs-a-common-language

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Public

Cisco’s Quantum Resilience Framework

Level 1 – Partial

- **Secure Communication**
  Third-party key management:
  サードパーティによる鍵管理のサポート（量子鍵配送（QKD）のサポートを含む）により、プロトコル層での完全な PQC を必要とせずに、暗号の俊敏性を実現します。

- **Secure Product**
  セキュアブートでは、LDWM などの確立されたハッシュベースの署名アルゴリズムを使用します。

レベル 1 は出発点であり、最終状態ではありません。これは、組織がより完全なレベルの量子耐性に向けて前進するための基盤となります。

Level 2 – Core

- **Secure Communication**
  Confidentiality:
  機密性の保護を、TLS、DTLS、IKEv2/IPsec、MLS、SSHなどの関連プロトコル全体にわたり実施します。顧客のリスク優先順位や進化する標準に基づいて、必要に応じて純粋なPQCまたはハイブリッドアプローチをサポートします。
- **Secure Product**
  完全なPQC信頼チェーン：
  ハードウェアの信頼の根源から実行中のアプリケーションに至るまで、ML-DSAやLMSなどのNIST承認アルゴリズムを用いた次世代セキュアブートに加え、CNSA 2.0に準拠したソフトウェアおよびファームウェアの完全性検証を含みます。

レベル2では、転送中のデータのリスクと、保護を実施するプラットフォームの完全性の両方に対処すると同時に、顧客が自社のセキュリティ、相互運用性、およびコンプライアンスのニーズを反映した方法でPQCを採用できる柔軟性を提供します。

Level 3 – Extended

- **Secure Communication**
  Confidentiality:
  機密性 を関連プロトコル全体に適用するとともに、デバイス、ユーザー、およびシステムの量子耐性認証 および身元確認を実現します。

- **Secure Product**
  PQC で署名されたセキュアな一意のデバイス識別子(SUDI)、および、アテステーション ID キー証明書(AIK) により、デバイスは自身の身元を暗号的に証明し、ライフサイクル全体を通じて改ざんされていないことを実証できます。

Level 3では、Level2の領域に加えて、
PQC で署名されたセキュアな一意のデバイス識別子およびアテステーション ID キー証明書 により、デバイスは自身の身元を暗号的に証明し、ライフサイクル全体を通じて改ざんされていないことを実証できます。

© 2026 Cisco and/or its affiliates. All rights reserved.

※CNSA2.0に準拠する為には、Level 2以上に対応することが必須

Cisco Public

Cisco Live 2026でのアナウンスについて

シスコの主要製品ポートフォリオ全体における量子耐性通信の新たな進展:

2026年12月までにシスコの主要製品ポートフォリオの大部分で量子耐性通信機能を実現するというコミットメントに基づき、シスコは、最も機密性の高い企業トラフィックが流れるシステムに対して、ポスト量子保護を拡大しています。また、量子耐性通信に関するロードマップを以下のURLで公開しています。

- Quantum-Safe Communications Roadmap
  https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/quantum-safe-communications-roadmap.pdf

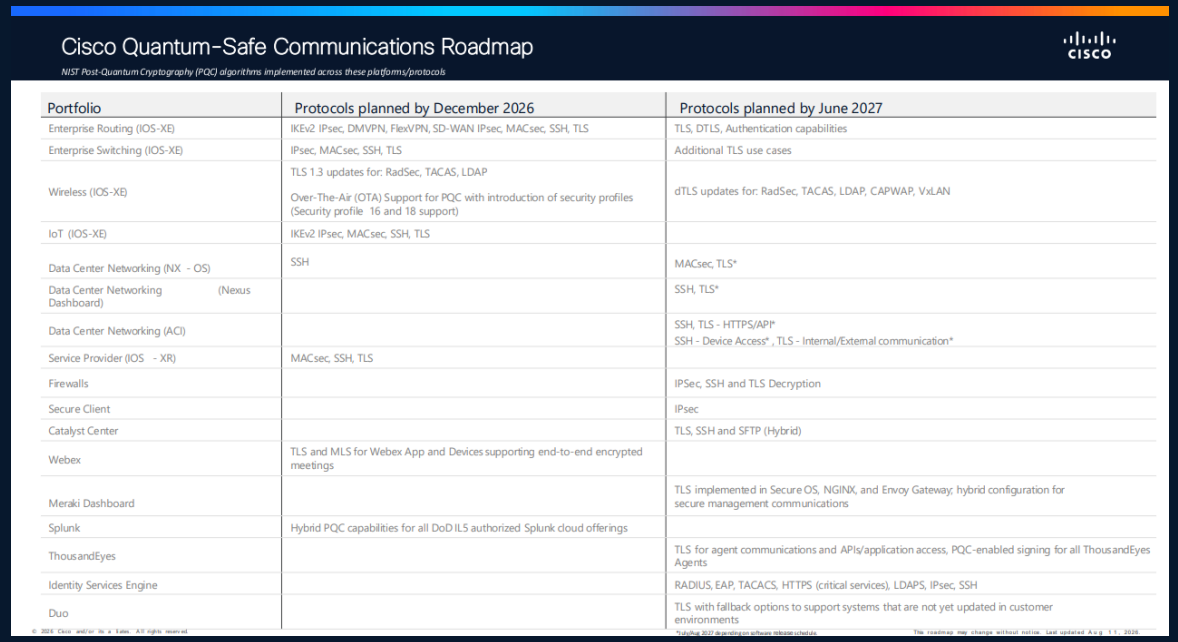
新しいインフラストラクチャでは、デフォルトで量子耐性を確保:

本日(2026年6月2日)より、新たに導入されるすべてのキャンパス、ブランチ、データセンター向けのルーター、スイッチ、ファイアウォールシリーズには、量子耐性のあるセキュアブート機能(Quantum Secure Products)が搭載されます。

出典: Quantum Resilience Needs a Common Language. Here's Where to Start.
https://blogs.cisco.com/security/quantum-resilience-needs-a-common-language

© 2026 Cisco and/or its affiliates. All rights reserved.

Quantum-Safe Communications / Product Roadmap



Cisco Quantum-Safe Communications Roadmap

NIST Post-Quantum Cryptography (PQC) algorithms implemented across these platforms/protocols

Portfolio	Protocols planned by December 2026	Protocols planned by June 2027
Enterprise Routing (IOS-XE)	IKEv2 IPsec, DMVPN, FlexVPN, SD-WAN IPsec, MACsec, SSH, TLS	TLS, DTLS, Authentication capabilities
Enterprise Switching (IOS-XE)	IPsec, MACsec, SSH, TLS	Additional TLS use cases
Wireless (IOS-XE)	TLS 1.3 updates for: RadSec, TACAS, LDAP Over-The-Air (OTA) Support for PQC with introduction of security profiles (Security profile 16 and 18 support)	dTLS updates for: RadSec, TACAS, LDAP, CAPWAP, VxLAN
IoT (IOS-XE)	IKEv2 IPsec, MACsec, SSH, TLS	
Data Center Networking (NX - OS)	SSH	MACsec, TLS*
Data Center Networking (Nexus Dashboard)		SSH, TLS*
Data Center Networking (ACI)		SSH, TLS - HTTPS/API* SSH - Device Access* , TLS - Internal/External communication*
Service Provider (IOS - XR)	MACsec, SSH, TLS	
Firewalls		IPSec, SSH and TLS Decryption
Secure Client		IPsec
Catalyst Center		TLS, SSH and SFTP (Hybrid)
Webex	TLS and MLS for Webex App and Devices supporting end-to-end encrypted meetings	
Meraki Dashboard		TLS implemented in Secure OS, NGINX, and Envoy Gateway; hybrid configuration for secure management communications
Splunk	Hybrid PQC capabilities for all DoD IL5 authorized Splunk cloud offerings	
ThousandEyes		TLS for agent communications and APIs/application access, PQC-enabled signing for all ThousandEyes Agents
Identity Services Engine		RADIUS, EAP, TACACS, HTTPS (critical services), LDAPS, IPsec, SSH
Duo		TLS with fallback options to support systems that are not yet updated in customer environments

© 2026 Cisco and/or its affiliates. All rights reserved.

TriviaAug 2027 depending on software release schedule

This roadmap may change without notice. Last updated Aug 11, 2026.



Cisco Quantum-Safe Product Announcements (Cisco Live US 2026)

NIST Post-Quantum Cryptography (PQC) algorithms implemented across these platforms/protocols

Portfolio	Planned Products / Platforms	Quantum- Safe Communications	Quantum- Safe Products
Enterprise Routing (IOS-XE)			
	New Product Launches: Cisco Secure Router 8131H, 8151H-C, 8211, 8221, 8221L, 8225, 8650,Cisco 8255 Secure Router Node (Unified Edge)	Core	Core
Enterprise Switching (IOS-XE)			
	C9550 Fixed Core Switches, C9350 Fixed Access Switches	Core	Core
Enterprise Wireless (IOS-XE)			
	Future Shipments of: CW9800H1, CW9800H1-MCG, CW9800H2, CW9800M, CW9800L, CW9800L-MCG	Core	Core
Data Center Networking (NX-OS)			
	N9300 Fixed Switch (P200 based)	Core	Core
Service Provider (IOS-XR) —Software Release Only			
	• Cisco 8000, NCS5700 (excluding NCS57C3), NCS540 series (excluding N540-ACC-SYS, N540X-ACC-SYS, N540-24Z8Q2C-SYS) • EAP-TLS for MACsec on all MACsec capable IOS-XR platforms	Core	—
Firewalls & VPNs			
	• Future PQC SKUs for 1200, 3100, 4200 & 6100	Core	Core

© 2026 Cisco and/or its affiliates. All rights reserved.

This roadmap may change without notice. Last updated Aug 11, 2026.

Quantum-Safe Communications Roadmap
https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/quantum-safe-communications-roadmap.pdf

Note：最新のRoadmapは上記のURLからご確認ください。

© 2026 Cisco and/or its affiliates. All rights reserved.


CISCO