

耐量子計算機暗号への移行準備してますか？ ～2030年台の安全なネットワークに向けて～

高橋 康（パナソニック ホールディングス株式会社）

JANOG58@本会議場2F-B(真珠の間B) 愛媛県民文化会館 in 愛媛・松山
Day2 2026年7月16日(木) 10:15～11:00 (45分)

自己紹介（高橋 康）

経歴

- 2019年-2022年：富士通株式会社
- 2022年-現在：パナソニックホールディングス株式会社
 - 一貫して暗号に関するR&D業務を担当（ネットワーク素人です）
 - **JANOG参加は3回目**（56：初参加、57：初発表）

業務内容

- 弊社IoT機器(宅内家電など)のPQC移行支援を目的としたR&D
 - 動作評価・規格調査
 - 移行課題抽出 & 解決技術開発
 - 移行支援コンサル

趣味

- 将棋 (見る将)、最近矢倉だけ指せるようになりました(勝てるとは言っていない)



本発表のOverview・議論したいポイント

共有したい事実

- PQC移行はすでに複数の国・企業で開始
- 従来暗号とはスペックに差異があり、機器・サービスに影響

我々から伝えたいこと

- PQC移行はセキュリティのためではない、**製品・サービス維持のため**
- 移行には時間がかかることがあるので、**今から優先順位・取り組み開始時期検討**を行うべき

皆さんと議論したいこと

- **ネットワーク事業者はPQC移行にいつから着手すればよさそうですか？**
 - 2030年or2035年に間に合わせるためには、製品ライフサイクルを考えるといつ？
- **ネットワーク分野でのPQC移行において何が課題になりそうでしょうか？**
 - 例) パケットサイズの増大、次世代ルータの処理性能不足など

PQCについて

これからのセキュリティに必須な暗号

- NIST（米国国立標準技術研究所）主導で標準化された新しい公開鍵暗号方式
- 量子計算機の計算能力でも解読できない暗号方式

組織/地域	鍵交換・KEM	電子署名
NIST (米国)	ML-KEM, HQC	ML-DSA, SLH-DSA, FN-DSA
CNSA 2.0 (NSA)	ML-KEM	ML-DSA, LMS, XMSS
IETF	ML-KEM（が中心）	ML-DSA（が中心）
ETSI・EU (欧州)	ML-KEM, FrodoKEM	ML-DSA, SLH-DSA
ISO/IEC	ML-KEM, Classic McEliece	ML-DSA
日本 (CRYPTREC)	ML-KEM	未発表

- PQCはただ一つ的方式を指すものではなく、複数組織で複数方式が標準(候補)として採用

PQCは未来の技術ではなく、既に標準化され、導入が推奨されている技術

将来のセキュリティ担保ではなく、現在の製品・サービス持続可能性のため

Q1：お客様・取引先から「PQC対応してますか」と聞かれたことがありますか？

- 複数の国・組織で、重要システムでの移行がすでに開始
- CRA・JC-STARなどでもPQC移行可能であることが事実上の要件

国・地域	組織	内容
米国	NSA (CNSA 2.0)	国家安全保障システム向けにPQC移行を要求。ML-KEM、ML-DSAを採用。 [entangledfuture.com]
英国	NCSC	2028年までに暗号資産棚卸し、2035年までに移行完了を推奨 [ncsc.gov.uk] , [ncsc.gov.uk]
カナダ	CCCS	政府全体のPQC移行ロードマップ策定。2035年完了目標。 [cyber.gc.ca] , [canada.ca]
ドイツ	BSI	Crypto AgilityとHybrid運用を推奨 [bsi.bund.de]
オーストラリア	ASD / ACSC	2030年重要システム移行完了を目標

制度・認証	地域	PQCとの関係
CRA (Cyber Resilience Act)	EU	製品ライフサイクル全体のセキュリティ維持を要求。将来的な暗号移行計画の説明責任に直結。 [digital-stakeholders.europa.eu]
JC-STAR	日本	IoT製品のセキュリティ評価制度。暗号利用状況や更新可能性の説明が重要
CNSA 2.0	米国	国家安全保障用途でPQC利用方針を提示。 [entangledfuture.com]
Common Criteria / EUCC	EU	2025年からPQCアルゴリズムを採用対象に取り込み開始。 [media.defense.gov]

サプライチェーン要求、認証取得、外部サービスとの相互接続
といった製品・サービスの持続可能性のために必要

【参考】なぜPQC導入が必要か？

PQC移行開始国・組織

国・地域	組織	内容
米国	NIST	2024年にML-KEM、ML-DSA、SLH-DSAを正式標準化。組織に移行開始を推奨。 [etsi.org] , [ietf.org]
米国	NSA (CNSA 2.0)	国家安全保障システム向けにPQC移行を要求。ML-KEM、ML-DSAを採用。 [entangledfuture.com] , [entangledfuture.com]
英国	NCSC	2028年までに暗号資産棚卸し、2035年までに移行完了を推奨 [ncsc.gov.uk] , [ncsc.gov.uk]
カナダ	CCCS	政府全体のPQC移行ロードマップ策定。2035年完了目標。 [cyber.gc.ca] , [canada.ca]
EU	欧州委員会	PQC移行ロードマップを策定。加盟国へ移行計画策定を推奨。 [digital-st...europa.eu] , [digital-st...europa.eu]
ドイツ	BSI	「PQCへの移行を開始すべき」と明言。Crypto AgilityとHybrid運用を推奨。 [bsi.bund.de] , [bsi.bund.de]
オーストラリア	ASD / ACSC	PQC準備を推奨。長寿命システムへのPQC考慮を要求。2030年重要システム移行完了を目標。

PQC関連認証制度

制度・認証	地域	PQCとの関係
CRA (Cyber Resilience Act)	EU	製品ライフサイクル全体のセキュリティ維持を要求。将来的な暗号移行計画の説明責任に直結。 [digital-st...europa.eu]
JC-STAR	日本	IoT製品のセキュリティ評価制度。暗号利用状況や更新可能性の説明が重要。
CNSA 2.0	米国	国家安全保障用途でPQC利用方針を提示。 [entangledfuture.com] , [entangledfuture.com]
NIS2	EU	サプライチェーンを含むサイバーリスク管理を要求。PQC計画とも親和性が高い。 [aisec.fraunhofer.de] , [digital-st...europa.eu]
Common Criteria / EUCC	EU	2025年からPQCアルゴリズムを採用対象に取り込み開始。 [media.defense.gov]
FIPS 140-3エコシステム	米国	PQCアルゴリズムの実装・検証が進行。 [etsi.org] , [ietf.org]

PQC移行開始民間製品・サービス

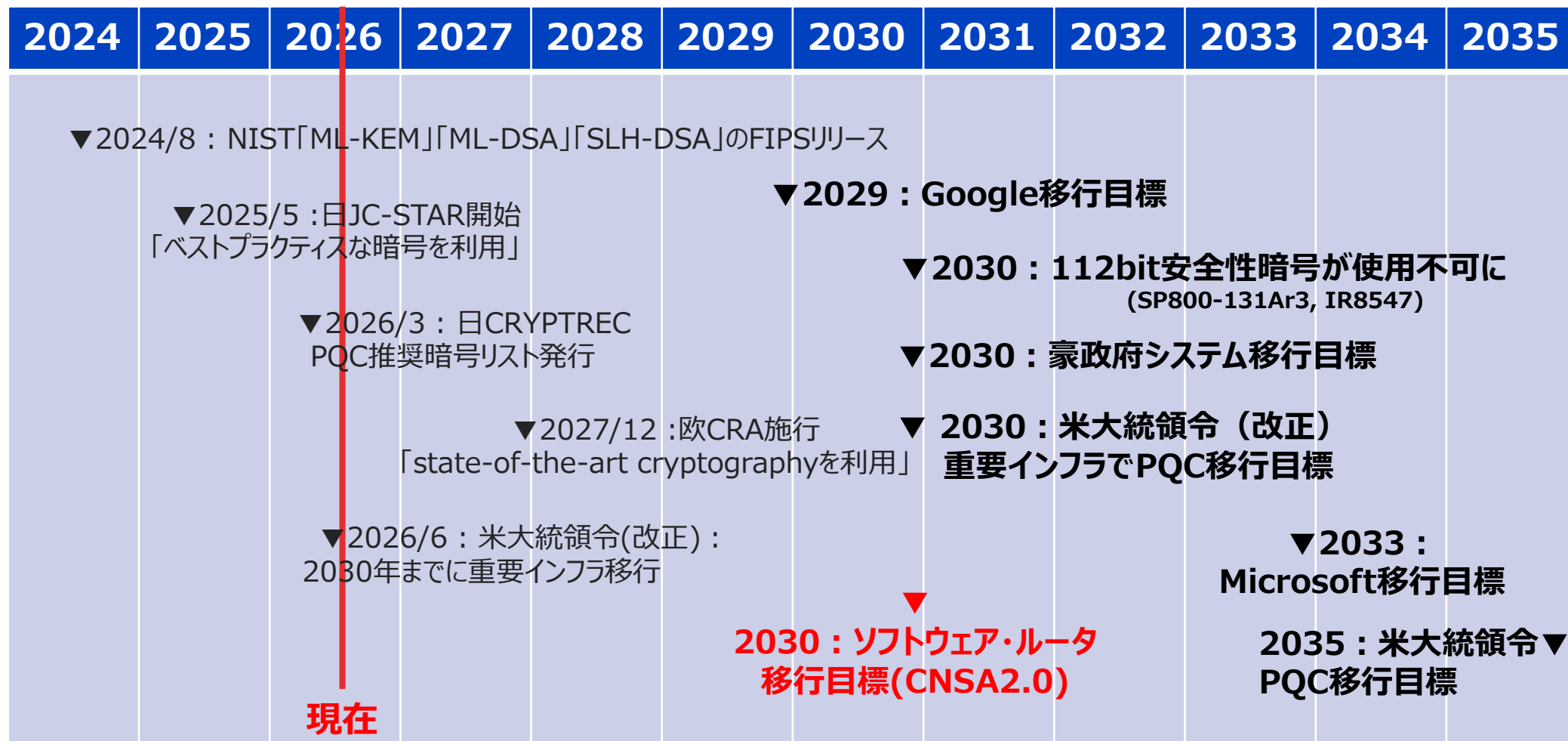
分類	企業	PQCへの取り組み
クラウド	AWS	AWS Certificate Manager等でPQC対応や検証を開始 [media.defense.gov]
クラウド	Google Cloud	Cloud KMSやCloud ArmorなどでPQC対応を推進 [nic.ad.jp]
クラウド	Microsoft Azure	Microsoft 365を含むQuantum Safe戦略を公開し移行を推進 [pq.cloudfl...search.com]
CDN・エッジ	Cloudflare	2029年フルPQC化目標 [nttdocomo-...elopers.jp]
モバイルOS	Android	ML-KEM Hybrid TLSをサポート。Chrome・Google Play基盤とも連動。 [nic.ad.jp]
PC OS	Apple (iOS / macOS)	Safariだけでなく、OSレベルでPQC対応TLSを有効化
PC OS	Windows	Windows Insider版からPQC対応API・証明書・TLS機能を提供開始 [developers...dflare.com]

いつまでに移行すればいいか？

7 / 16

(私の知る限り)全ての国・組織にて遅くとも2035年が期限

- ただし、重要インフラ・政府システムに限っている国は少なくない
- 最近では、Google・米国が2030年期限に前倒し



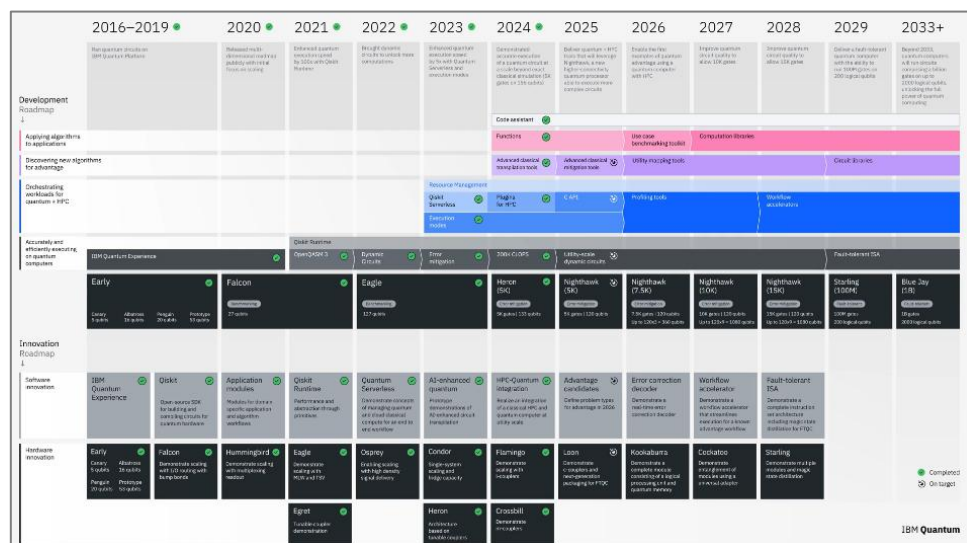
現在

2026年3月Googleらの論文で従来暗号の危殆化見込みが早まったため

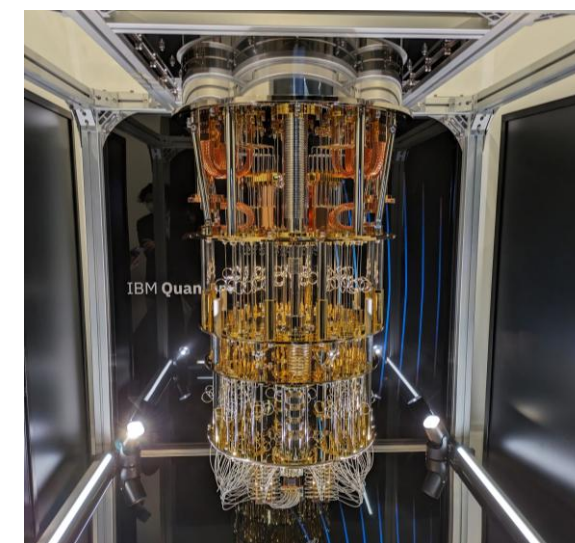
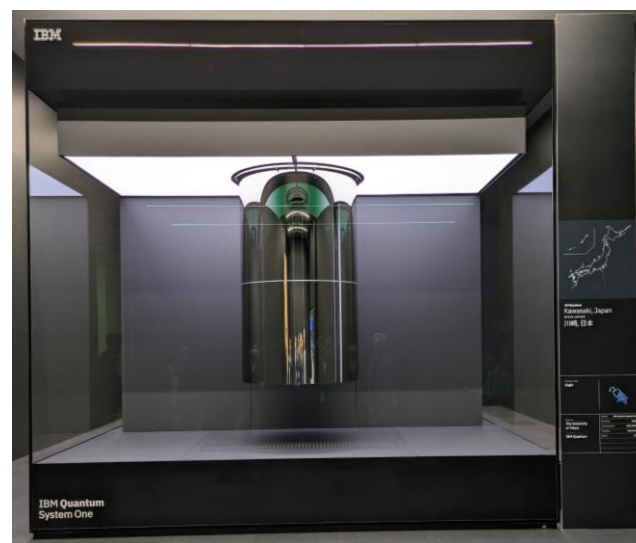
- RSA2048を100万量子ビット未満で解読可能
- ECDSAを1万量子ビット程度で解読可能

量子計算機の開発見込み

- 2030年前半には100万量子ビット程度の量子計算機が開発されるとの予想もある

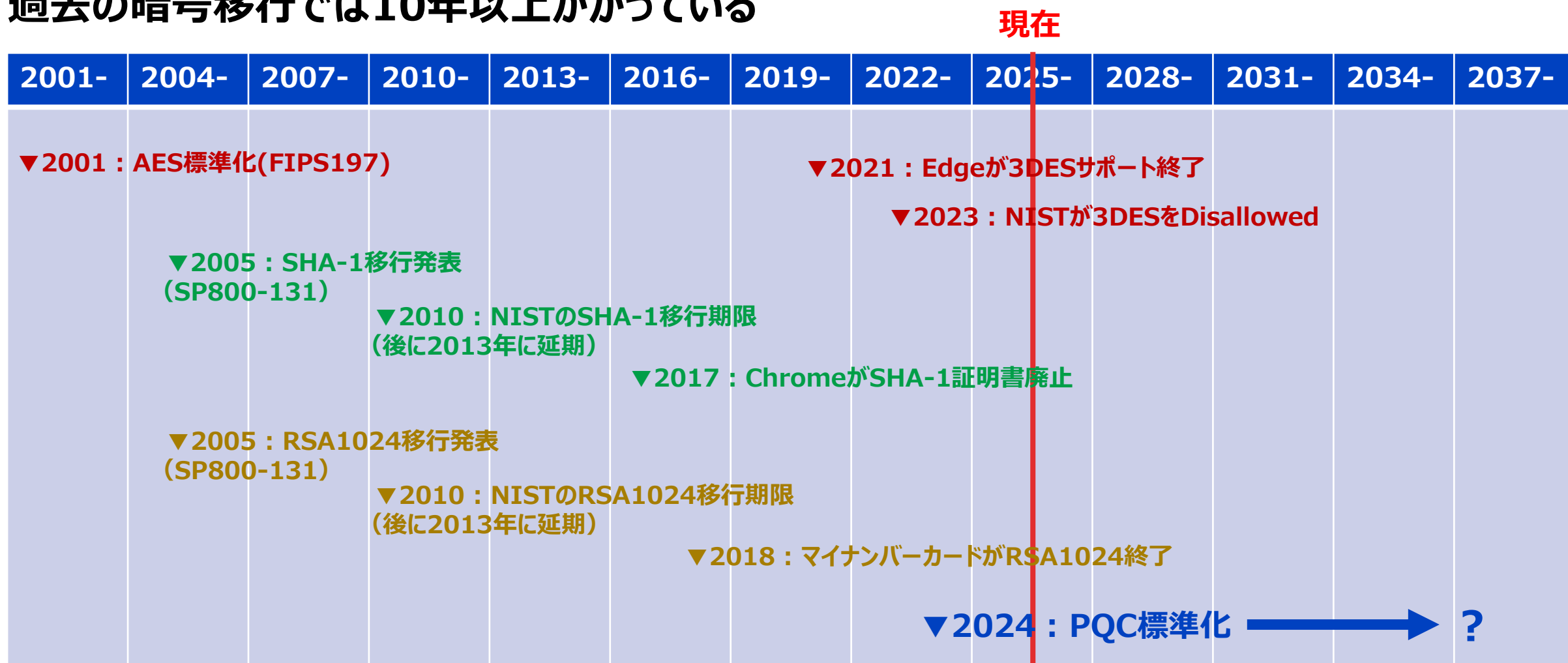


2025 IBM Quantum Roadmap update - IBM Mediacenter



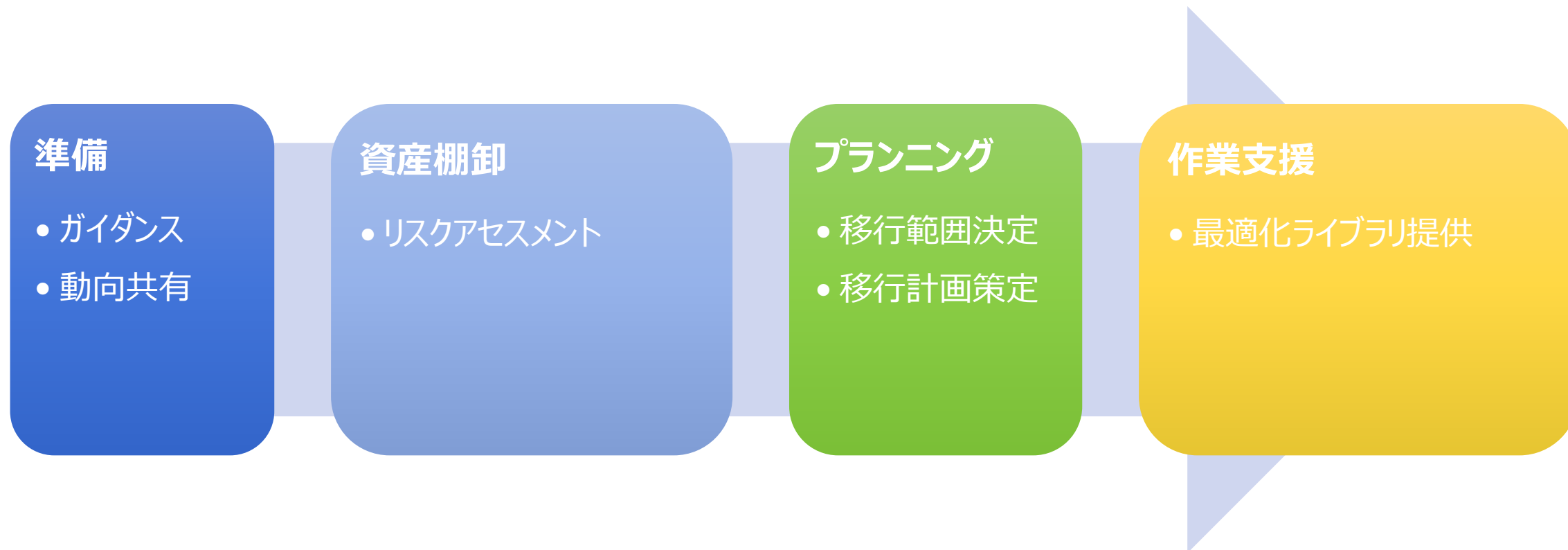
IBM量子計算機@川崎

過去の暗号移行では10年以上かかっている



PQC移行には10年～15年はかかる見込み

PQC移行に必要な作業概観



上記を自社単独で行うのは非常に困難
業界全体で協力していく必要がある

移行に向けた具体的な取り組み

PQC関連WG

- PQUIP WG : PQC導入・問題対応を集約
 - [draft-ietf-tls-ecdhe-mlkem-05 - Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3](#)
 - [draft-ietf-tls-mldsa-05 - Use of ML-DSA in TLS 1.3](#)

発行済RFC

- RFC 9941: SSH Key Exchange Method Using Hybrid Streamlined NTRU Prime
- RFC 9958: Post-Quantum Cryptography for Engineers

Post-Quantum Use In Protocols (pquiip)

About Documents Meetings History Photos Email expansions List archive »

WG	Name	Post-Quantum Use In Protocols
	Acronym	pquiip
	Area	Security Area [sec]
	State	Active
	Charter	charter-ietf-pquiip-01 Approved
	Document dependencies	Show
	Additional resources	GitHub Organization Grand list of WGs and protocols looking at PQC algorithms
Personnel	Chairs	Paul E. Hoffman , Sofia Cell
	Area Director	Paul Wouters
Mailing list	Address	pqc@ietf.org
	To subscribe	https://www.ietf.org/mailman/listinfo/pqc
	Archive	https://mailarchive.ietf.org/arch/browse/pqc/
Chat	Room address	https://zulip.ietf.org/#narrow/stream/pquiip

Charter for Working Group

Some IETF protocols rely upon cryptographic mechanisms that are considered secure given today's "classical computers" but would be vulnerable to attacks by a Cryptographically Relevant Quantum Computer (CRQC). These mechanisms rely upon algorithms based on integer factorization or the discrete logarithm problem. Outside of the IETF, active work is underway to develop and validate Post-Quantum Cryptography (PQC) mechanisms that are expected to be resilient to the cryptanalysis capabilities of future CRQCs (e.g., CFRG, US NIST). Select IETF WGs (e.g., LAMPS, TLS, IPSECME, COSE) have already begun standardizing revised protocol behaviors. The focus of Post-Quantum Use in Protocols (PQUIP) WG is to support this growing body of work in the IETF to facilitate the evolution of IETF protocols and document associated operational guidance with respect to PQC.

The WG will provide a standing venue to discuss PQC (operational and engineering) transition issues and experiences to date relevant to work in the IETF. The WG will also provide a venue of last resort to discuss PQC-related issues in IETF protocols that have no associated maintenance WGs. This

IETF PQUIP WG

Status: Informational
More info: [Datatracker](#) | [IPR](#) | [Info page](#)

Stream: Internet Engineering Task Force (IETF)
RFC: [9941](#)
Category: Informational
Published: April 2026
ISSN: 2070-1721
Authors: [M. Friedl](#) [J. Mojzis](#) [S. Josefsson](#)
[OpenSSH](#) [TinySSH](#)

Table of Contents

1. Introduction
2. Requirements Language
3. Key Exchange Method: sntrup761x25519-sha512
4. Security Considerations
5. IANA Considerations
6. References
 - 6.1. Normative References
 - 6.2. Informative References

[Appendix A. Test Vectors](#)
[Acknowledgements](#)
[Authors' Addresses](#)

RFC 9941

Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512

Abstract

This document describes a widely deployed hybrid key exchange method in the Secure Shell (SSH) protocol that is based on Streamlined NTRU Prime sntrup761 and X25519 with SHA-512.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

RFC9941

ETSI

- ETSI TR 103 619
 - Migration strategies and recommendations to Quantum Safe schemes (2020)
- ETSI TR 103 966
 - Quantum-Safe Cryptography (QSC); Deployment Considerations for Hybrid Schemes (2024)
- ETSI EG 203 310
 - Quantum Computing Impact on Security of ICT Systems [[standards....alspec.com](https://standards.etsi.org/EG/203/310/)]

ISO

- ISO/IEC 14888
 - 電子署名ファミリ (XMSS,LMSも含まれる)
- ISO/IEC 18033
 - KEM/暗号化 (FrodoKEM,BIKEも含まれる)

PQCと従来暗号の違い

- ・ 長所：従来暗号と比べて**高速**（1.5倍～10倍）
- ・ 短所：従来暗号と比べて**鍵サイズとメモリ使用量が大い**（10倍～100倍）

システムへの移行時に予想される課題

- ・ 鍵サイズが大い → 小セキュア領域機器やICカードへの搭載が困難
- ・ メモリ使用量が大い → 省リソース機器での動作が困難

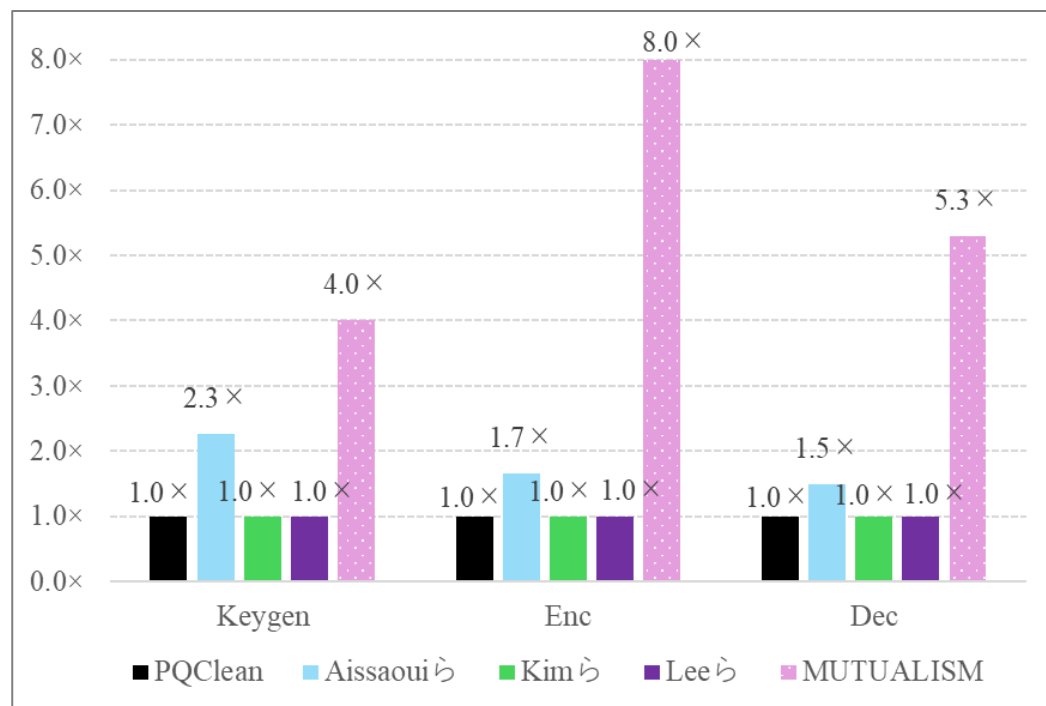
署名アルゴリズム	Stack Usage
ECDSA (従来暗号)	1584 byte
ML-DSA (PQC)	38320 byte

ML-DSAのスタック消費量

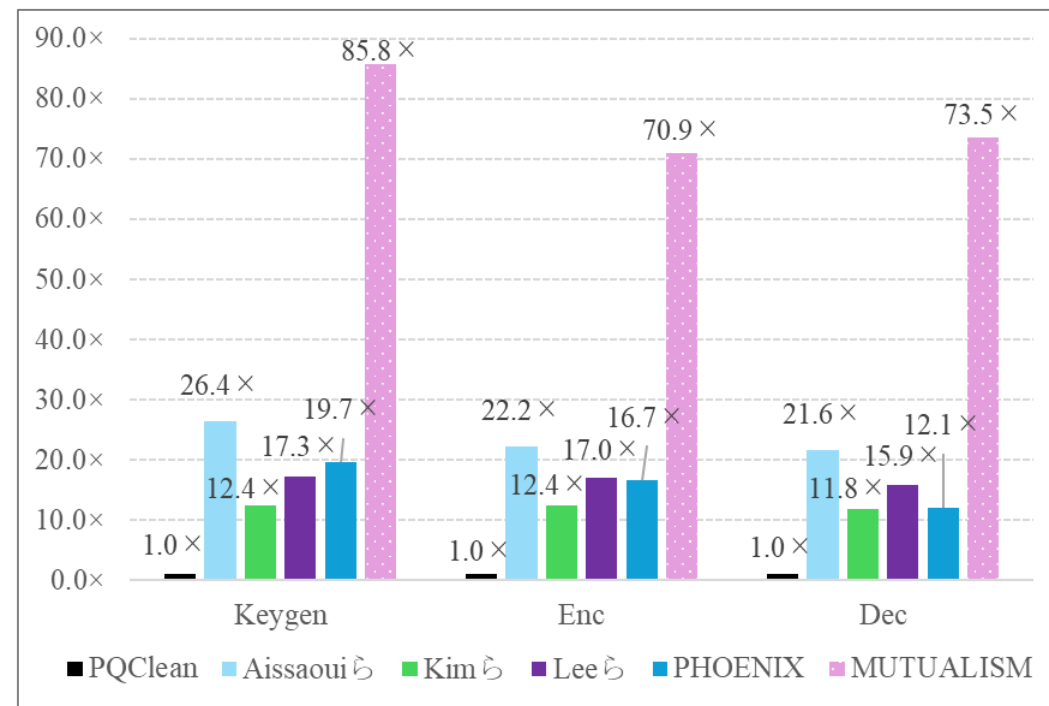
宅内IoT機器のような省リソース機器では動作に課題
→ アカデミア・OSS・民間サービスで解決技術開発が盛ん

HQCに対するメモリ使用量と処理時間削減方式

- C. Liu et. al, “MUTUALISM: Low-Footprint and High-Throughput Software Implementation of HQC for Resource-Constrained Devices”, ACM WiSec2026
- メモリ使用量を約**4~8倍**、処理時間を約**70~85倍**改善



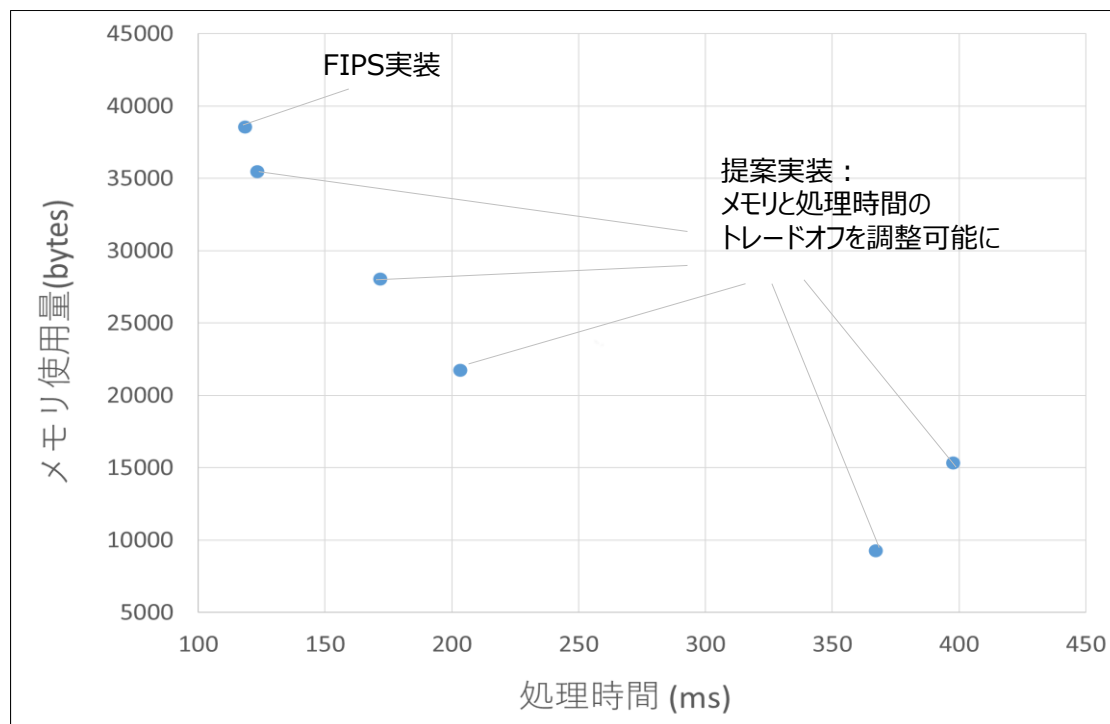
提案方式HQCのメモリ改善倍率



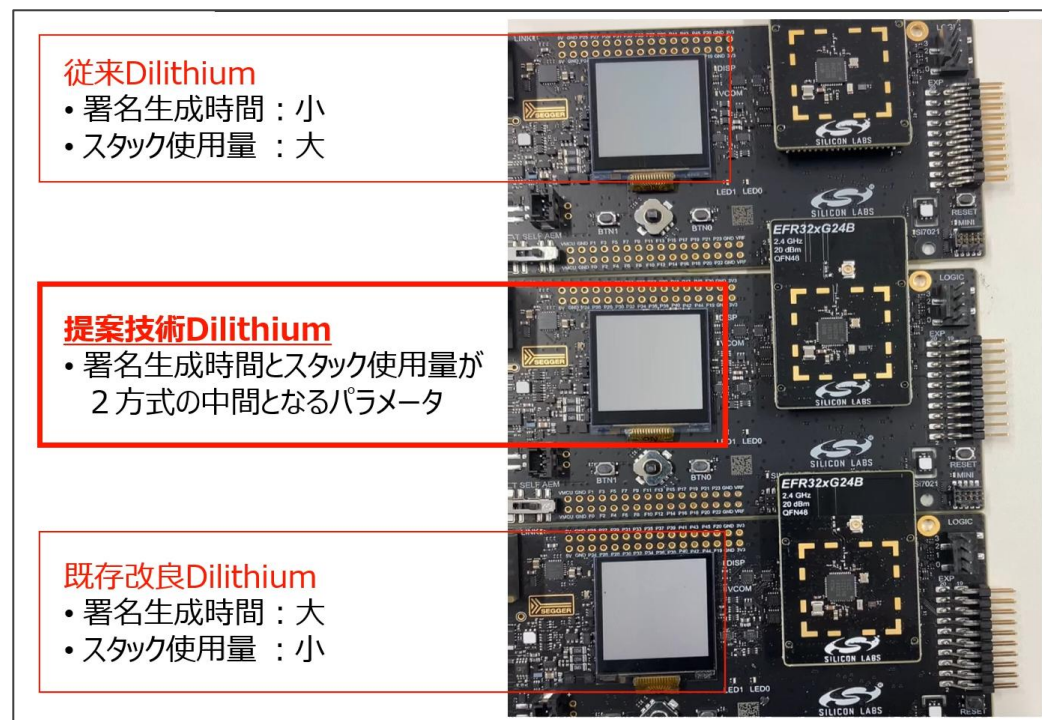
提案方式HQCの処理時間改善倍率

ML-DSAに対する開発処理時間スタック使用量パラメトライズ方式

- Y. Takahashi et. al, “Parameterizing Time-Memory Trade-off for CRYSTALS-Dilithium and Its Flexible Implementation”, IEICE Trans. Info.&Sys., 2025
- メモリ使用量と処理時間のどちらか選択した方を**約4倍改善**



提案方式ML-DSAの処理時間・スタック使用量トレードオフ関係図

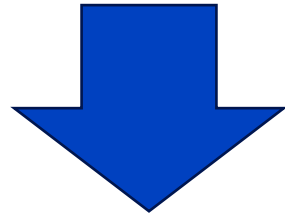


提案手法実装動画

インターネットルーティング分野での PQC移行動向

我々の近年の興味：

**IoT機器の中でも、IoT家電・車載業界では
PQC移行に向けた取り組みが進んでいる**



ネットワークレイヤーはどうだろうか？

DNSSEC

- 議論進行中（進行中ドラフトあり）
- [draft-sheth-pqc-dnssec-strategy-01 - Post-Quantum Cryptography Strategy for DNSSEC](#)
- [draft-fregly-dnsop-slh-dsa-mtl-dnssec-06 - Stateless Hash-Based Signatures in Merkle Tree Ladder Mode \(SLH-DSA-MTL\) for DNSSEC](#)

RPKI

- ドラフト初期段階
- [draft-yoshikawa-sidrops-pqc-rpki-01 - Post-Quantum Signature Algorithm Profile and Migration Considerations for the Resource Public Key Infrastructure \(RPKI\)](#)

BGPSEC・ASPA

- なし

主要学会の論文ピックアップ

- **M. Mellia, SIGCOMM2020**
 - DNSSECに仕様変更なしでPQC導入は不可能
- **S. Bae, ICISC2022**
 - IPsecにPQCを導入実装し、処理時間を詳細評価
- **A. S. Rawat, AsiaCCS2025**
 - PQC署名対応DNSSECは実用的処理時間でない -> PQC鍵交換とMACでPQC-DNSSECを実現

Algorithm	NIST Verdict	Approach	Private key	Public key	Signature	Sign/s	Verify/s
Crystals-Dilithium-II [29]	Finalist	Lattice	2.8kB	1.2kB	2.0kB		
Falcon-512 [31]	Finalist	Lattice	57kB	0.9kB	0.7kB	3,307	20,228
Rainbow- I_a [56]	Finalist	Multivariate	101kB	158kB	66B	8,332	11,065
RedGeMSS128 [16]	Candidate	Multivariate	16B	375kB	35B	545	10,365
Sphincs ⁺ -Haraka-128s [11]	Candidate	Hash	64B	32B	8kB		
Picnic-L1-FS [17]	Candidate	Hash	16B	32B	34kB		
Picnic2-L1-FS [17]	Candidate	Hash	16B	32B	14kB		
EdDSA-Ed25519 [12]		Elliptic curve	64B	32B	64B	25,935	7,954
ECDSA-P256 [12]		Elliptic curve	96B	64B	64B	40,509	13,078
RSA-2048 [12]		Prime	2kB	0.3kB	0.3kB	1,485	49,367

Table 3: Signature algorithms in round three of the NIST competition [3] (security level I). DNSSEC candidate algorithms are shaded gray. Attributes meeting DNSSEC's requirements fully or partially are marked blue or orange, others in pink.

M. Mellia, SIGCOMM2020

Table 2: A comparison between SL-DNSSEC and signature-based DNSSEC methods. SD : Standard DNS (TCP Fallback).

	SL-DNSSEC	DNSSEC over SD	DNSSEC over ARRF/QBF
No TCP fallback	✓	✗	✓
Low bandwidth usage	✓	✗	✗
Fast resolution	✓	✗	✓
DDoS amp. resistant	✓	✓	✗
No network flooding	✓	✓	✗
1 packet sent/recvd.	✓	✗	✗
Reliability	✓	✓	✗

A. S. Rawat, AsiaCCS2025

RPKI,BGPsecではまだ十分に検討されていない

SIDN（＝オランダのトップレベルドメイン .nl のレジストリ運営者）のPQC移行活動は盛ん

- PATADの実装

(関連IETFドラフト: [draft-sheth-pqc-dnssec-strategy-00](#))

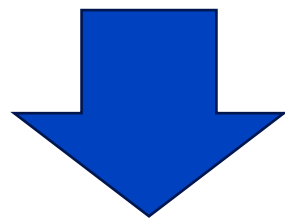
- PQC対応DNSSECベンチマークのためのオープンソースライブラリ
- 動作実験結果：「ハードウェアアクセラレーションを使えば性能影響は限定的」

- RPKIへのPQC対応検討

(関連論文: [PQC for the RPKI | RIPE Labs](#))

- RPKIに適したPQC署名を評価・性能影響の見積もり
->FN-DSAをPQC成分にしたハイブリッドが有望
- サイズと検証時間を削減する改良PQC-RPKI方式を提案
- 既存の移行手順RFC6916は非現実的とし、より良い移行方法を提案

**インターネットルーティングプロトコルのPQC移行活動は途上
まだ十分に検討されていないプロトコルも存在**



**我々の最近の取り組み：
ネットワークプロトコルに対して安全なPQC移行を行いたい！**

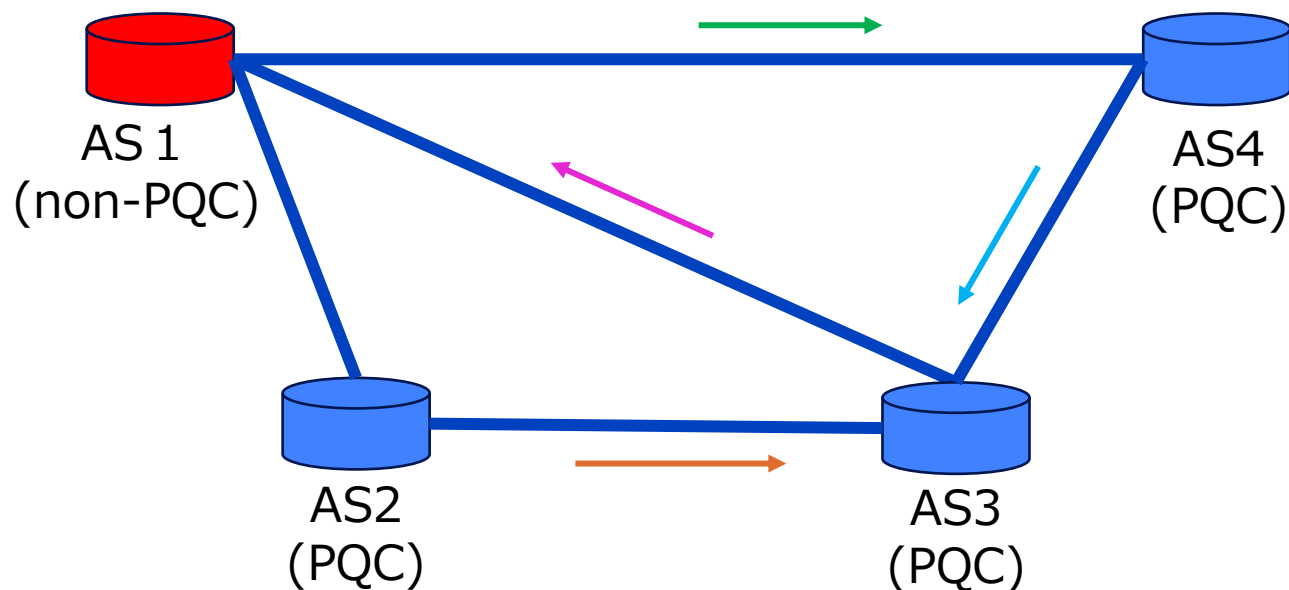
パナソニックのBGPsecに関する PQC移行技術

PQC部分導入時の①BGP経路収束性を評価&②安全な導入方法を提案

- なぜ部分導入を考えるのか？
 - > ASを管理するISPごとにガバメント差、境界ルータのPQC処理リソース不足[Mellia,2020]
 - > PQC対応ASと非対応ASの混在が予想

経路収束性：経路状態が一意の状態に収束する性質

- この性質が満たされると、BGPは安全かつ正常に実行終了



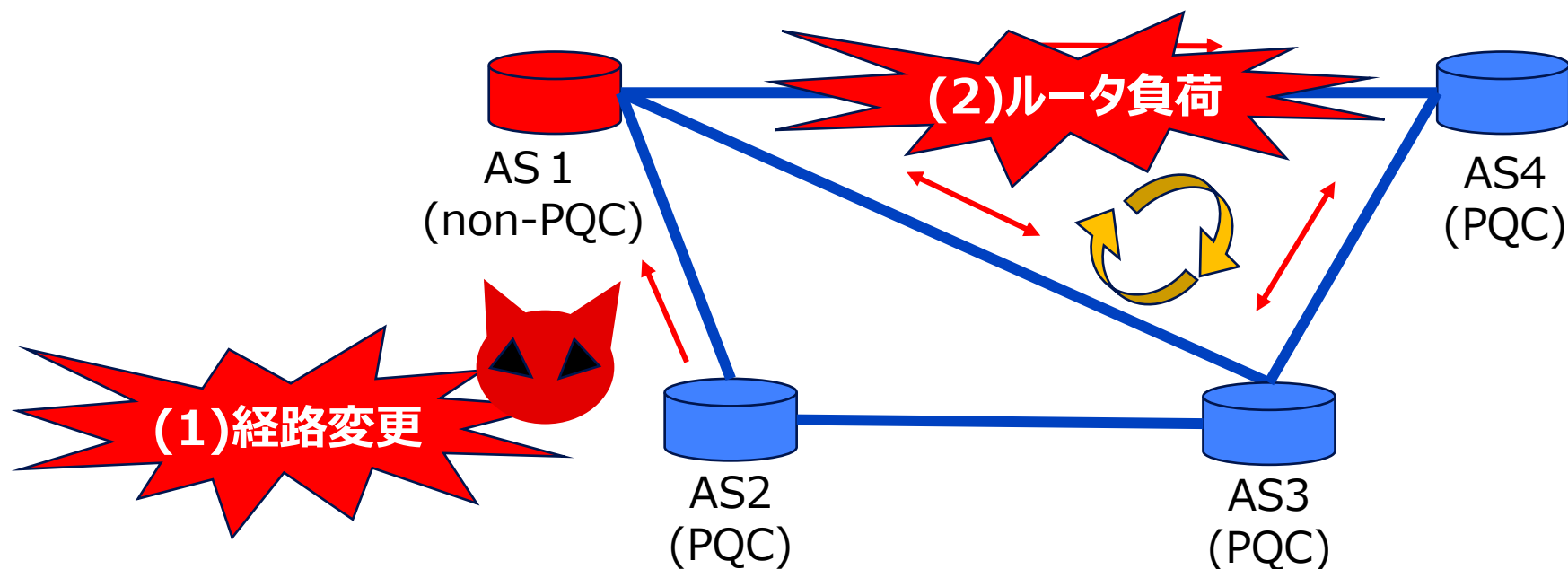
一意に収束
⇒正常終了

経路収束性が満たされていない場合：以下2つのパターンが考えられる

- (1)収束経路が一意でない -> 攻撃者による経路変更攻撃[Maria,2017]
- (2)経路が収束しない -> ルータへの負荷増加[Yang,2022]

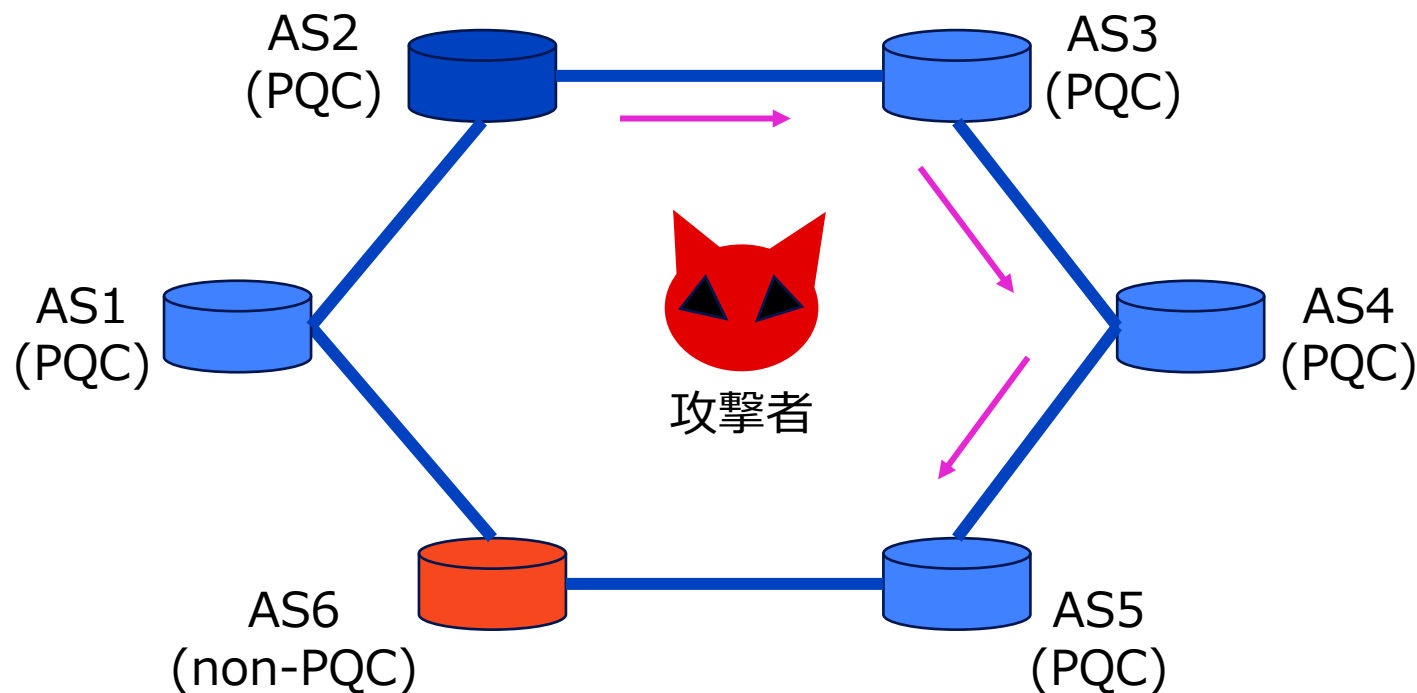
PQC部分導入時に(1)と(2)のそれぞれが起こりうる具体例を発見[*] (今回(1)のみ紹介)

[*]高橋ら,“PQC-BGPsec：耐量子計算機暗号がインターネットルーティングにもたらす影響”, 暗号と情報セキュリティシンポジウム(SCIS), 2026.



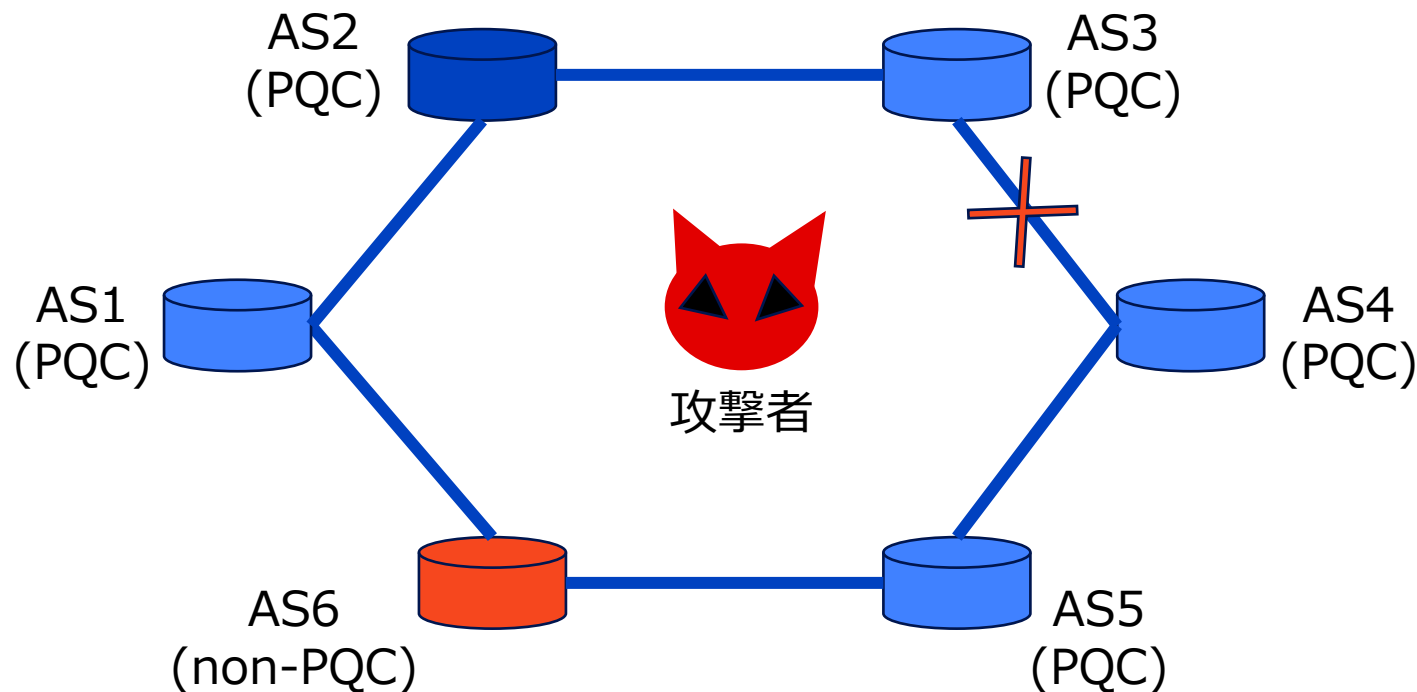
(1)収束経路が一意でない例 = BGP Wedge

- BGP Wedge[Yang, 2022] : ネットワークが接断した際, 意図した安定状態とは別状態に収束する
- PQC部分導入時に、攻撃者は**non-PQCのASを通るような収束経路に変更する攻撃**が可能



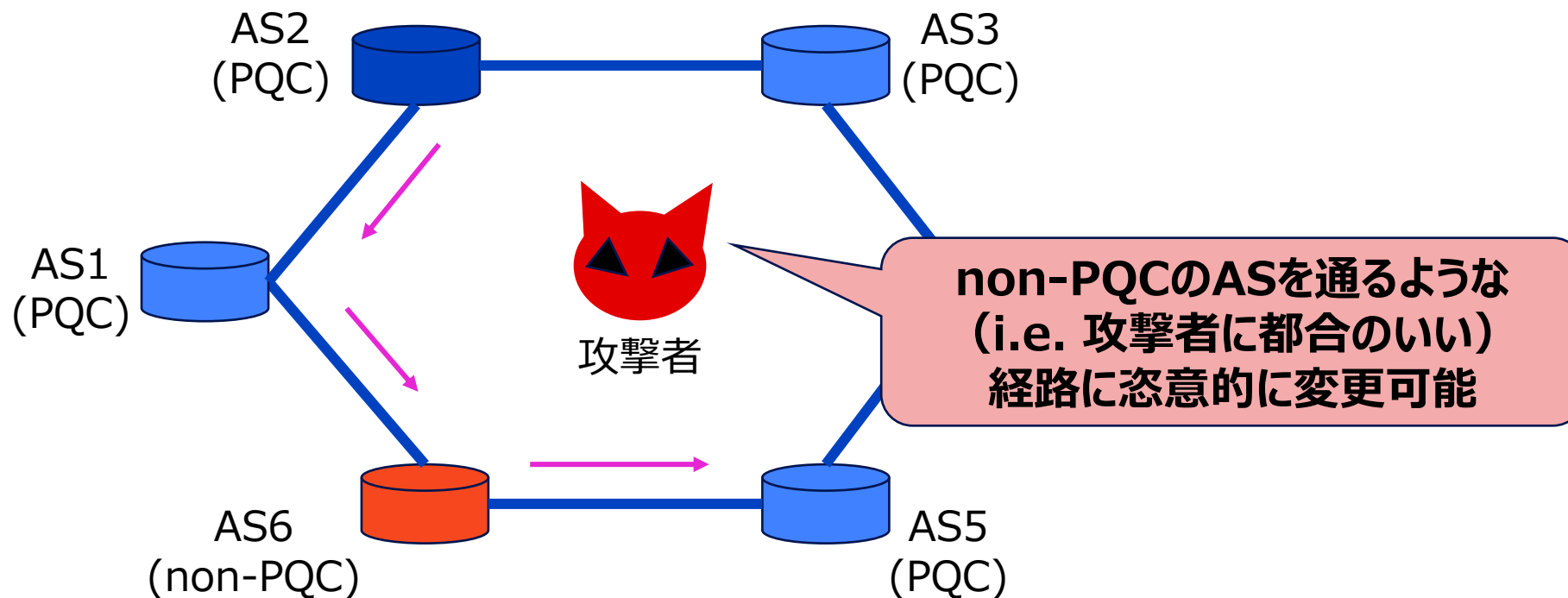
(1)収束経路が一意でない例 = BGP Wedge

- BGP Wedge[Yang, 2022] : ネットワークが接断した際、意図した安定状態とは別状態に収束する
- PQC部分導入時に、攻撃者は**non-PQCのASを通るような収束経路に変更する攻撃**が可能



(1)収束経路が一意でない例 = BGP Wedge

- BGP Wedge[Yang, 2022] : ネットワークが接断した際, 意図した安定状態とは別状態に収束する
- PQC部分導入時に、攻撃者は**non-PQCのASを通るような収束経路に変更する攻撃**が可能

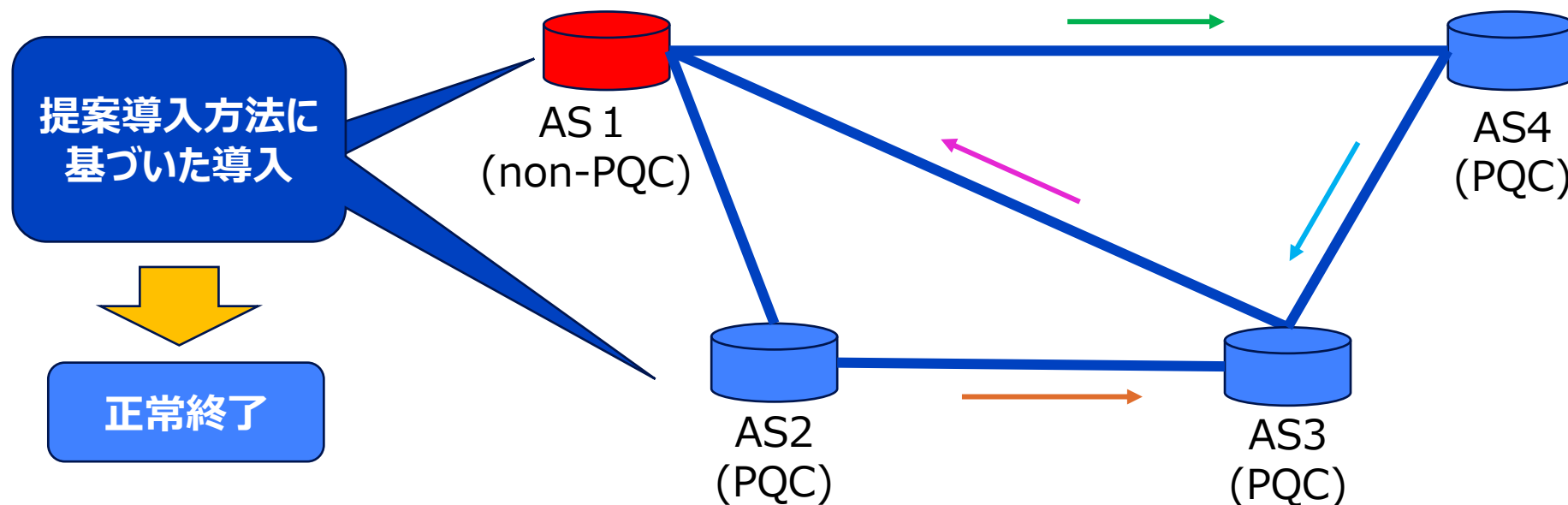


【再掲】経路収束性が満たされていない場合：以下2つのパターンが考えられる

- (1)収束経路が一意でない -> 攻撃者による経路変更攻撃
- (2)経路が収束しない -> ルータへの負荷増加

(1),(2)のそれぞれに対処するPQC導入方法を提案

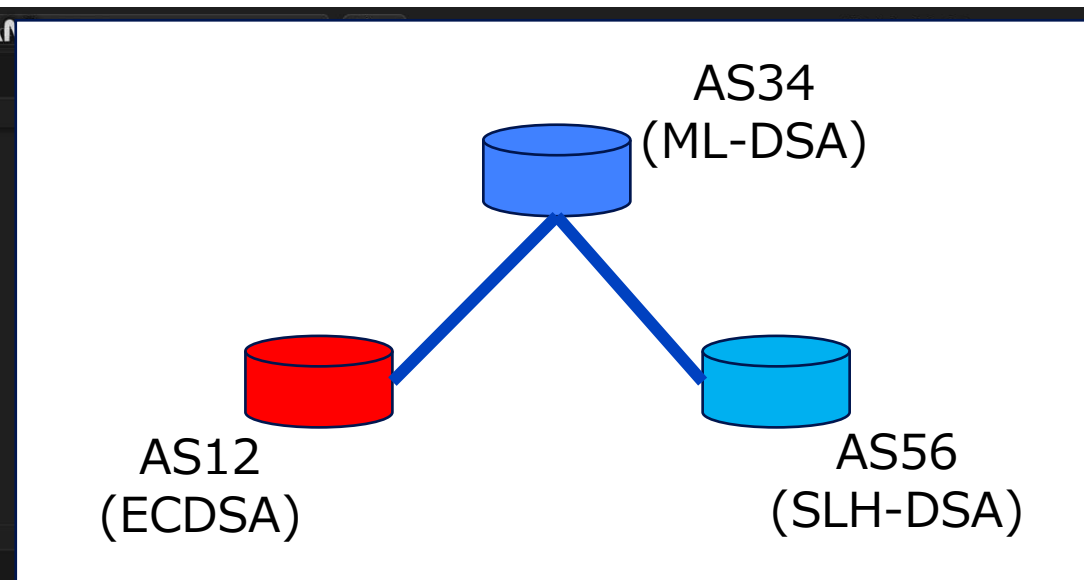
- 提案PQC導入方法を用いれば、一意の経路に収束することを示した



```
! janog.yml
config_mix > ! janog.yml
Asahara.Yoshikatsu, 昨日 | 1 author (Asahara.Yoshikatsu)
1 AS_Setting:
2   12:
3     image: srx
4     sigalgo: ecdsa
5   34:
6     image: srx
7     sigalgo: mldsa44
8   56:
9     image: srx
10    sigalgo: slhdsa-sha2-128f
11 Peer_info:
12   - [12, 34]
13   - [34, 56]
14
```

問題 5 出力 デバッグコンソール ターミナル ポート SPELL CHECKER 5

panasonic@PC-20240220A027:~/work/PQC-BGPsec/BGPsec\$



発表まとめ&議論

本発表のOverview・議論したいポイント

共有したい事実

- PQC移行はすでに複数の国・企業で開始
- 従来暗号とはスペックに差異があり、機器・サービスに影響

我々から伝えたいこと

- PQC移行はセキュリティのためではない、**製品・サービス維持のため**
- 移行には時間がかかることがあるので、**今から優先順位・取り組み開始時期検討**を行うべき

皆さんと議論したいこと

- **ネットワーク事業者はPQC移行にいつから着手すればよさそうですか？**
 - 2030年or2035年に間に合わせるためには、製品ライフサイクルを考えるといつ？
- **ネットワーク分野でのPQC移行において何が課題になりそうでしょうか？**
 - 例) パケットサイズの増大、次世代ルータの処理性能不足など

連絡先 : takahashi.yasushi@jp.panasonic.com

幸せの、チカラに。

