あのネットワーク技術の今と予想する10年後 ～PQC編～

高橋 康（パナソニック ホールディングス株式会社）

JANOG58@サブ会議場3F(第8会議室)
Day1 2026年7月15日(水) 15:45～16:45 (1時間)

Panasonic Digital Transformation & Cyber-Physical Systems Division

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
  - 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・お客様IoT機器のPQC移行に向けた研究開発＆コンサル

宣伝

- 明日も発表します！！

10:15-11:00
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～(45分)
高橋 康(パナソニック ホールディングス株式会社)

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

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

NIST PQC標準選定方式

鍵交換・KEM	電子署名
ML-KEM HQC	ML-DSA SLH-DSA FN-DSA

PQCは暗号研究・標準化の話から
TLS・SSH・IPsec・DNSSEC・RPKIの移行設計の話へ移っている

なぜPQC導入が必要か？

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

- 複数の国・組織で、重要システムでの移行がすでに開始
- 機器認証でも暗号利用の妥当性・更新可能性＝PQC移行可能性は重要要件

PQC移行が必要な理由3選

相互接続性	Chromeブラウザ・Android OSはPQC移行済み
認証・制度	JC-STAR・CRAなどで暗号利用の妥当性・更新可能性が要件
サプライチェーン	米国主導で多くの国・企業でPQC移行が推奨

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？

いつまでに移行すればいいか？

(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**

PQC移行のタイムライン例

期間	運用者がやること
2026–2028	Crypto Inventory、ベンダ対応確認、検証環境準備
2028–2030	重要経路・管理系・証明書系のPoC、調達要件化
2030–2035	本番移行、旧方式縮小、監査・顧客説明

Q2：PQC移行への取り組みを始めていますか？
（方式調査、動作評価などの活動を含む）

各レイヤのPQC移行における影響

領域	IETF進捗状況	増えるもの	NOC/バックボーンへの影響例
SSH	RFC化済み	鍵交換メッセージ、CPU	管理ログイン、NETCONF/SFTP/SCP
TLS	RFC化直前	ClientHello、証明書チェーン、署名検証	装置GUI、API、Telemetry、LB/WAF
IPsec	標準化中	IKE交換サイズ、CPU	拠点間VPN、管理VPN
DNSSEC	実証・ドラフト段階	DNS応答サイズ、署名検証、キャッシュ	UDP断片化、TCP fallback、Anycast/Resolver負荷
RPKI	初期ドラフト	証明書・CRL・CMS object、Validator処理	Repository同期、Validator CPU/メモリ
Router	-	直接影響は限定的な可能性	RTRのVRPモデルが維持されれば影響はValidator側中心

Q3：どのレイヤが一番PQC移行の影響が大きそうですか？

議論したいポイント

共有したい事実

- PQC移行は各プロトコルレイヤでの移行の話にシフト
- 従来暗号とはスペックに差異があり、機器・サービスに影響の可能性

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**

皆さんと議論したいこと

- **PQCの影響は、皆さんのネットワークでは最初にどこへ来るか？**
  - TLS、SSH、IPsec、DNSSEC、RPKI、管理プレーン、顧客向けサービスのどれか？
- **証明書発行者やベンダが明日PQC対応したら、自社はすぐ使えるか？**
  - 使えないとしたら、詰まるのはクライアント、機器、監視、証明書管理、MTU、運用手順のどれか？
- **2030/2035に間に合わせるには、NOCとして何をいつ始めるべきか？**
  - Inventory、検証、ベンダ確認、調達仕様、PoC、本番切替の順番

幸せの、チカラに。

Panasonic Digital Transformation & Cyber-Physical Systems Division

証明書サイズの比較

方式	公開鍵サイズ	署名サイズ
ECDSA P-256	64 B	64 B
ML-DSA-44	1,312 B	2,420 B
ML-DSA-65	1,952 B	3,309 B
ML-DSA-87	2,592 B	4,627 B
Falcon-512	897 B	666～752 B
Falcon-1024	1,793 B	1,280～1,462 B
SLH-DSA-128s	32 B	7,856 B
SLH-DSA-192s	48 B	16,224 B
SLH-DSA-256s	64 B	29,792 B

ネットワークプロトコル・機器スペック上、これは課題になるか？

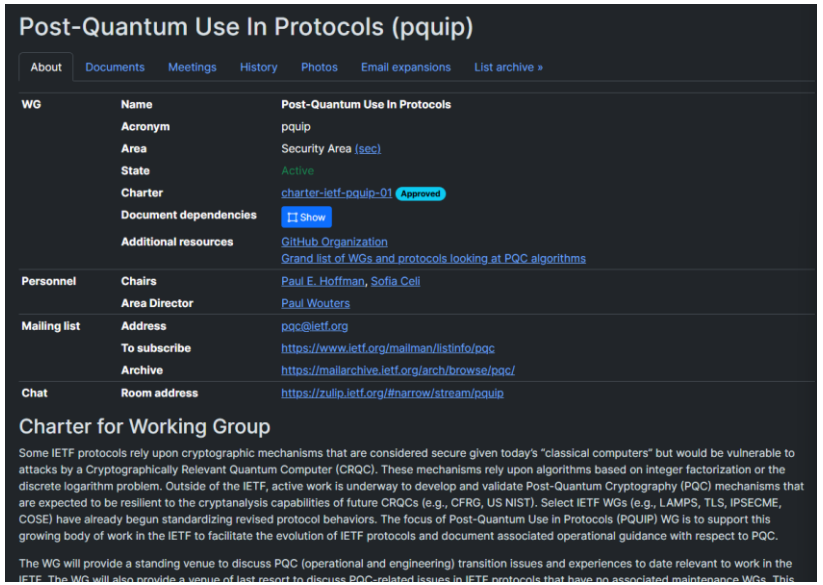
IETFのPQC関連ドラフト・RFC状況

PQC関連WG

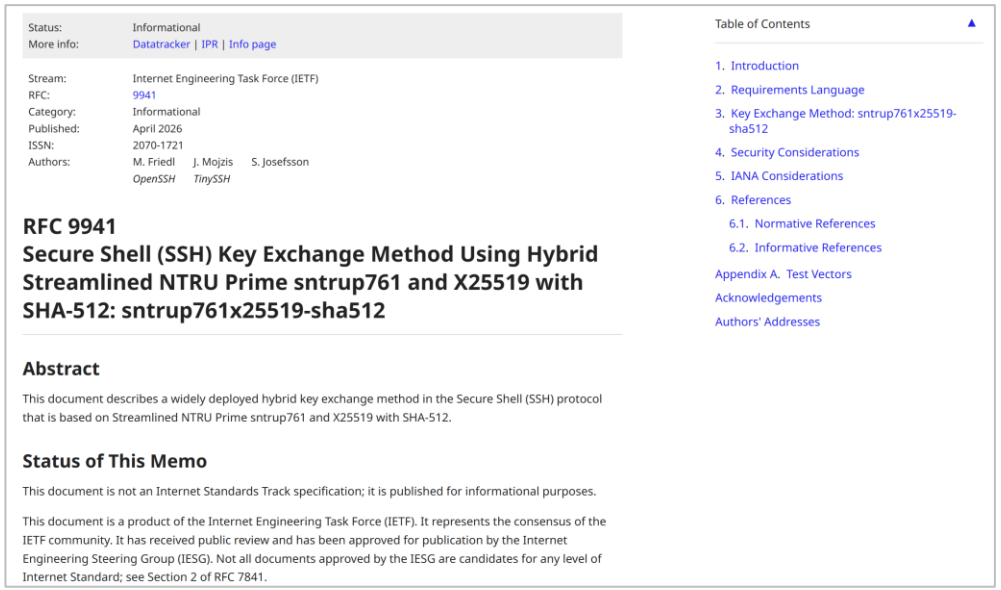
- PQUIP WG：PQC導入・問題対応を集約
  - draft-ietf-tls-ecdhe-mlkem-05 - Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3
  - draft-ietf-tls-mldsa-05 - Use of ML-DSA in TLS 1.3

発行済RFC

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



IETF PQUIP WG



RFC9941

IETFのPQC関連ドラフト・RFC状況

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**

RPKI,BGPsecではまだ十分に検討されていない

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

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はただ一つの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

なぜPQC導入が必要か？

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-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]
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]

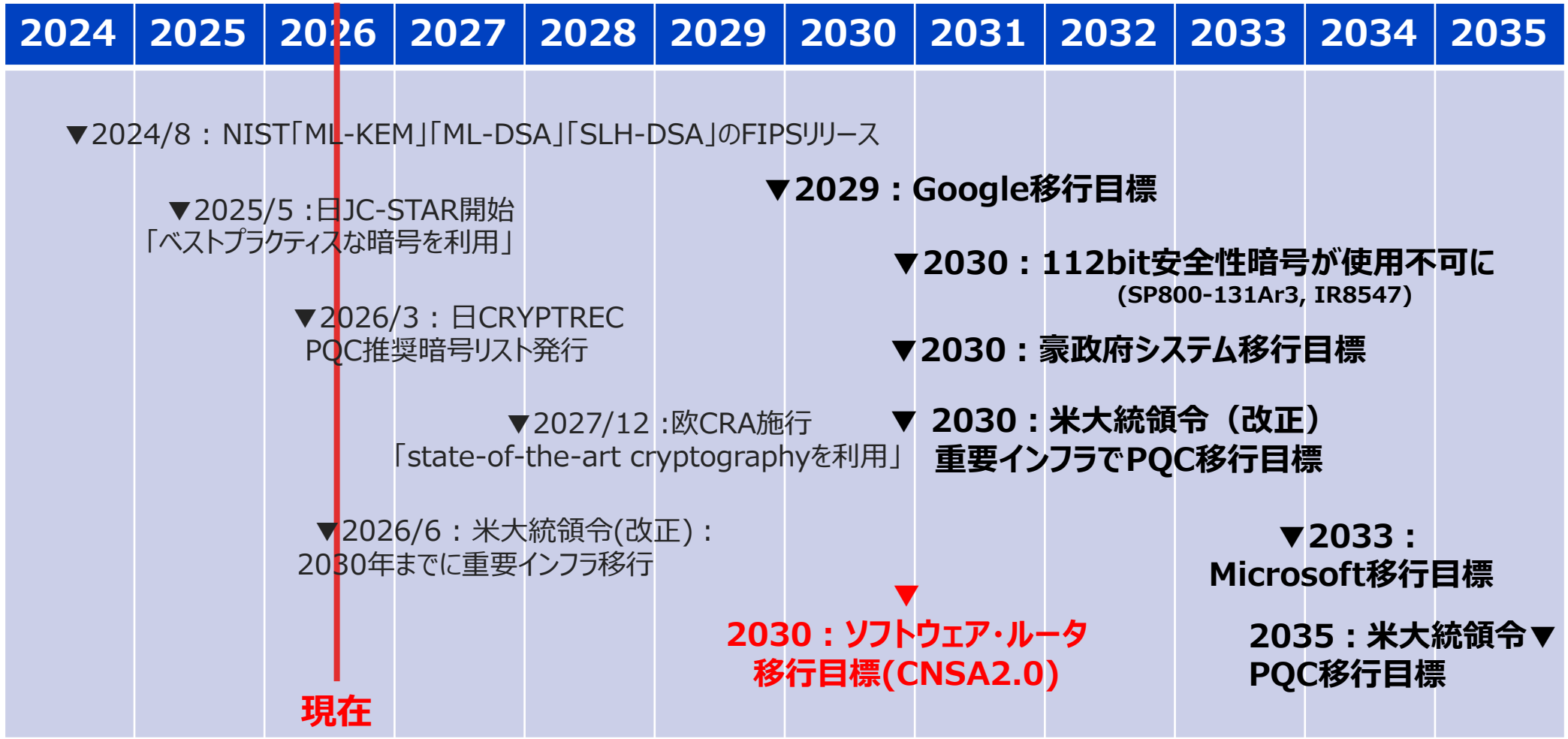
PQC移行開始民間製品・サービス

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？

(私の知る限り)全ての国・組織にて遅くとも2035年が期限

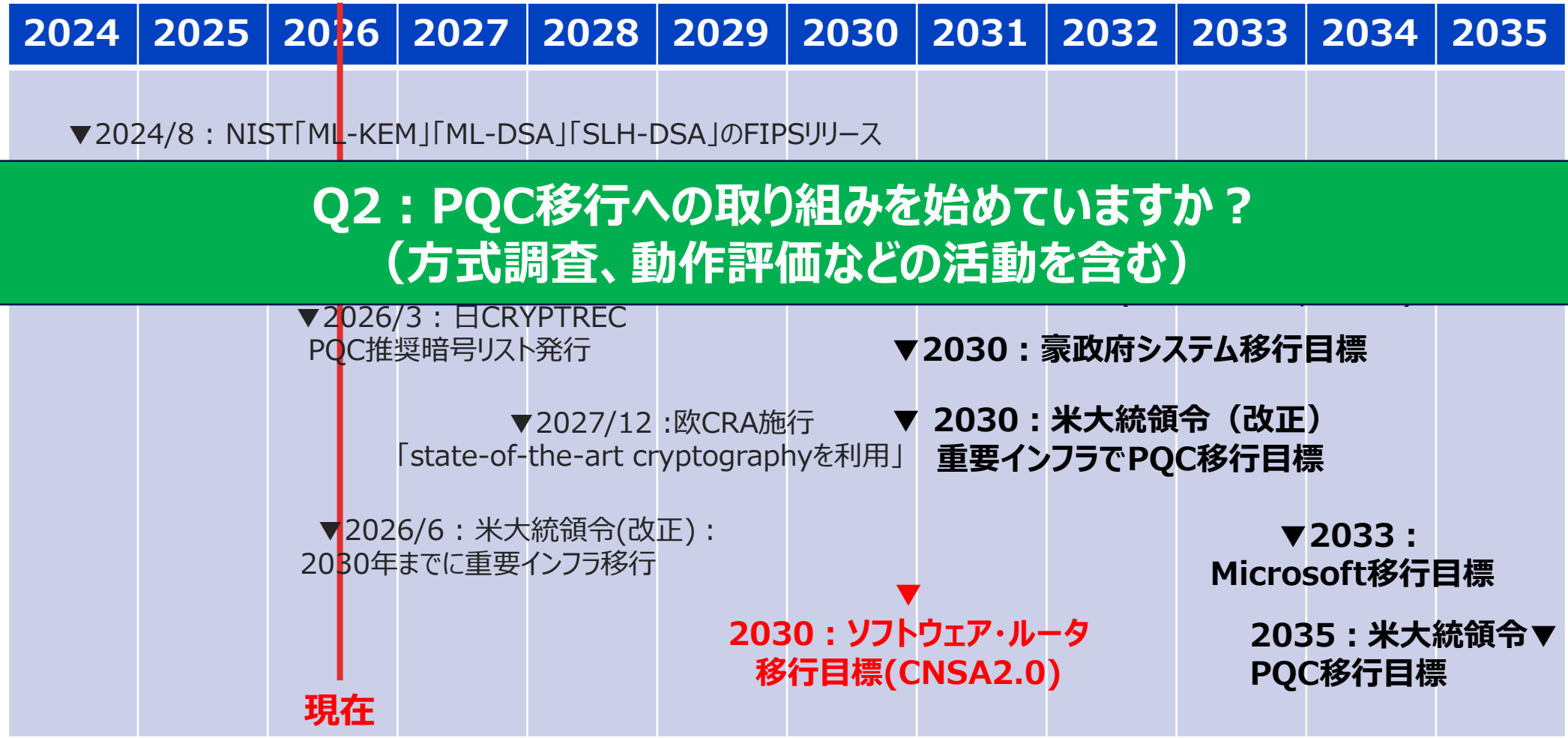
- ただし、重要インフラ・政府システムに限っている国は少なくない
- 最近では、Google・米国が**2030年期限に前倒し**



いつまでに移行すればいいか？

(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**



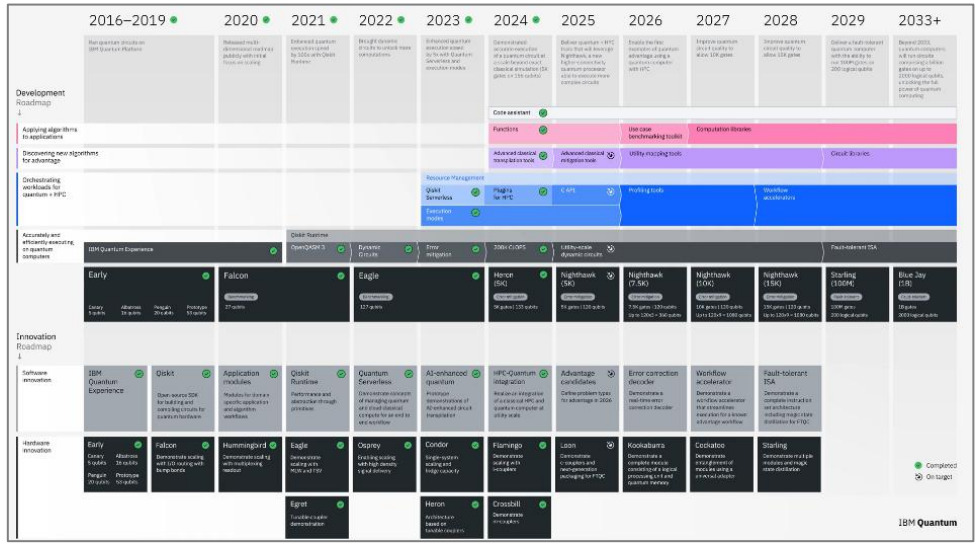
【参考】なぜ2035年->2030年に早まっている？

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

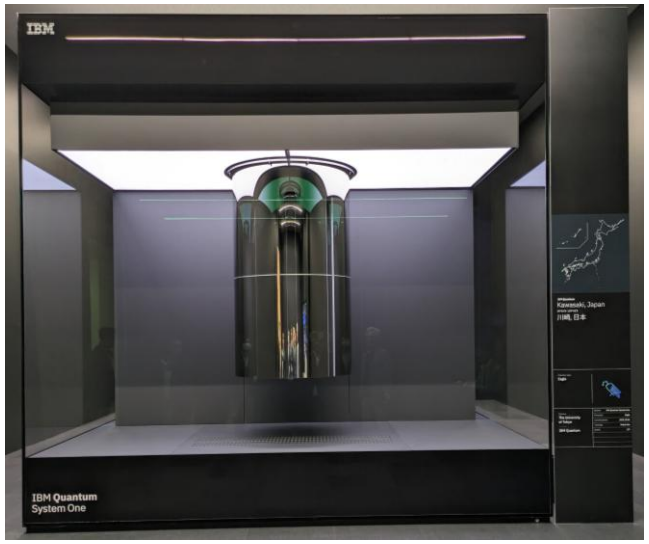
- RSA2048を100万量子ビット未満で解読可能
- ECDSAを1万量子ビット程度で解読可能

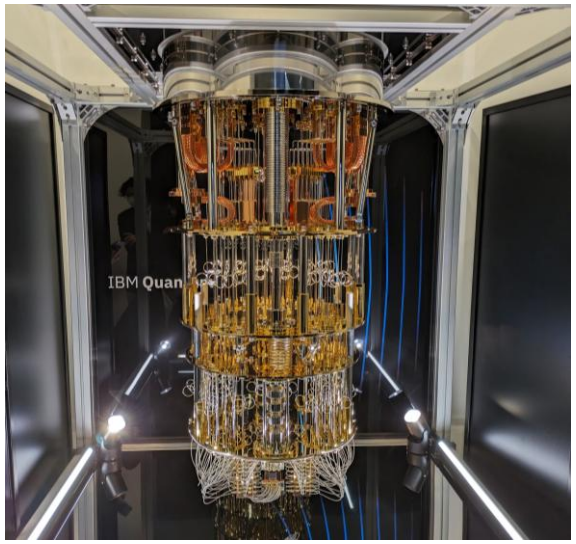
量子計算機の開発見込み

- 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]

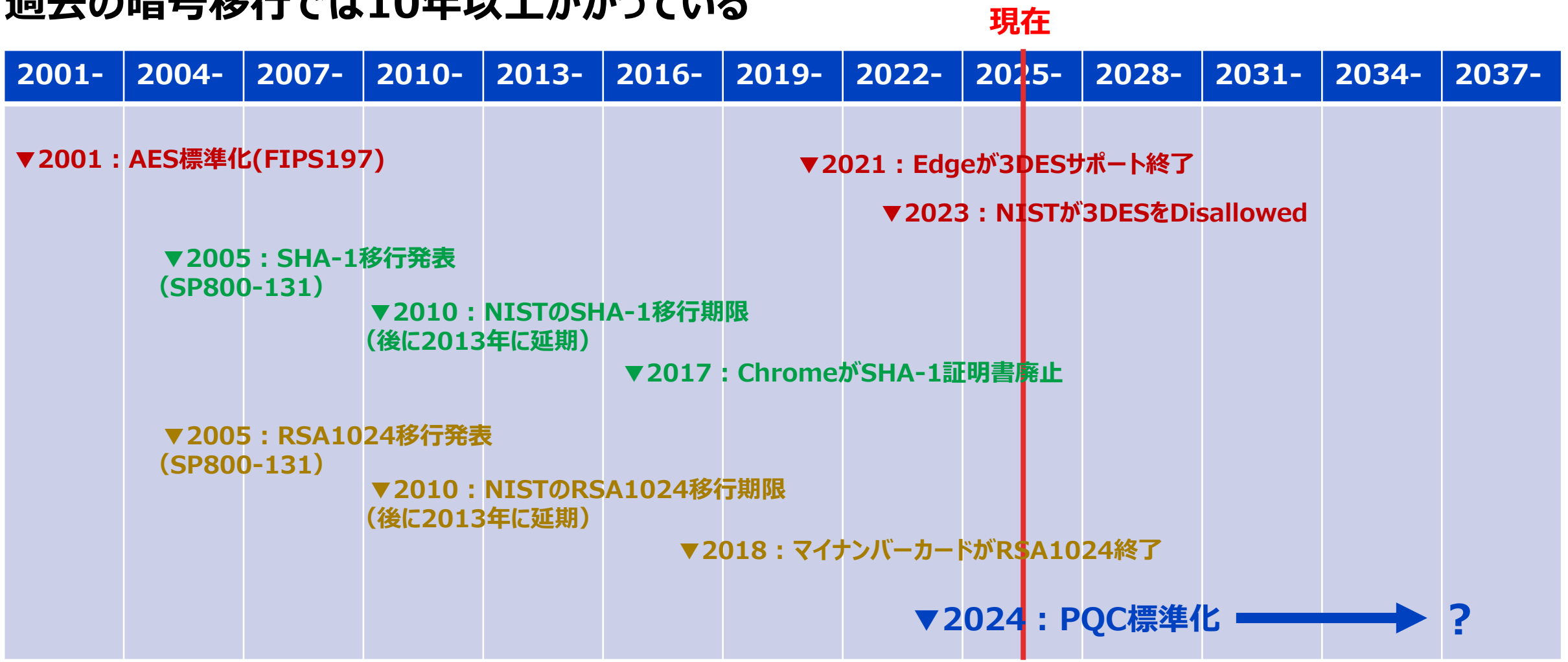




IBM量子計算機@川崎

どのくらい時間がかかるか？

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移行作業フロー

PQC移行に必要な作業概観

準備
- ガイダンス
- 動向共有

資産棚卸
- リスクアセスメント

プランニング
- 移行範囲決定
- 移行計画策定

作業支援
- 最適化ライブラリ提供

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

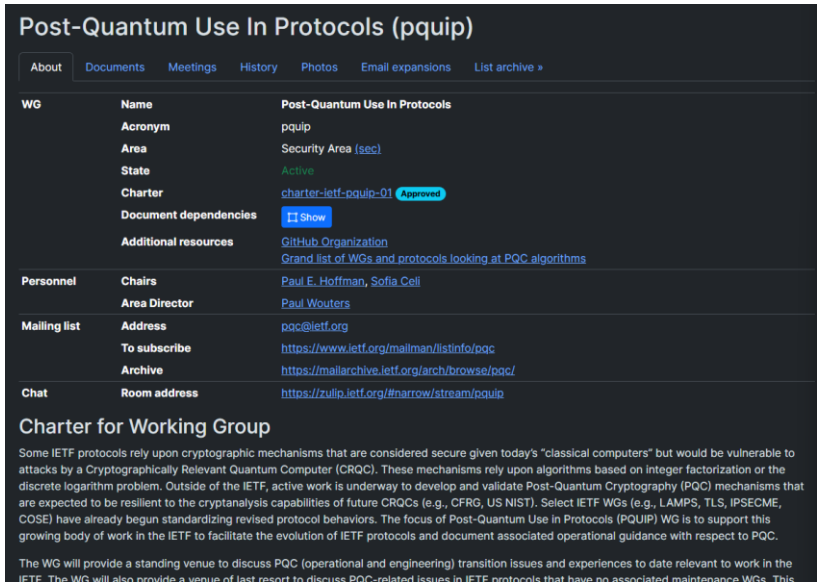
IETFのPQC関連ドラフト・RFC状況

PQC関連WG

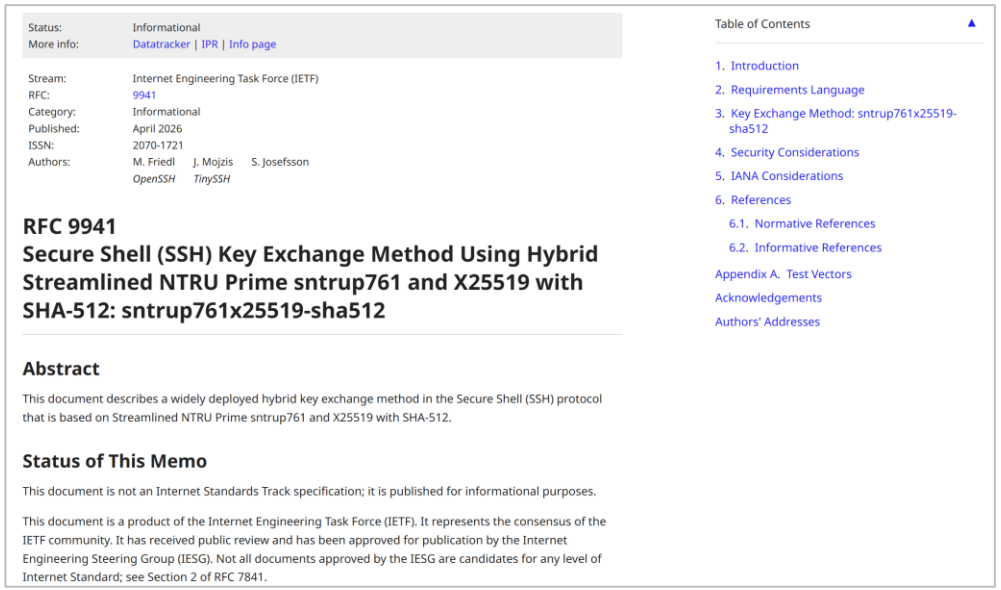
- PQUIP WG：PQC導入・問題対応を集約
  - draft-ietf-tls-ecdhe-mlkem-05 - Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3
  - draft-ietf-tls-mldsa-05 - Use of ML-DSA in TLS 1.3

発行済RFC

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



IETF PQUIP WG



RFC9941

【参考】その他のPQC関連ドラフト・RFC状況

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]

ISO

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

実用上での課題

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きい**（10倍~100倍）

システムへの移行時に予想される課題

- 鍵サイズが大きい　　-> 小セキュア領域機器やICカードへの搭載が困難
- メモリ使用量が大きい -> 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**

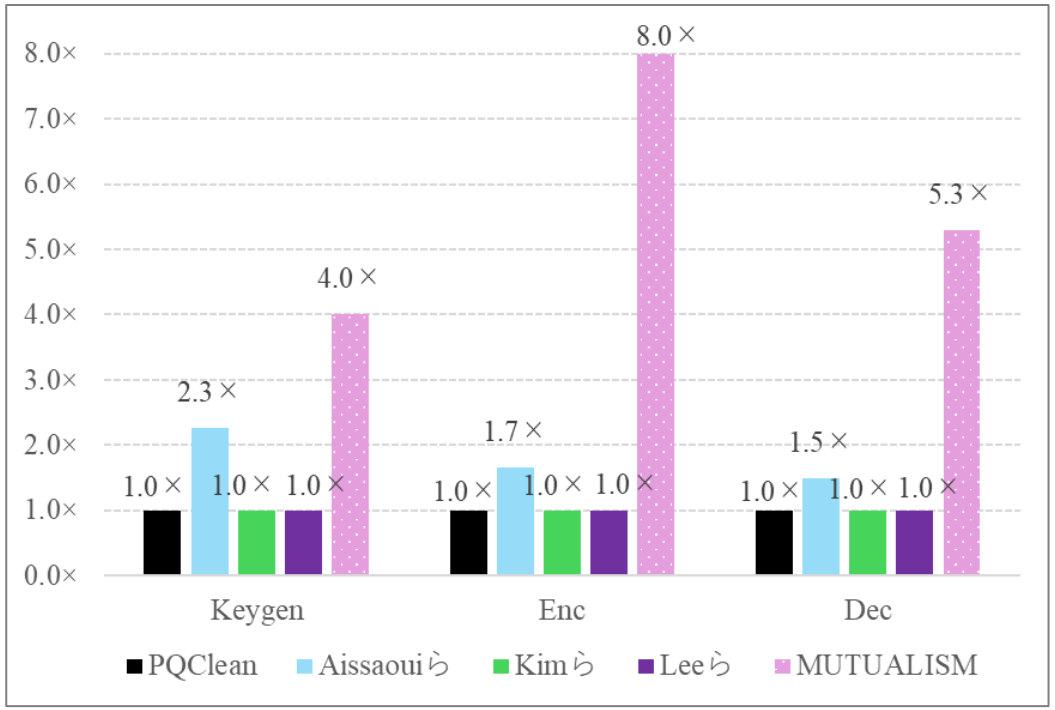
ML-DSAのスタック消費量

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

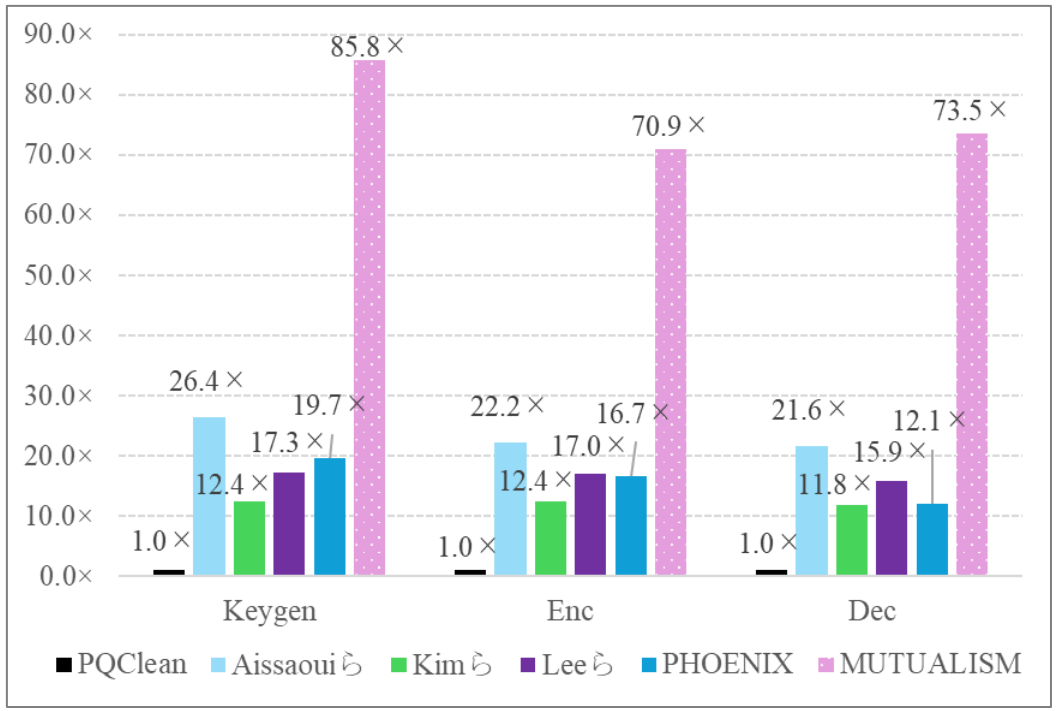
パナソニックのPQC改良技術①：HQC

HQCに対するメモリ使用量と処理時間削減方式

- C. Liu et. all, “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

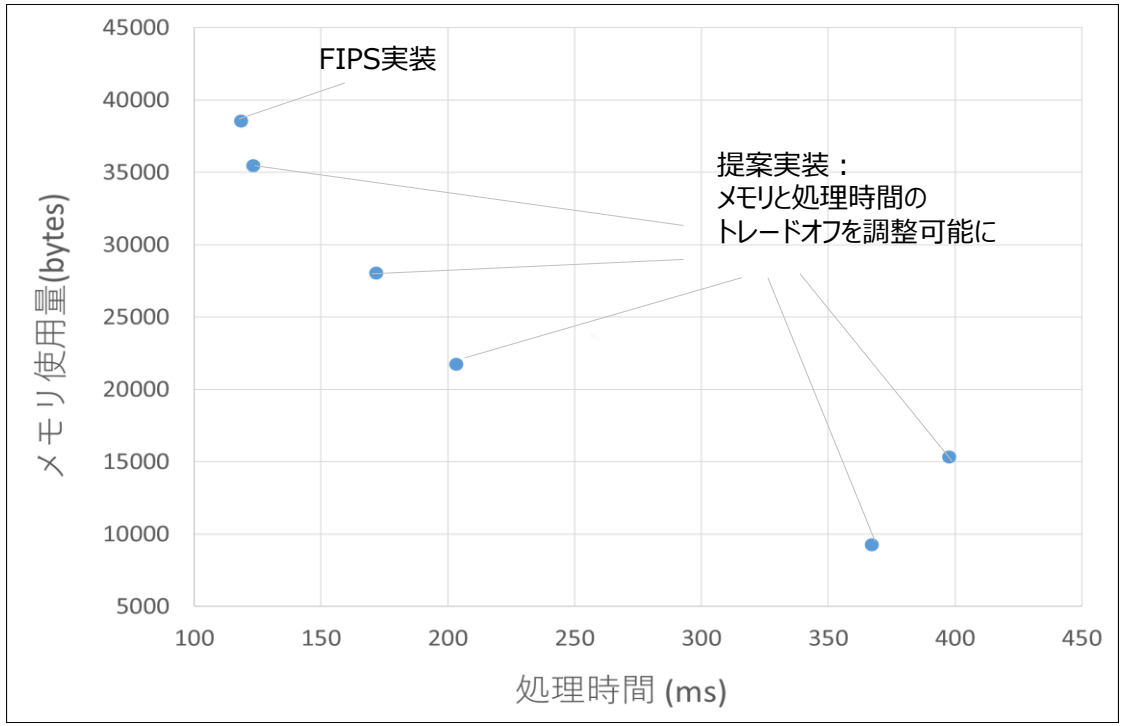


提案方式HQCの処理時間改善倍率

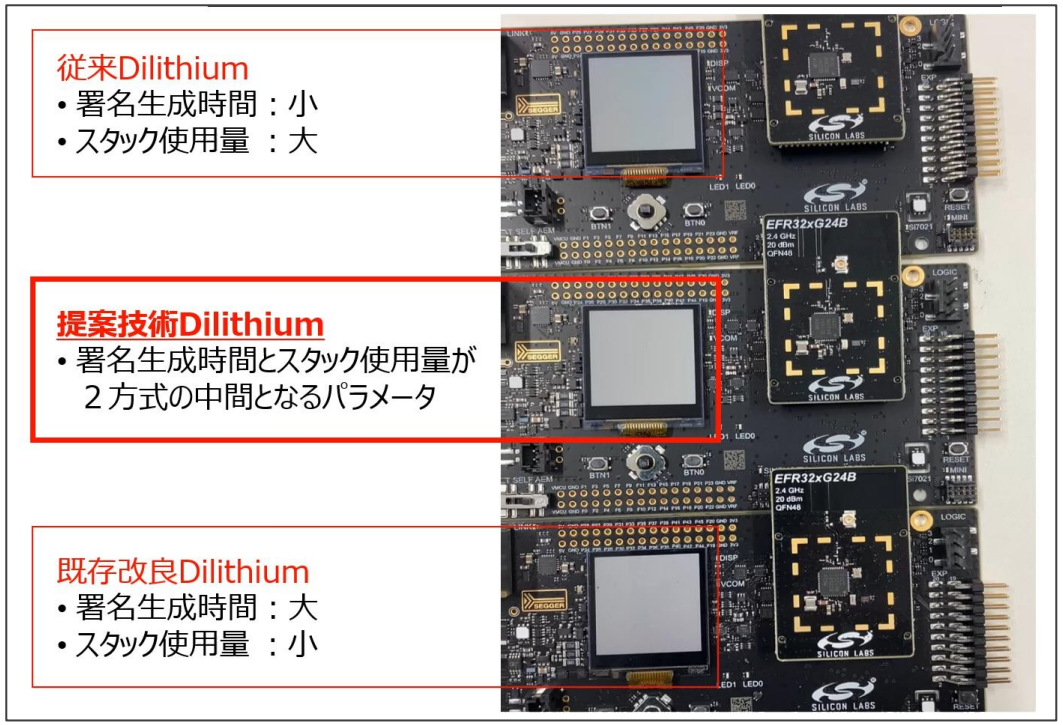
パナソニックのPQC改良技術②：ML-DSA

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

IETFのPQC関連ドラフト・RFC状況

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**

アカデミアレイヤーでのPQC関連研究

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-Ed22519 [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

実用に向けた実装活動

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

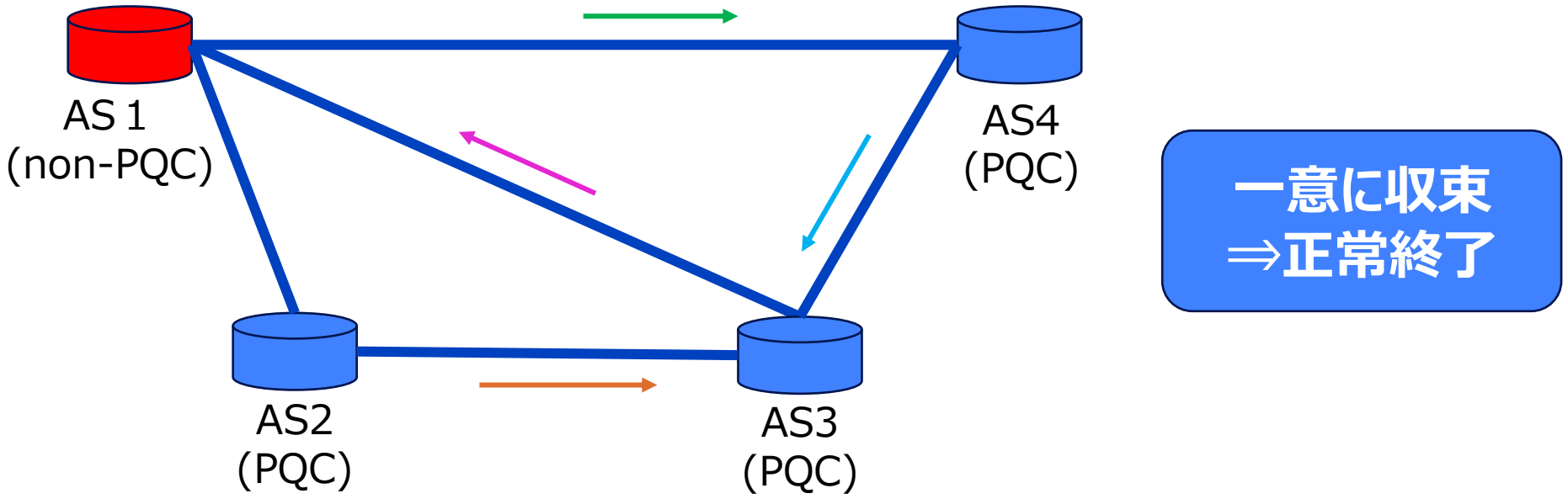
パナソニックのBGPsecに関するPQC移行技術

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



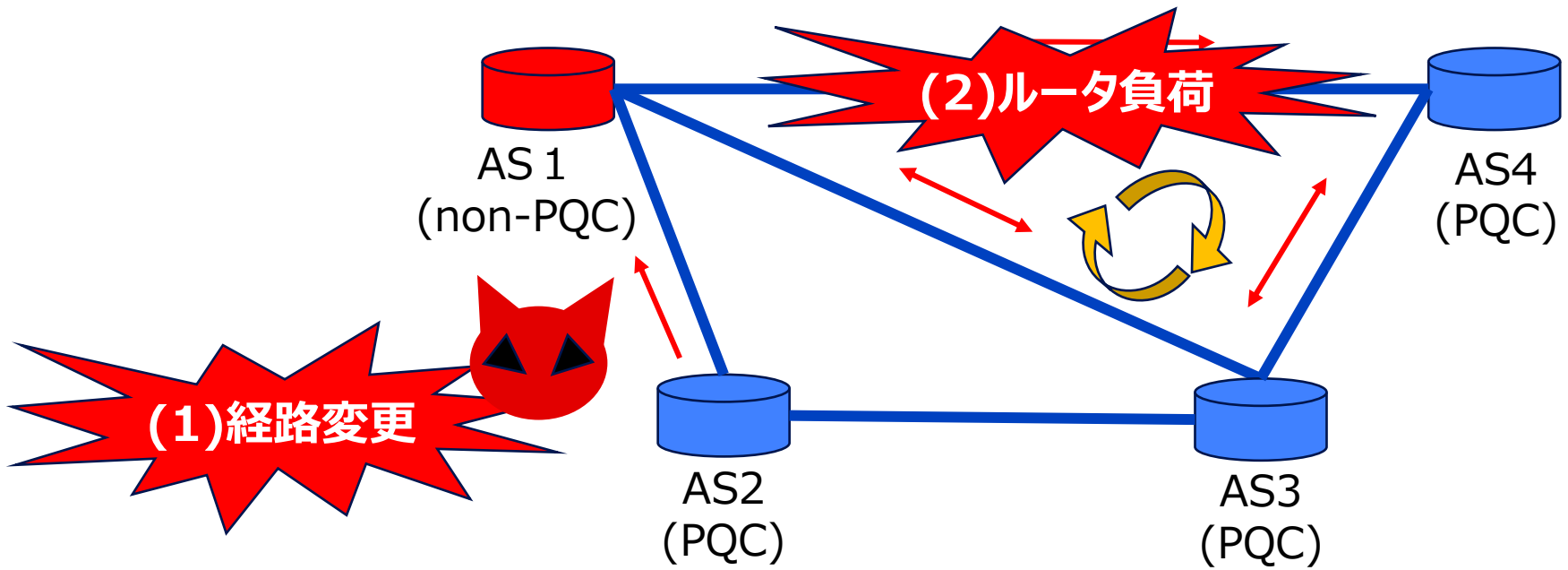
パナソニックのBGPsecに関するPQC移行技術

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）

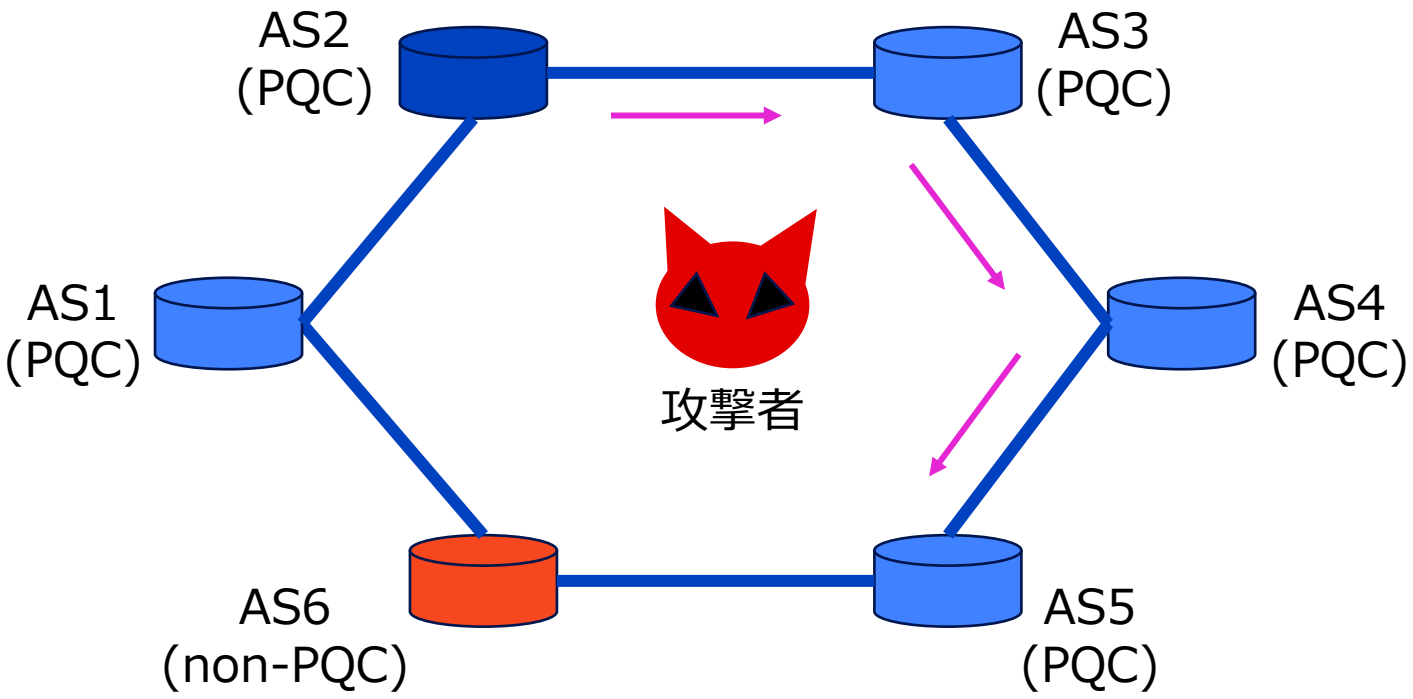
[*]高橋ら,“PQC-BGPsec：耐量子計算機暗号がインターネットルーティングにもたらす影響”, 暗号と情報セキュリティシンポジウム(SCIS), 2026.



パナソニックのBGPsecに関するPQC移行技術

(1)収束経路が一意でない例＝BGP Wedge

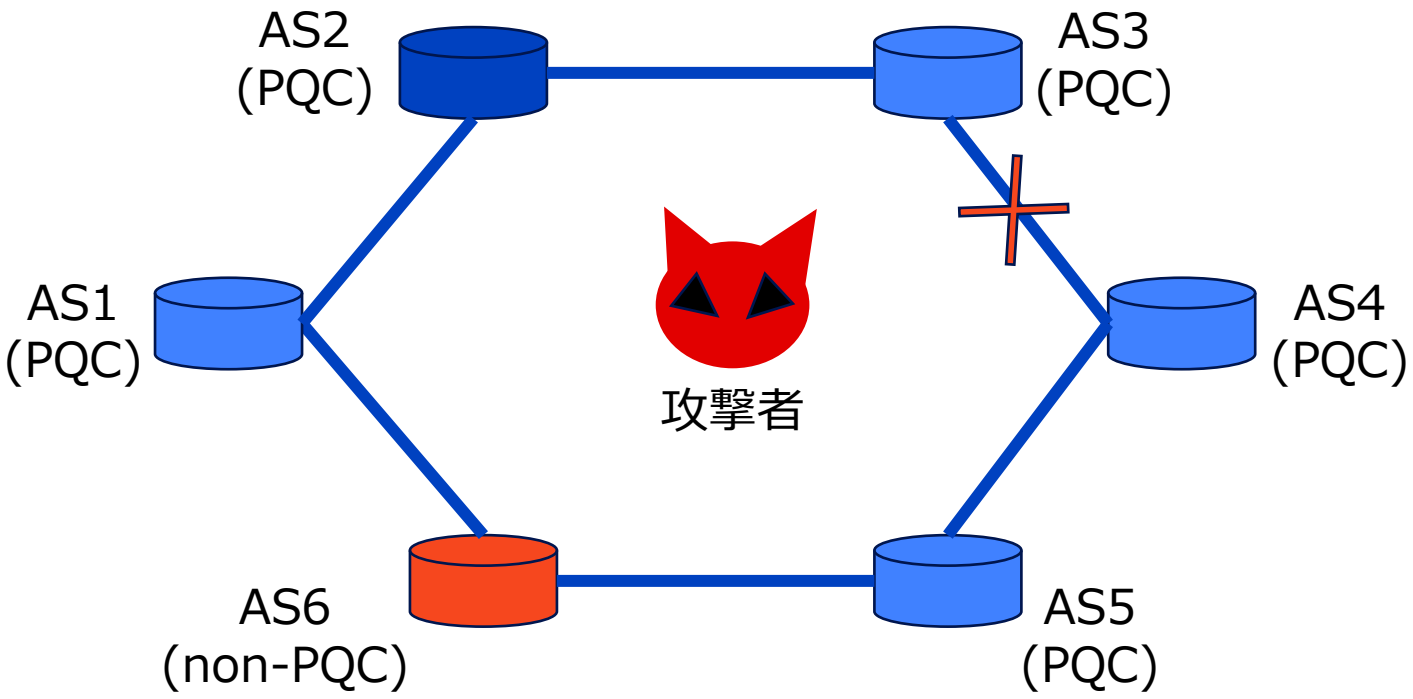
- BGP Wedge[Yang, 2022]：ネットワークが接断した際，意図した安定状態とは別状態に収束する
- PQC部分導入時に、攻撃者は**non-PQCのASを通るような収束経路に変更する攻撃**が可能



パナソニックのBGPsecに関するPQC移行技術

(1)収束経路が一意でない例＝BGP Wedge

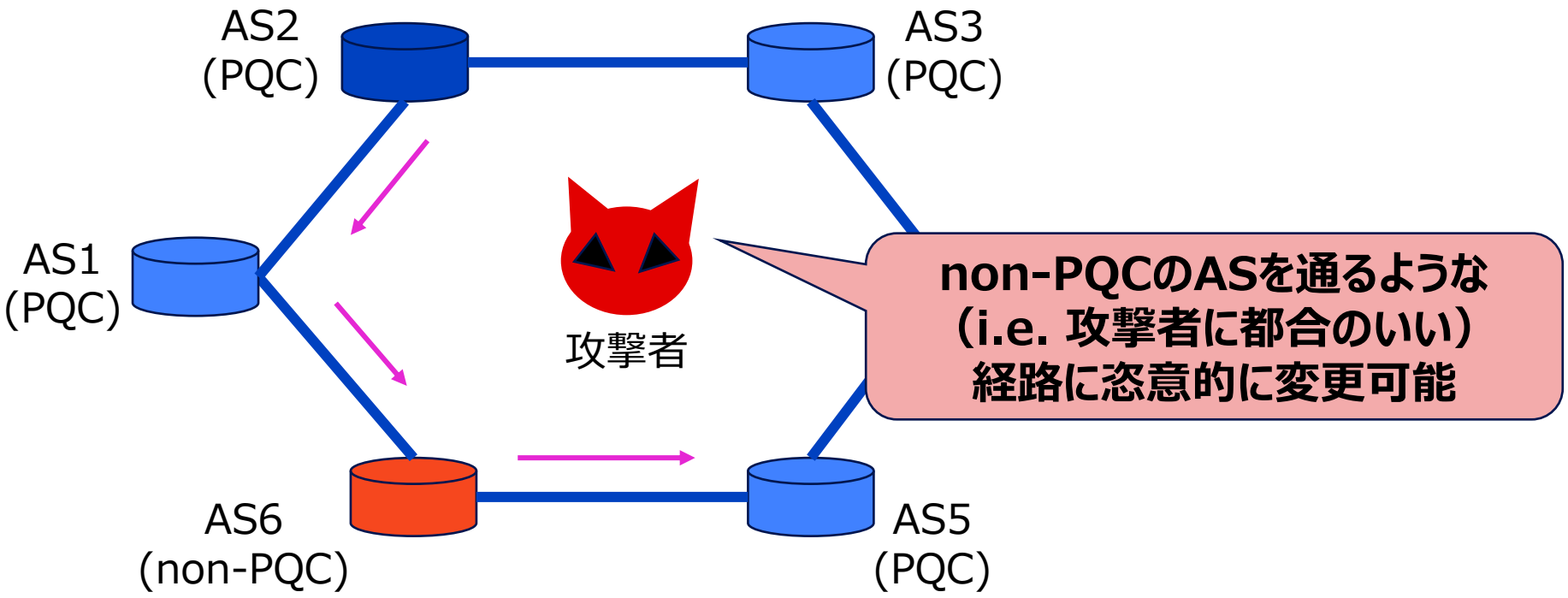
- BGP Wedge[Yang, 2022]：ネットワークが接断した際，意図した安定状態とは別状態に収束する
- PQC部分導入時に、攻撃者は**non-PQCのASを通るような収束経路に変更する攻撃**が可能



パナソニックのBGPsecに関するPQC移行技術

(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



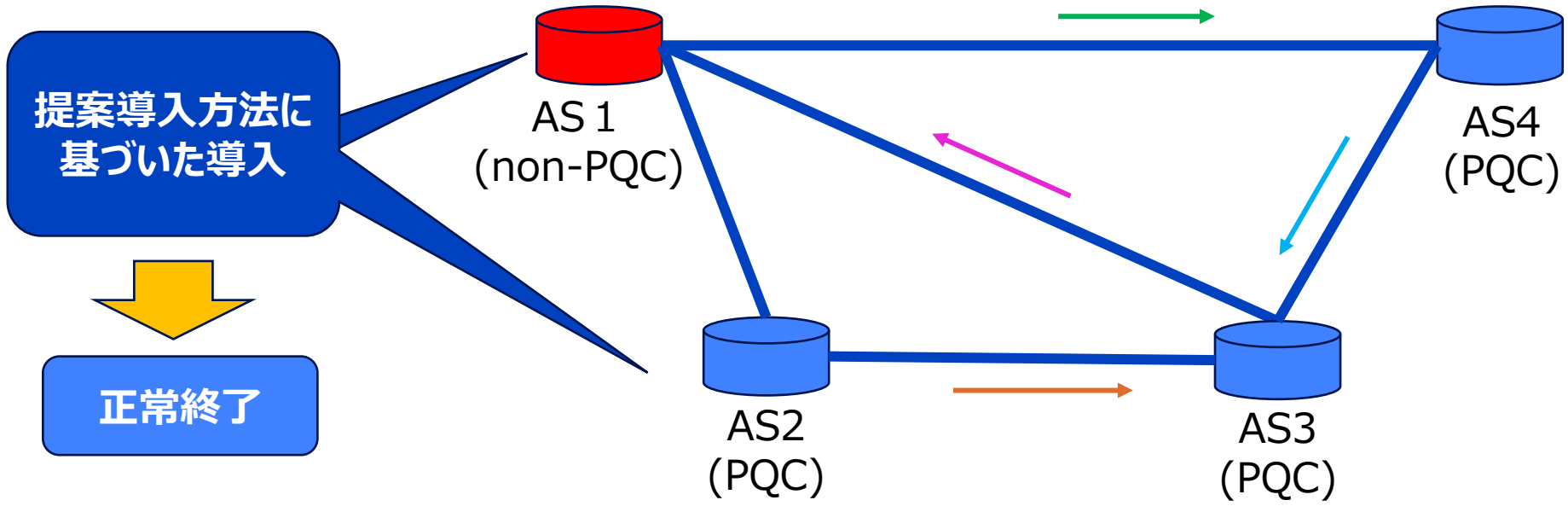
パナソニックのBGPsecに関するPQC移行技術

【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



【動画】PQC対応BGPsecネットワーク構築デモ