量子計算機時代に向けた安全なネットワークの実現 ～耐量子計算機暗号～

高橋 康　（パナソニック ホールディングス株式会社）
矢内 直人（パナソニック ホールディングス株式会社）

JANOG57@本会議場3（グラングリーン大阪北館5F 5-1 in 大阪・梅田）
Day3 2026年2月13日(金) ~~13:40～14:40~~ 14:00～15:00 (1時間)

Panasonic Digital Transformation & Cyber-Physical Systems Division

自己紹介（高橋 康）

所属：

- **パナソニックホールディングス株式会社**

  DX・CPS本部 デジタル・AI技術センター セキュリティソリューション部 2 課

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２回目（前回が初参加）

現在の業務内容

- 弊社IoT機器（宅内家電など）を対象にPQC動作評価・規格調査
- IoT機器への適用課題を抽出＆解決技術を開発
- 知財出願、論文投稿、プロトタイプ実装、など

趣味

- ポケカ、将棋 (見る将)、最近マイクラを始めました

自己紹介（矢内 直人）

所属：

- **パナソニックホールディングス株式会社**

  DX・CPS本部 デジタル・AI技術センター セキュリティソリューション部 2 課

経歴

- 2014年–2023年：大阪大学
- 2024年–現在：パナソニックホールディングス株式会社

学位論文は暗号の研究、阪大時代はセキュリティの研究を幅広く実施

現職では暗号に関するR&D業務を担当

JANOG参加は4回目

現在の業務内容

- 暗号技術のプロジェクトマネジメント
- テーマ問わず社内メンバの研究指導
- 各種国プロの獲得と主導

趣味

- 研究

議論ポイント

PQCについて知っていましたか？

2035年までにPQC移行を推奨されていることを知っていましたか？

PQC移行に着手されていますか？

されている　ー＞いつから着手していて、どのくらい移行が進んでいますか？

されていない ー＞PQC動向のキャッチアップはされていますか？

いつから着手するという予定はありますか？

PQC移行において課題になりそうなことは何でしょうか？

（例えば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）

このセッションの進め方

PQCとは何か

- 量子計算機による危殆化 -> PQC
- ハイブリッド方式

PQC移行動向

- 米国、欧州、日本、IETF活動動向

パナソニックのPQC技術開発

- IoT機器向けPQC改良技術開発
- PQC対応SSL/TLSライブラリ実装

インターネットルーティングプロトコルのPQC移行動向

- IETF活動動向、SIDNの活動、関連論文

パナソニックのBGPsecに関するPQC移行技術

- PQC部分導入時の①経路収束性を評価＆②安全な導入方法を提案

質疑＆議論

PQCとは何か

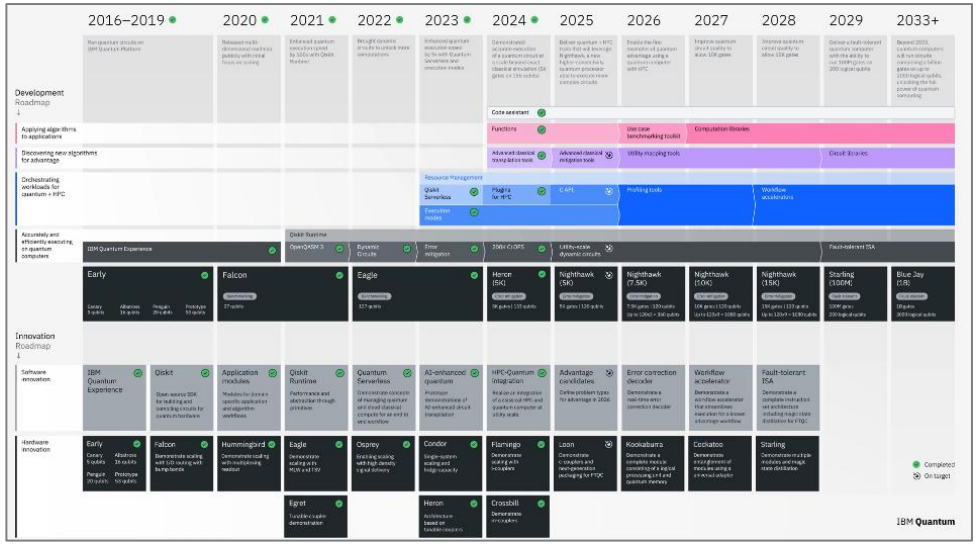
PQCとは何か

量子計算機

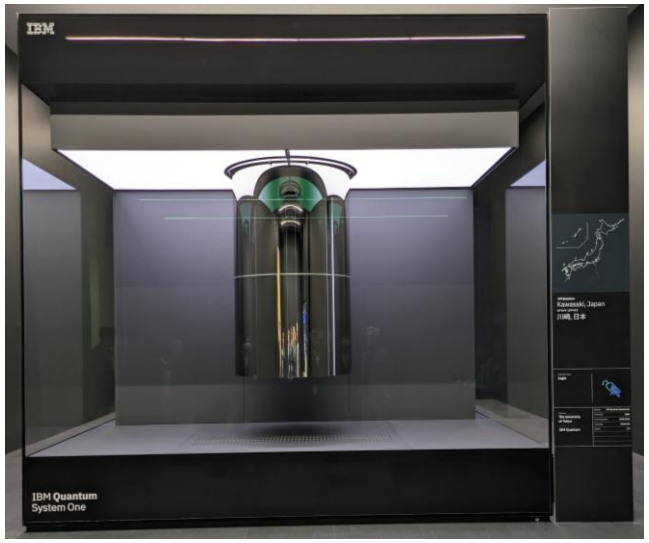
- 量子現象を利用した次世代計算機
- 一部の計算問題を**従来計算機（＝古典計算機）よりも高速に解ける**
- 世界的に量子計算機の開発が活発（例：1121-qubit計算機をIBMが開発）

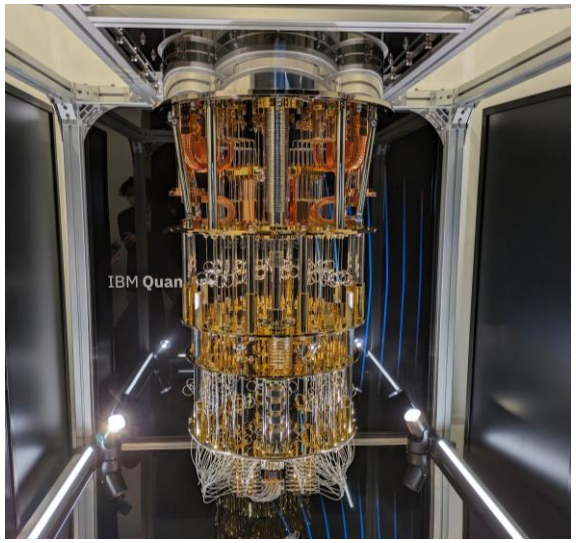
公開鍵暗号の危殆化

- 実用的な量子計算機があれば、現在使用されている**公開鍵暗号（RSA,ECDSA）を解読可能**
- 2030年までにRSA2048が破られるかも？[Quantum Briefing Note]



2025 IBM Quantum Roadmap update - IBM Mediacenter





IBM量子計算機@川崎

PQCとは何か

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

- 量子計算機の計算能力に耐えうる公開鍵暗号
- 世界的にPQCへの標準化・移行準備が進んでいる（∵システムの**暗号移行には長期間かかる**ため）

鍵交換	署名
ML-KEM (FIPS 203)	**ML-DSA** (FIPS 204)
	FN-DSA (2026年発行予定)
HQC (2027年発行予定)	**SLH-DSA** (FIPS 205)

NISTPQC標準選定方式

RSA暗号に対する推奨鍵長の変遷

PQCとは何か

ハイブリッド方式

- PQCと従来暗号を組み合わせることで、いずれか一方が危殆化した際にも安全な方式
- 鍵交換ではRFC発行済みで実用化
- 署名では**複数の実現方式が乱立**（一部IETFドラフトlast call）
- 国ごとにも推奨する温度感が異なる（独仏は明確に推奨、ETSIは使用許可）

実現方式	相互接続性	ダウングレード耐性	証明書サイズ
カメレオン	高	低	大
マルチ	高	低	小
コンカチネーション	低	高	小
ネスト	低	高	小
フュージョン	低	高	大

ハイブリッド証明書スペック比較

議論ポイント

PQCについて知っていましたか？

2035年までにPQC移行を推奨されていることを知っていましたか？

PQC移行に着手されていますか？

されている　ー＞いつから着手していて、どのくらい移行が進んでいますか？

されていない ー＞PQC動向のキャッチアップはされていますか？

いつから着手するという予定はありますか？

PQC移行において課題になりそうなことは何でしょうか？

例えば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移行動向

PQC移行動向

PQC標準化は米国が先導、近年欧州・英国・豪州も動きが活発に

- 国や組織によって移行期限が異なる（**2030年の国も！**）

2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035

▼**2022/5**：米大統領令(ジョー・バイデン大統領がPQC移行に関する大統領令に署名)

▼**2024/8**：NIST FIPS発行（3つのPQC標準方式「ML-KEM」「ML-DSA」「SLH-DSA」をリリース）

▼**2024/10**：NIST SP800-131Ar3を発行 （**2035年**までに移行を推奨）

▼**2025/3**：英NCSC 移行タイムライン発行（**2035年**までに移行）

▼**2025/11**：内閣官房NCO（原則**2035年**をめどに移行）

▼**2025/12**：豪ASD ガイドライン発行（**2030年**までに移行）

▼**2025/6**：欧州委員会 PQC移行ガイドラインを発行（**2035年**までに移行）

▼
2030：112bit PKI Deprecated
(SP800-131Ar3, IR8547)

▼
2030：ソフトウェア・ルータ
移行目標(CNSA2.0)

現在

▼
2035：米大統領令
PQC移行目標

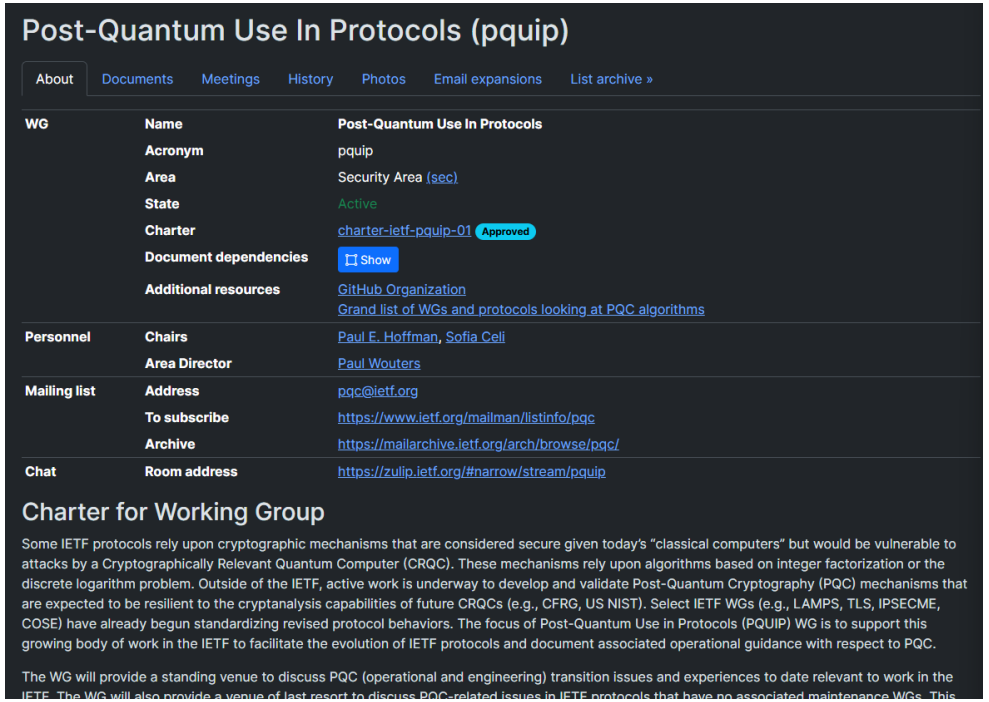
▼
2035：米NSA移行目標

▼
2035：ブラウザ・クラウド
サービス移行目標
(CNSA2.0)

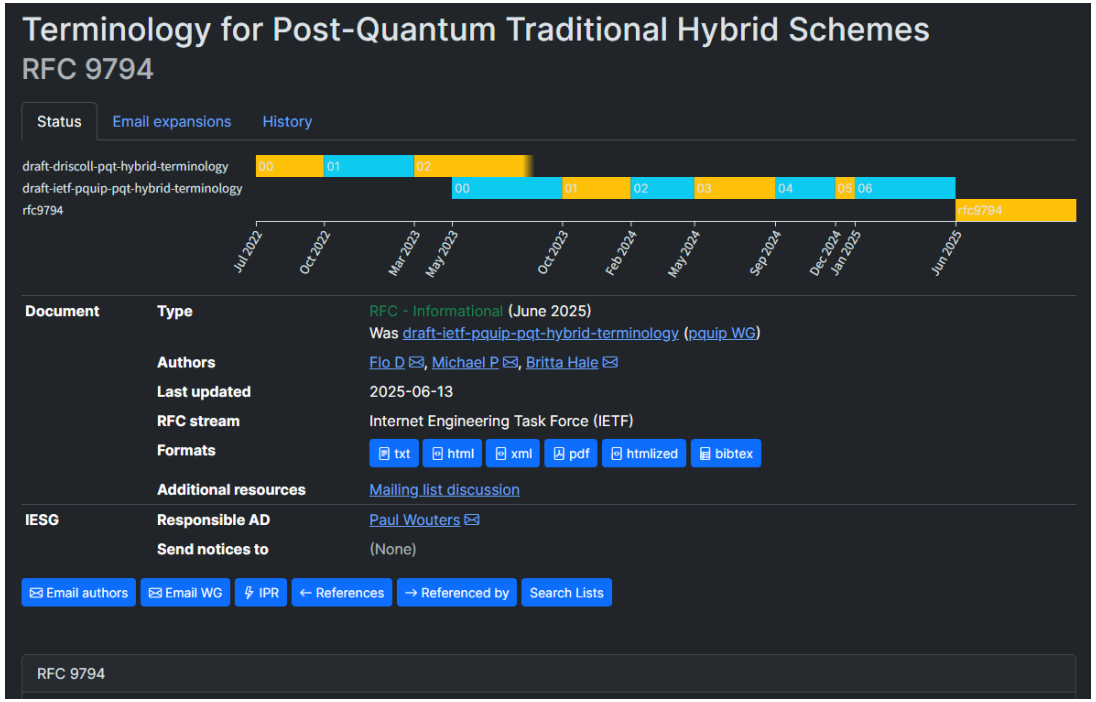
PQC移行動向

IETFの動向

- PQUIP WG：様々なWG/RGでまたがって議論されていたPQCの導入・問題対応を集約
  - I-D Post-Quantum Cryptography for Engineers draft-ietf-pquip-pqc-engineers-14(rev:2025-09-11)
  - I-D Hybrid signature spectrums draft-ietf-pquip-hybrid-signature-spectrums-07(rev:2025-09-17)
- **一部RFCも発行済**
  - Terminology for Post-Quantum Traditional Hybrid Schemes RFC 9794



IETF PQUIP WG



RFC9794

議論ポイント

PQCについて知っていましたか？

2035年までにPQC移行を推奨されていることを知っていましたか？

PQC移行に着手されていますか？

されている　ー＞いつから着手していて、どのくらい移行が進んでいますか？

されていない ー＞PQC動向のキャッチアップはされていますか？

いつから着手するという予定はありますか？

PQC移行において課題になりそうなことは何でしょうか？

例えば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

パナソニックのPQC技術開発

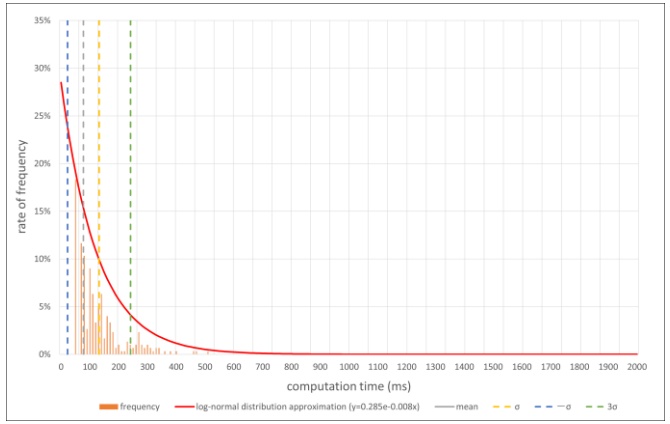
PQC移行に向けて

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



ML-DSAの処理時間

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

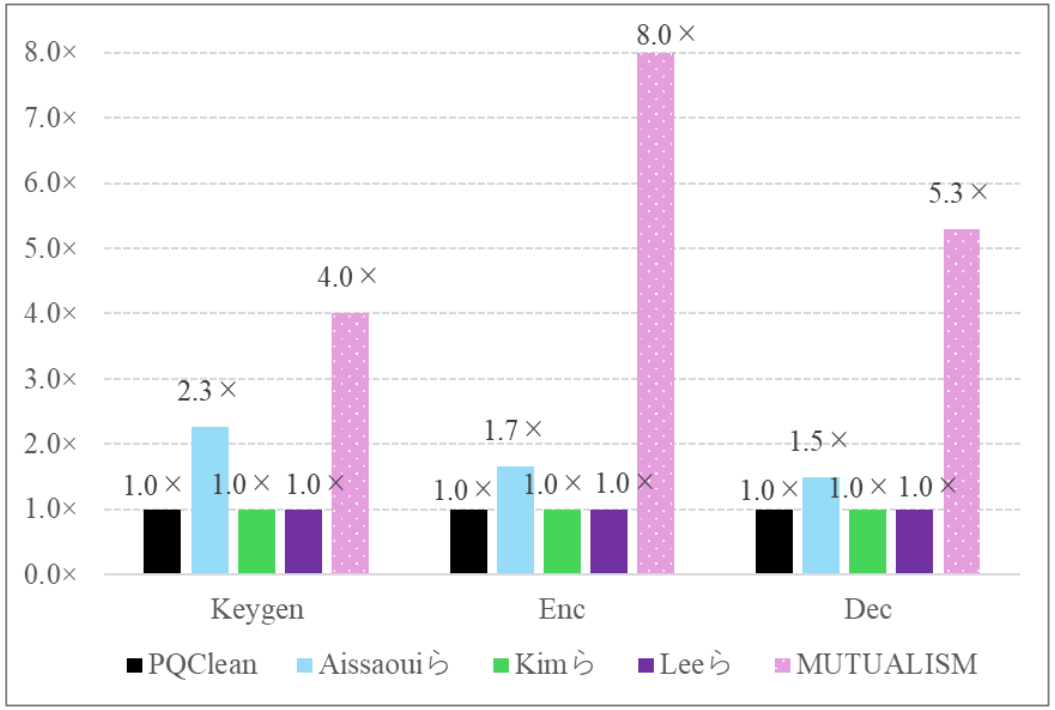
ML-DSAのスタック消費量

【パナソニックの取り組み】
宅内IoT機器に対するPQC移行に向けた課題抽出・解決技術開発

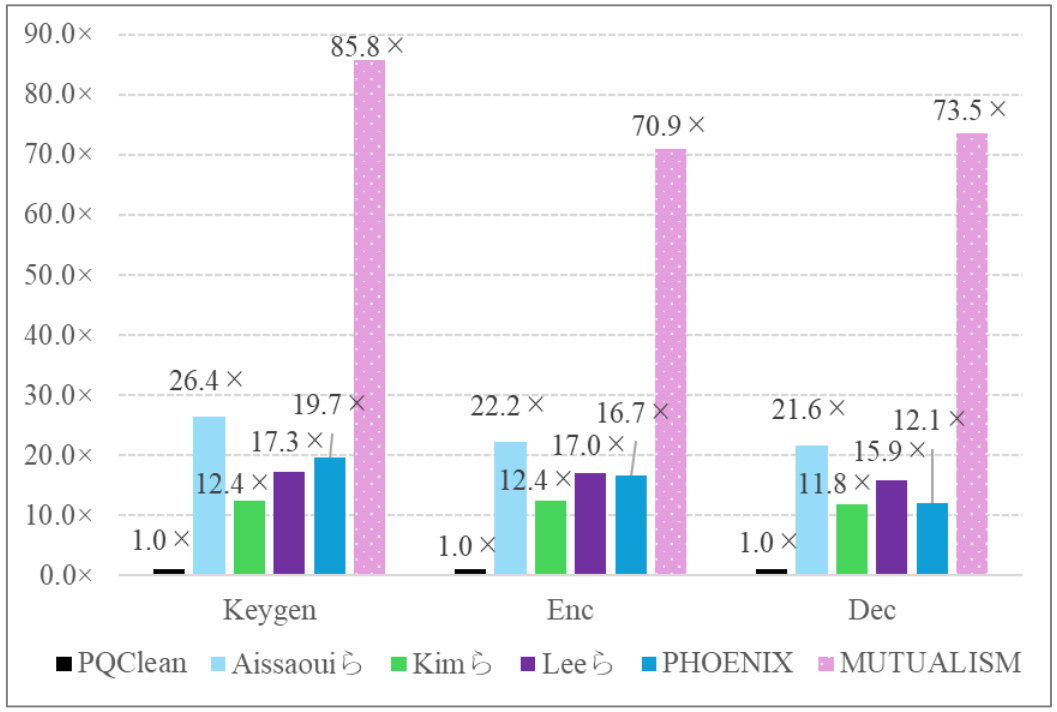
パナソニックのPQC技術開発①：HQCの改良

HQCに対するメモリ使用量と処理時間削減方式

- 劉ら,“HQCの省リソース機器向けソフトウェア実装”, 暗号と情報セキュリティシンポジウム(SCIS), 2026.
- 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

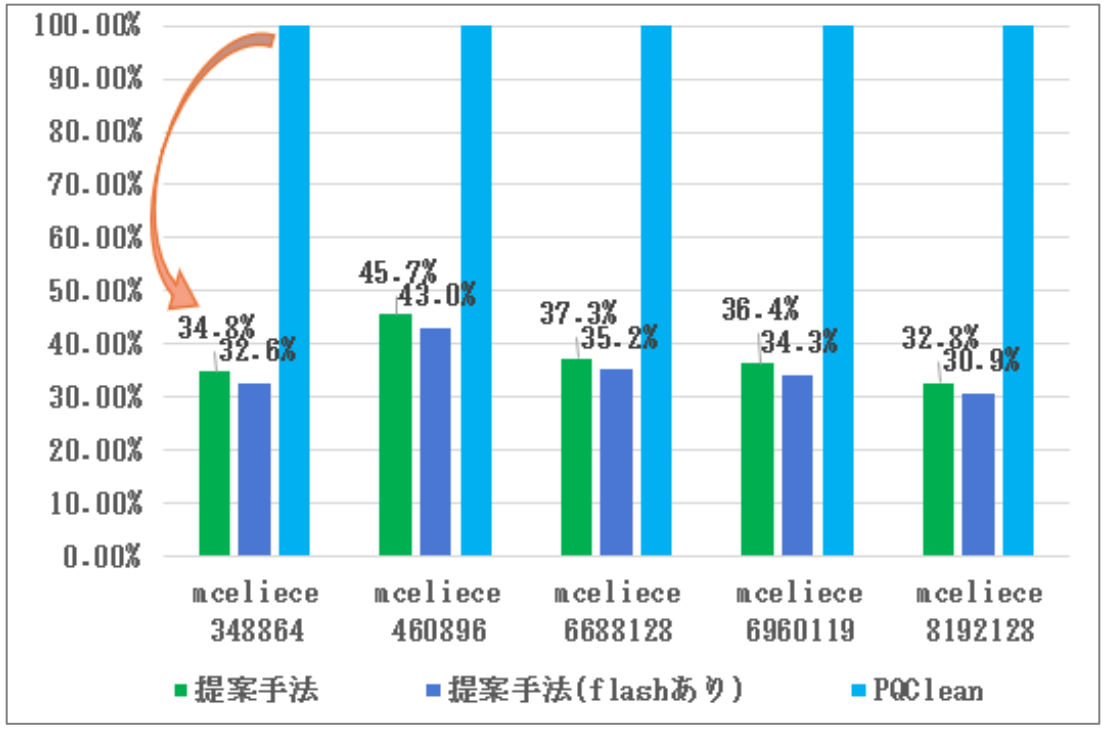
パナソニックのPQC技術開発②：McElieceの改良

McElieceに対するメモリ使用量と処理時間削減方式

- C. Liu et. al, “Giant Footprint Sharing: A Memory-Efficient Decryption Implementation for Classic McEliece”, IEICE Trans. Fund. Elect., Comm.&Comp. Sci., 2025
- メモリ使用量を**約2~3倍**、処理時間を**約2~3倍**改善

Implementation method	mceliece 348864 [bytes (ms)]	mceliece 460896 [bytes (ms)]
PQClean	23,360 (5028.1 ms)	38,224 (10170.0 ms)
Roth et al. [17]	16,816 (4925.2 ms)	-
Chen et al. [19]	18,192 (61.0 ms)	34,664 (144.4 ms)
Our implementation	8,136 (74.5 ms)	17,472 (191.0 ms)
Our implementation (with flash memory)	7,624 (79.7 ms)	16,448 (198.1 ms)

提案方式McElieceの処理時間

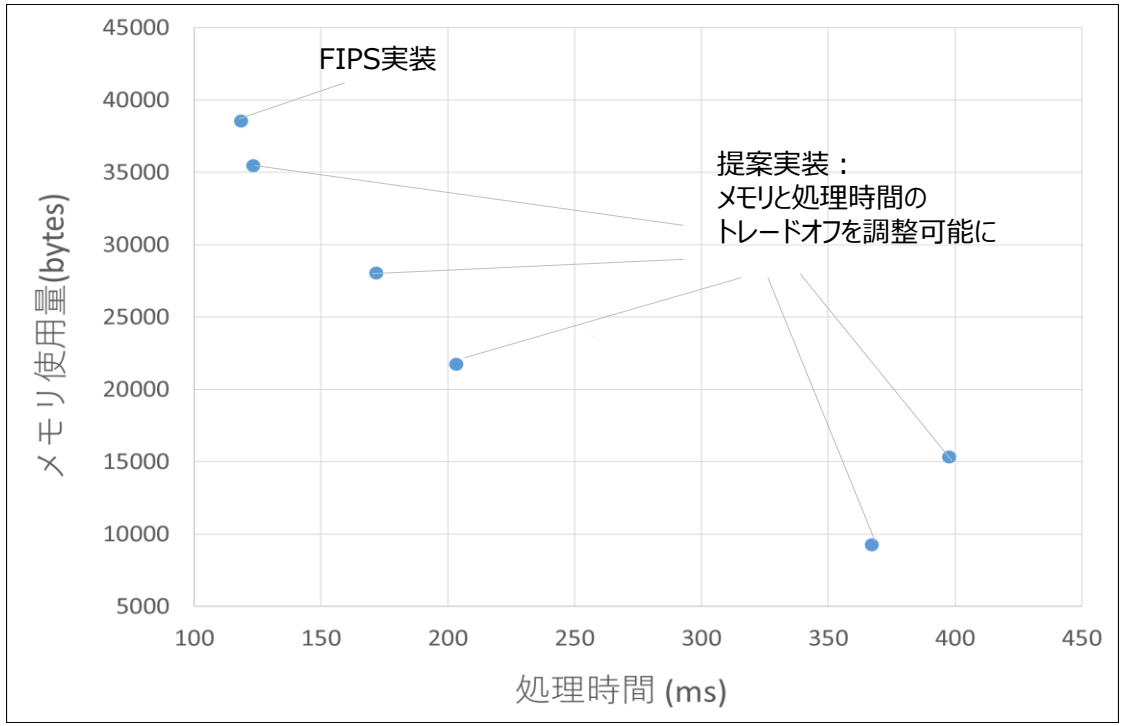


提案方式McElieceのメモリ改善倍率

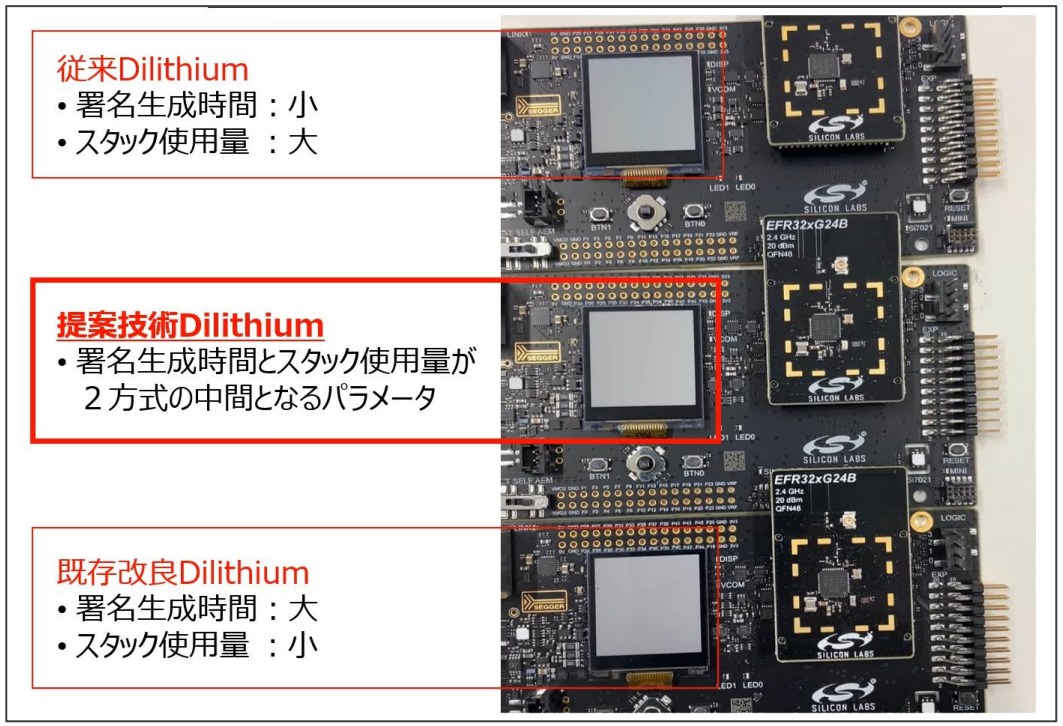
パナソニックのPQC技術開発③：ML-DSAの改良

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

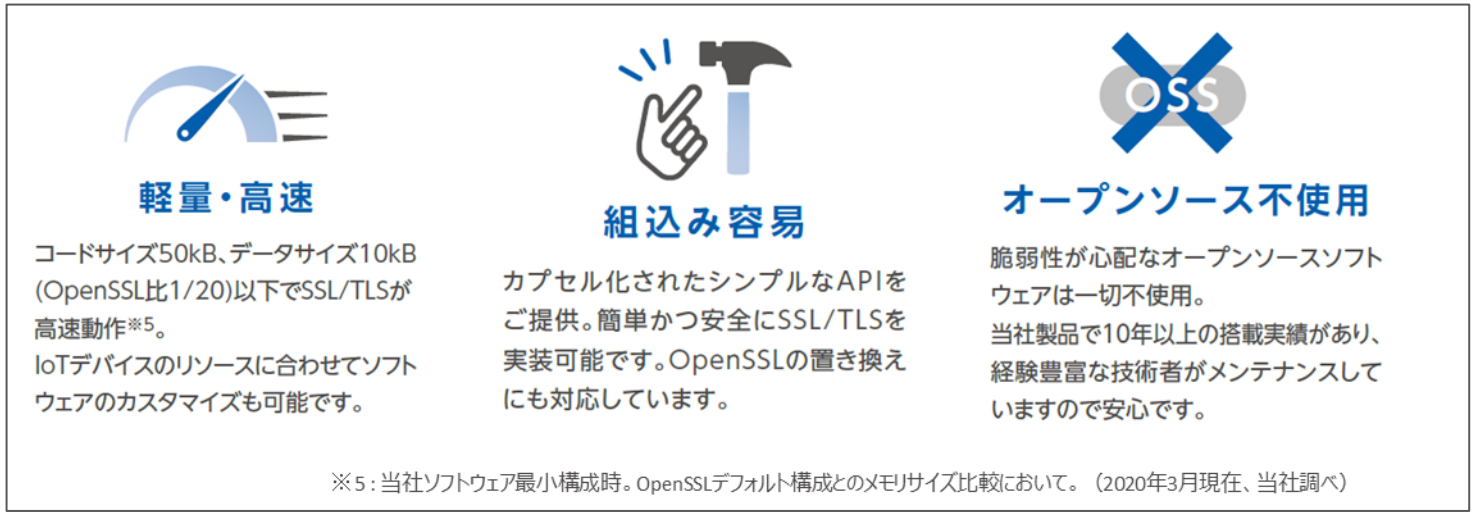
パナソニックのPQC技術開発④：PQC対応SSL/TLSライブラリ開発

パナソニックのライブラリ開発ノウハウ

- IoT機器向けの省メモリSSL/TLSライブラリを10年前から他社納入実績

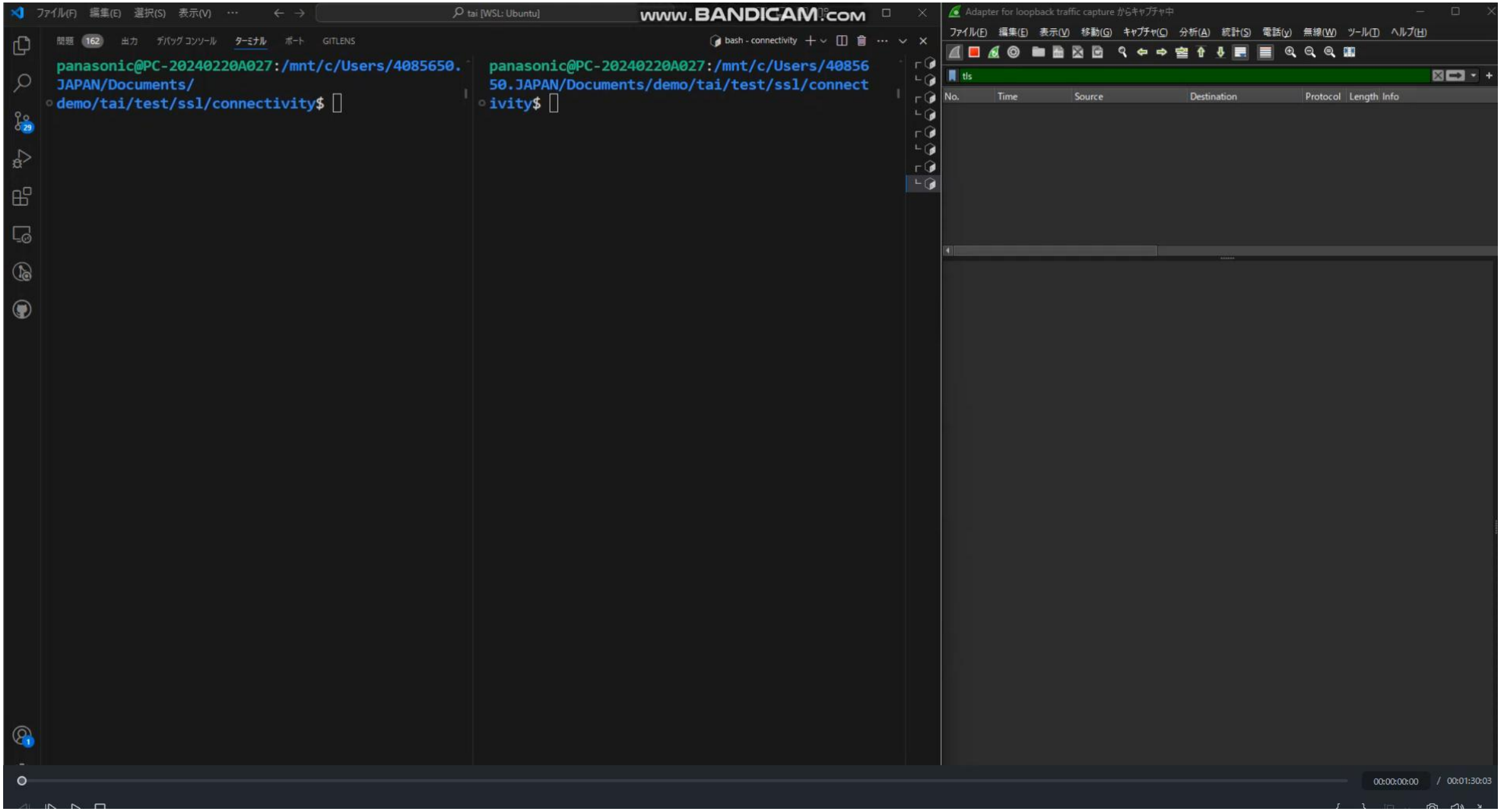
SSL/TLSへのPQC対応開発

- MLDSA,MLKEMの**FIPS203,204準拠スクラッチ実装＆弊社SSL/TLSライブラリ適用**
- ハイブリッド署名(マルチ方式)機能も導入済み



PQC対応・非対応IoT機器混在環境において
互換性のあるSSL/TLS通信が可能に

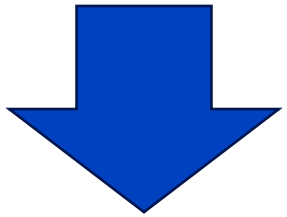
【動画】PQC対応SSL/TLSライブラリ動作デモ



インターネットルーティングプロトコルの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？

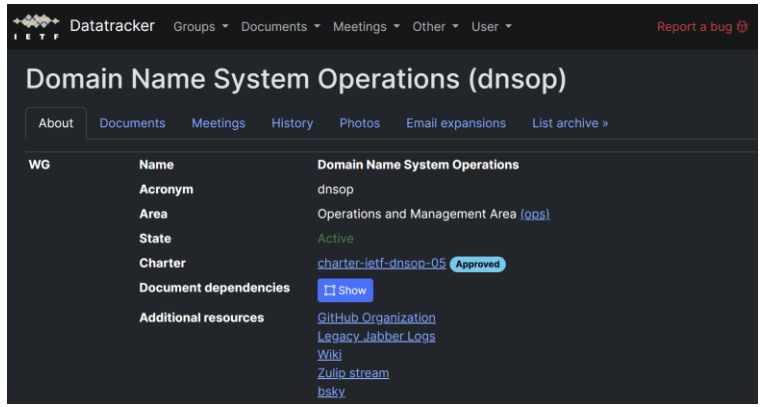
インターネットルーティングプロトコルのPQC移行動向

RPKI・BGP

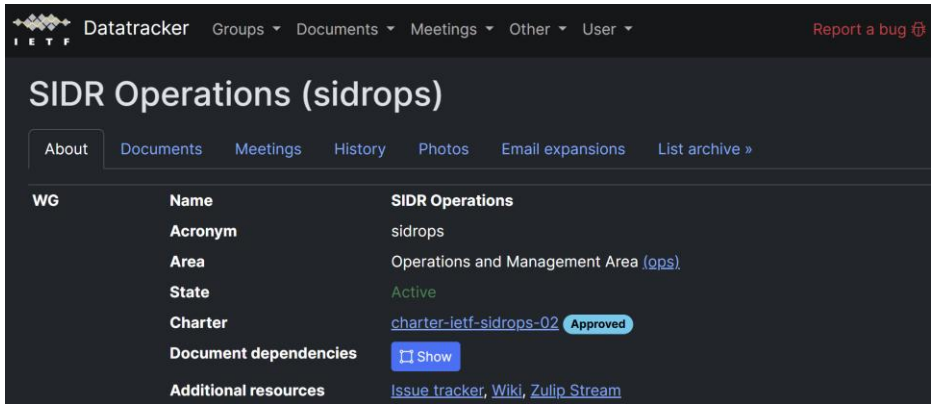
- IETF WG：SIDROP
- PQC関連**RFC・IETFは未確認**

DNSSEC

- IETF WG：DNSOP WG (公式), PQ DNSSEC (非公式)
- ドラフト: draft-sheth-pqc-dnssec-strategy-00,draft-fregly-research-agenda-for-pqc-dnssec-01
- PQC関連**RFCは未確認**



DNSOP WG



SIDROP WG

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

インターネットルーティングプロトコルのPQC移行動向

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

①DoH/DoTでのハイブリッド鍵交換実験

（関連IETFドラフト: draft-kwiatkowski-tls-ecdhe-mlkem-02**）**

- ChromeがML-KEMとECDHのハイブリッドをSSL/TLSに実装
  -> SIDN Labs運用 dns4all.eu のDoH/DoTサーバでハイブリッドをサポートできるか実験
- Chromeのフラグ有効化・DoH設定手順・接続確認まで提示

②PATAD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」

③RPKI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移行動向

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

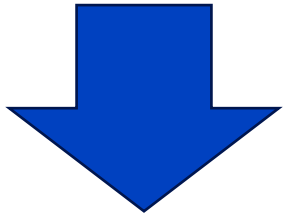
Table 2: A comparison between SL-DNSSEC and signature-based DNSSEC methods. SD : Standard DNS (TCP Fallback).

	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

BGPsec、RPKIなどまだ十分に検討されていないプロトコルも存在

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



我々の目標：
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

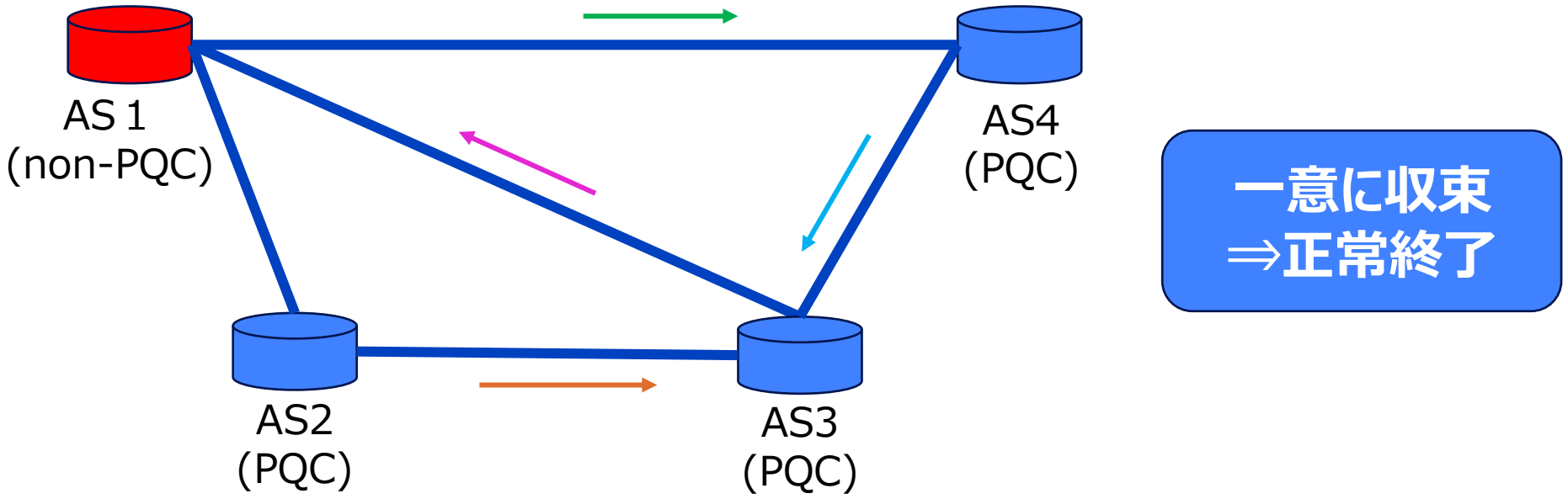
パナソニックのBGPsecに関するPQC移行技術

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



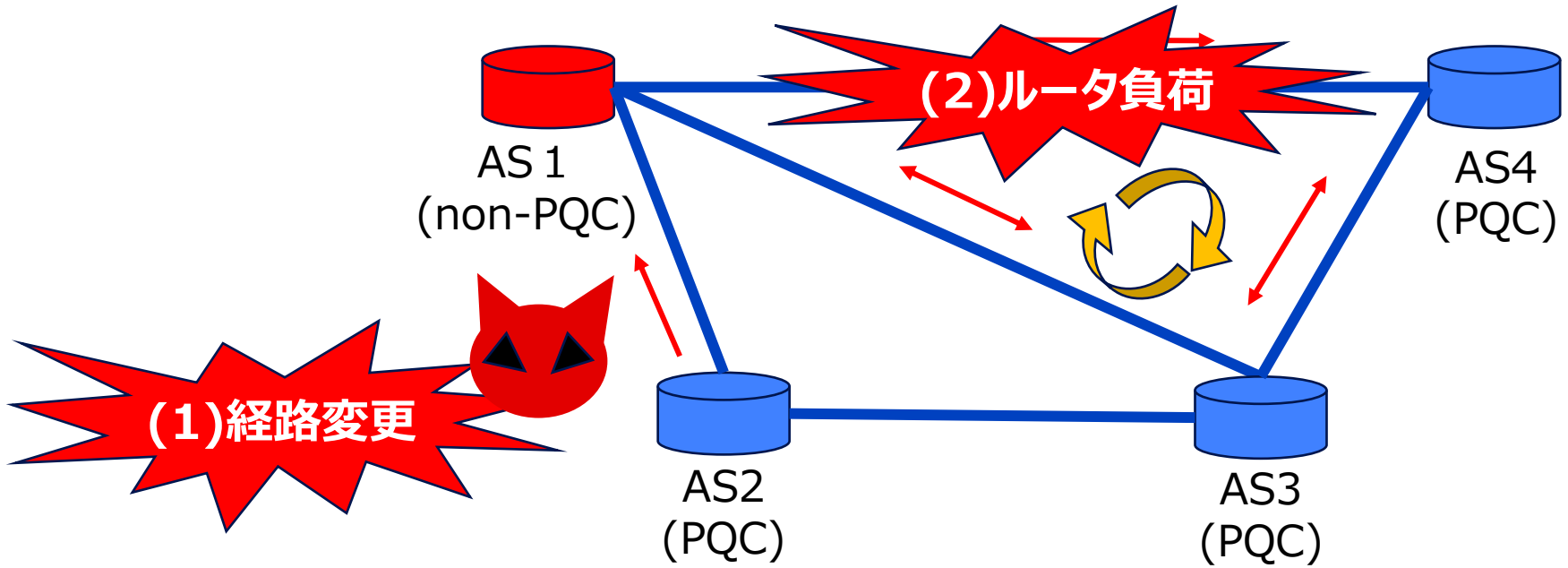
パナソニックのBGPsecに関するPQC移行技術

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）

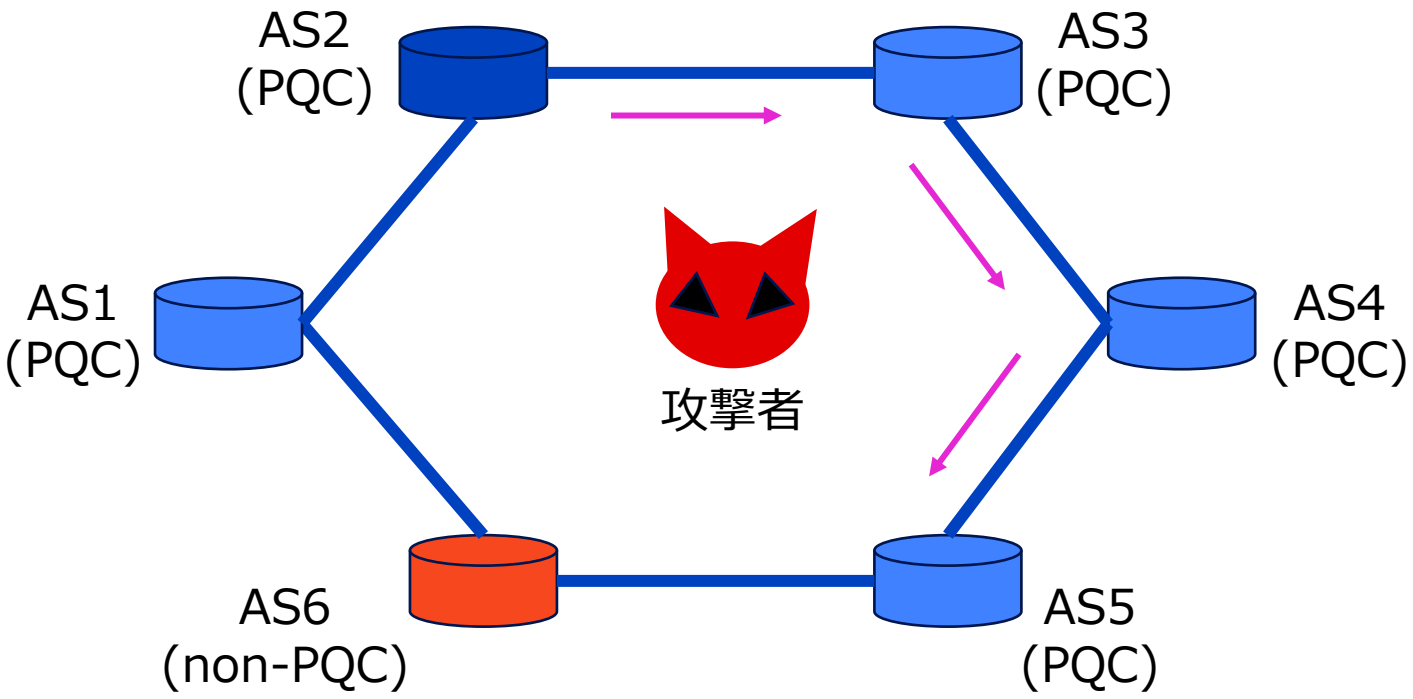
[*]高橋ら,“PQC-BGPsec：耐量子計算機暗号がインターネットルーティングにもたらす影響”, 暗号と情報セキュリティシンポジウム(SCIS), 2026.



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

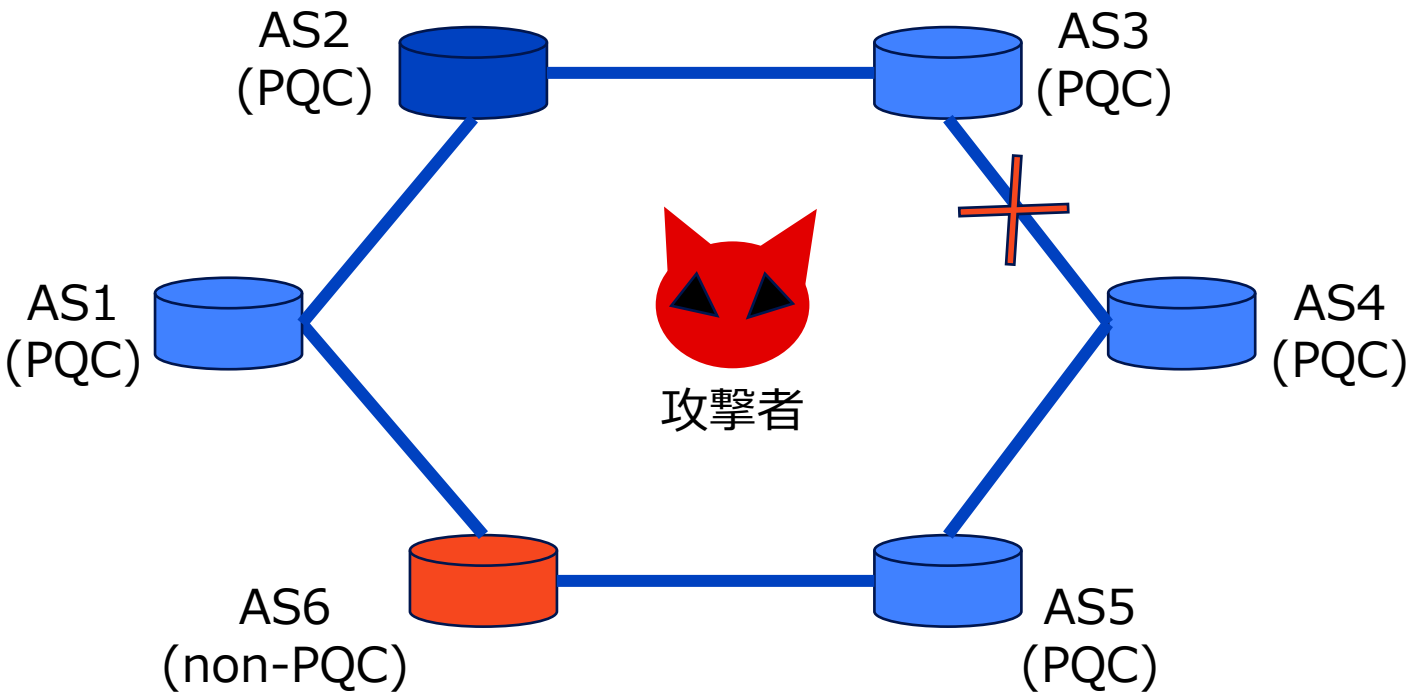
- BGP Wedge[Yang, 2022]：ネットワークが接断した際，意図した安定状態とは別状態に収束する
- PQC部分導入時に、攻撃者は**non-PQCのASを通るような収束経路に変更する攻撃**が可能



パナソニックのBGPsecに関するPQC移行技術

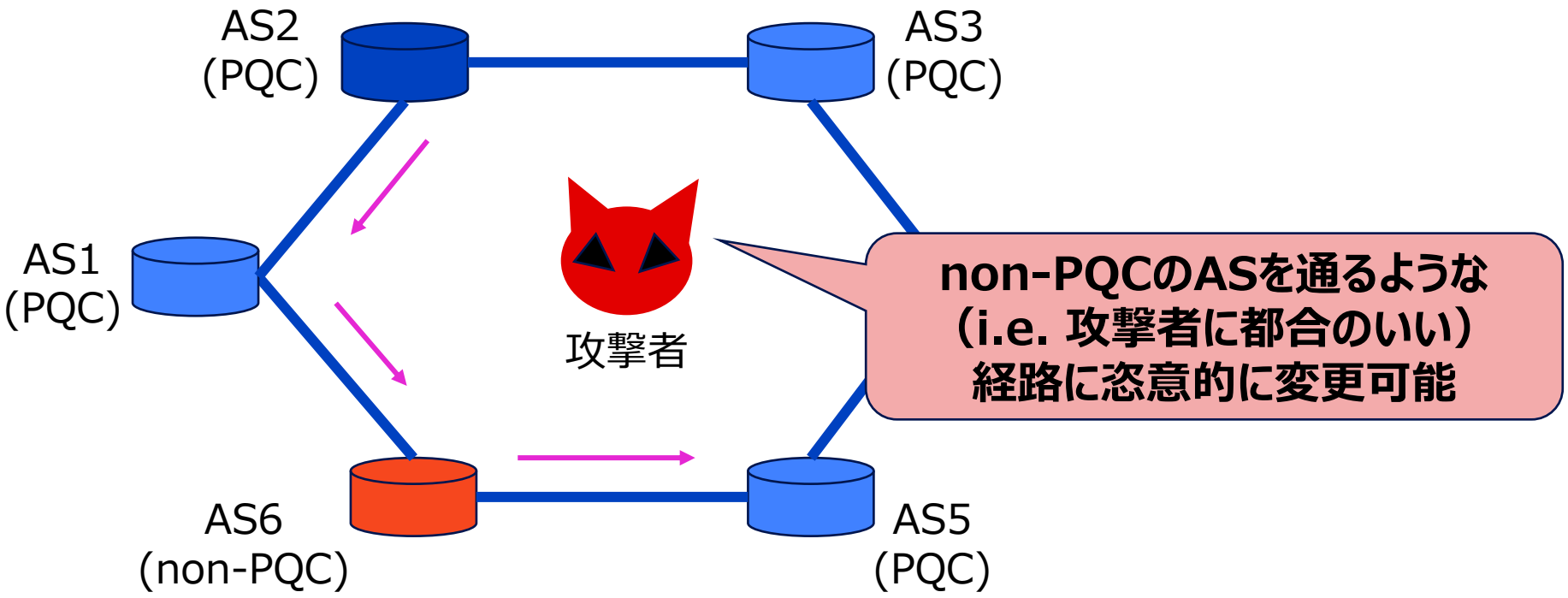
(1)収束経路が一意でない例＝BGP Wedge

- 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



(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

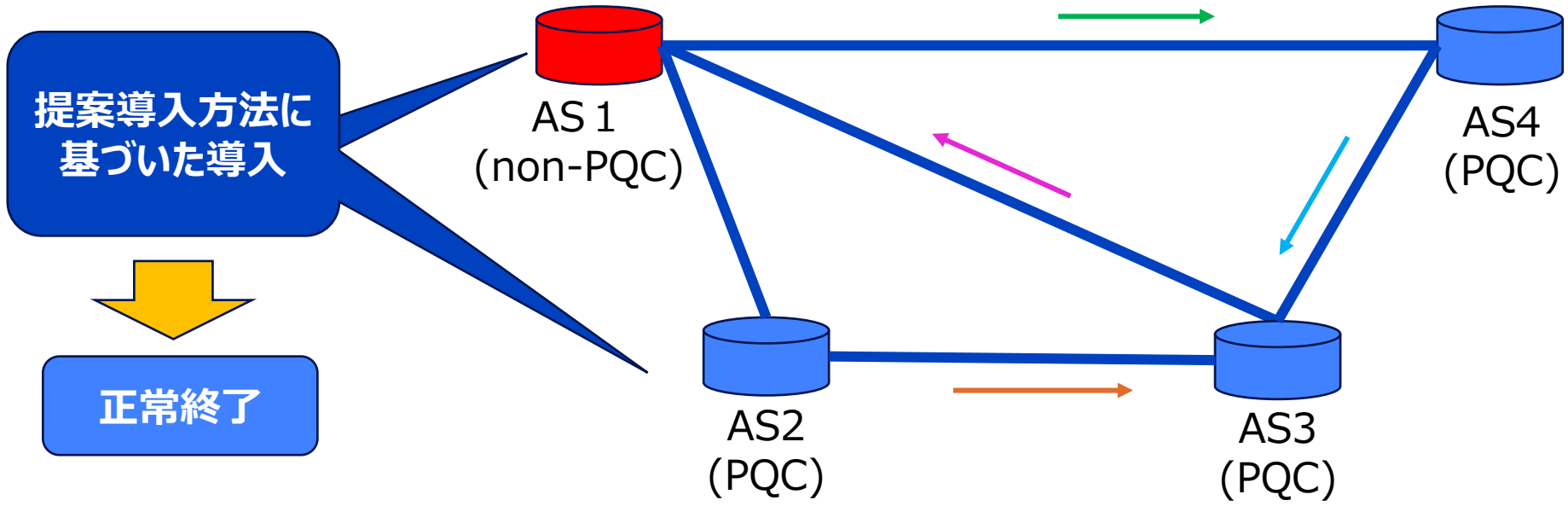


【再掲】経路収束性が満たされていない場合：以下２つのパターンが考えられる

- (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



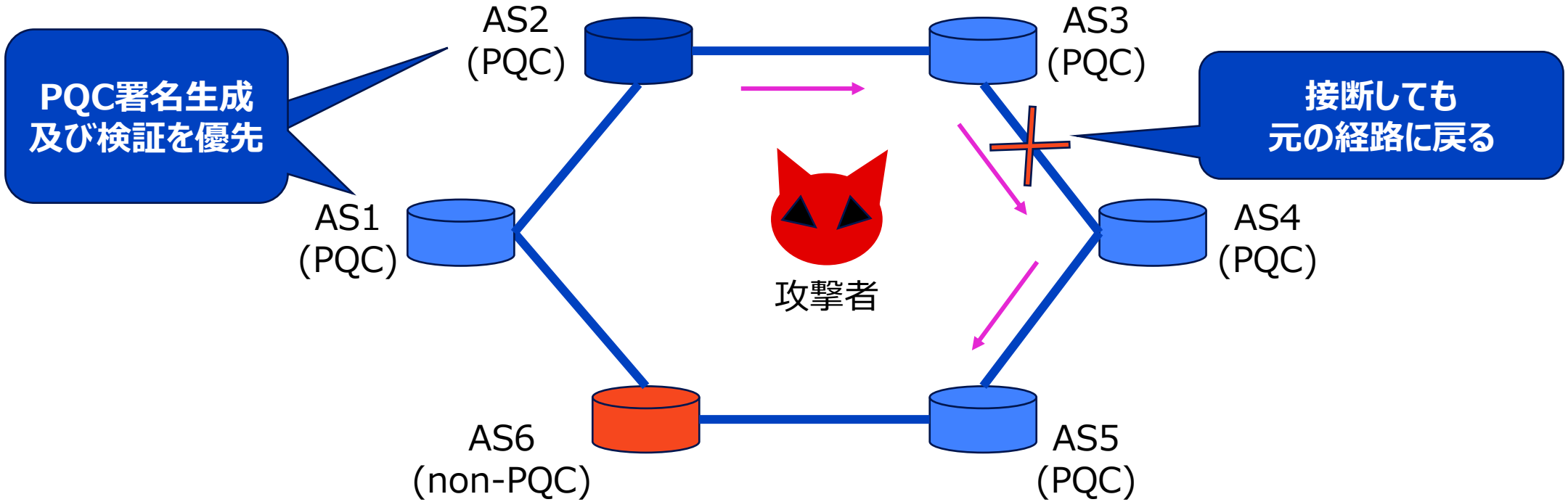
パナソニックのBGPsecに関するPQC移行技術

【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)に対処する導入方法：ポリシーの統一

- ポリシー：ASが経路選択する際のセキュリティ・経済性・経路長などの要件に対する優先度
- 全てのASが**従来署名よりPQCを常に優先するポリシーを採用**すれば、収束経路は一意に定まる



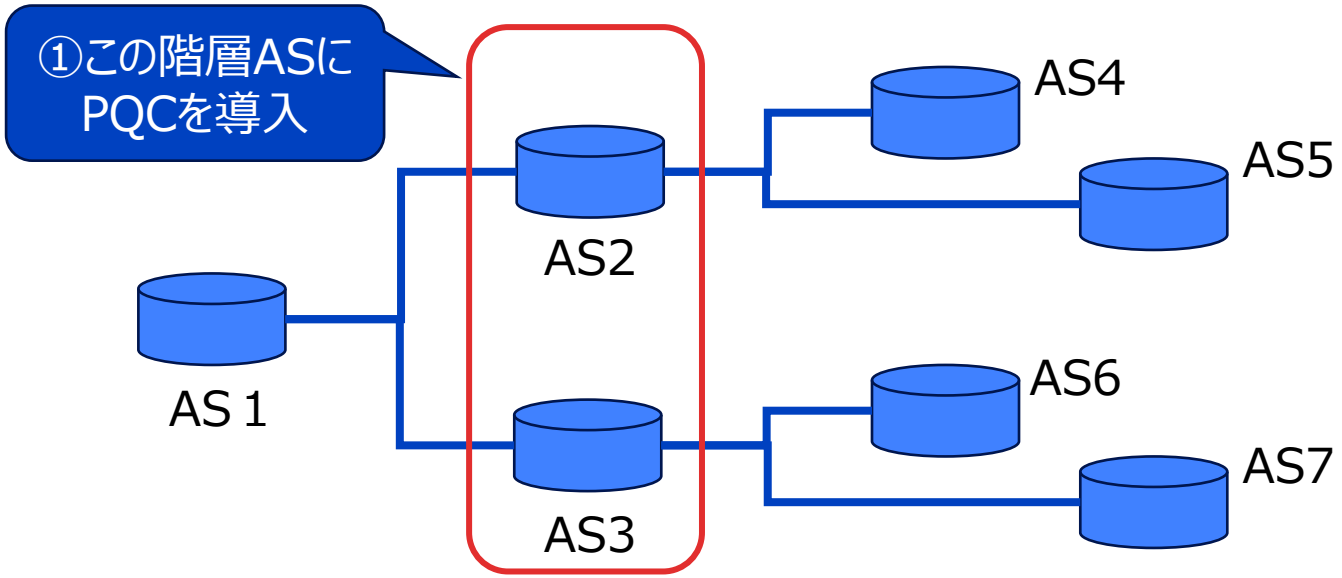
パナソニックのBGPsecに関するPQC移行技術

【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**

(2)に対処する導入方法：階層単位でのPQC導入順序

- ネットワークが階層構造の場合、以下のPQC導入順序であれば経路が収束：
  ①任意の階層のAS全てにPQCを導入（これをN層目とする）
  ②N-1層目 or N+1層目のAS全てにPQCを導入、以下これを繰り返す

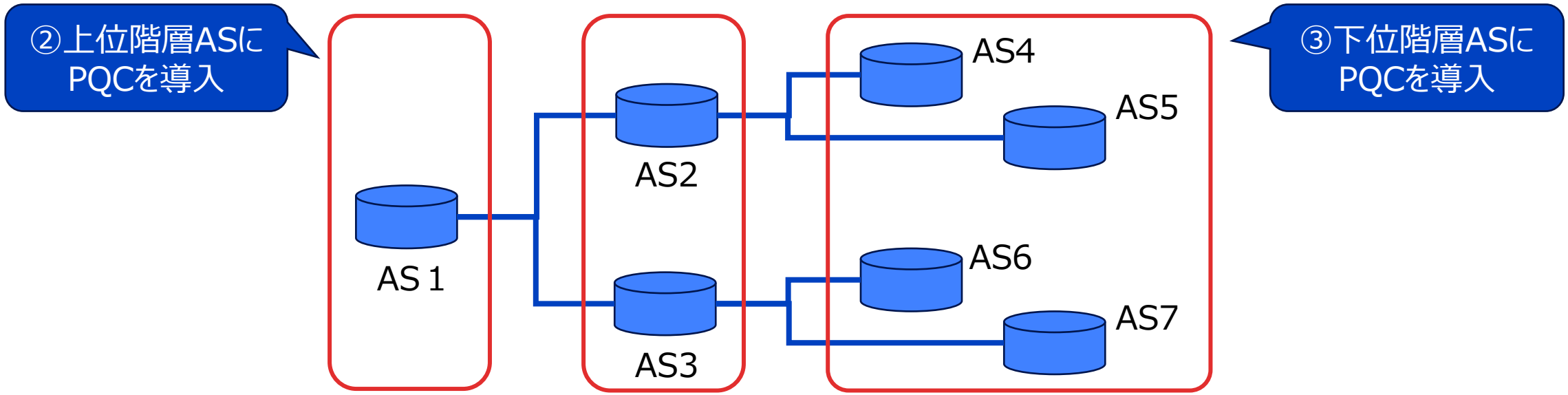


【再掲】経路収束性が満たされていない場合：以下２つのパターンが考えられる

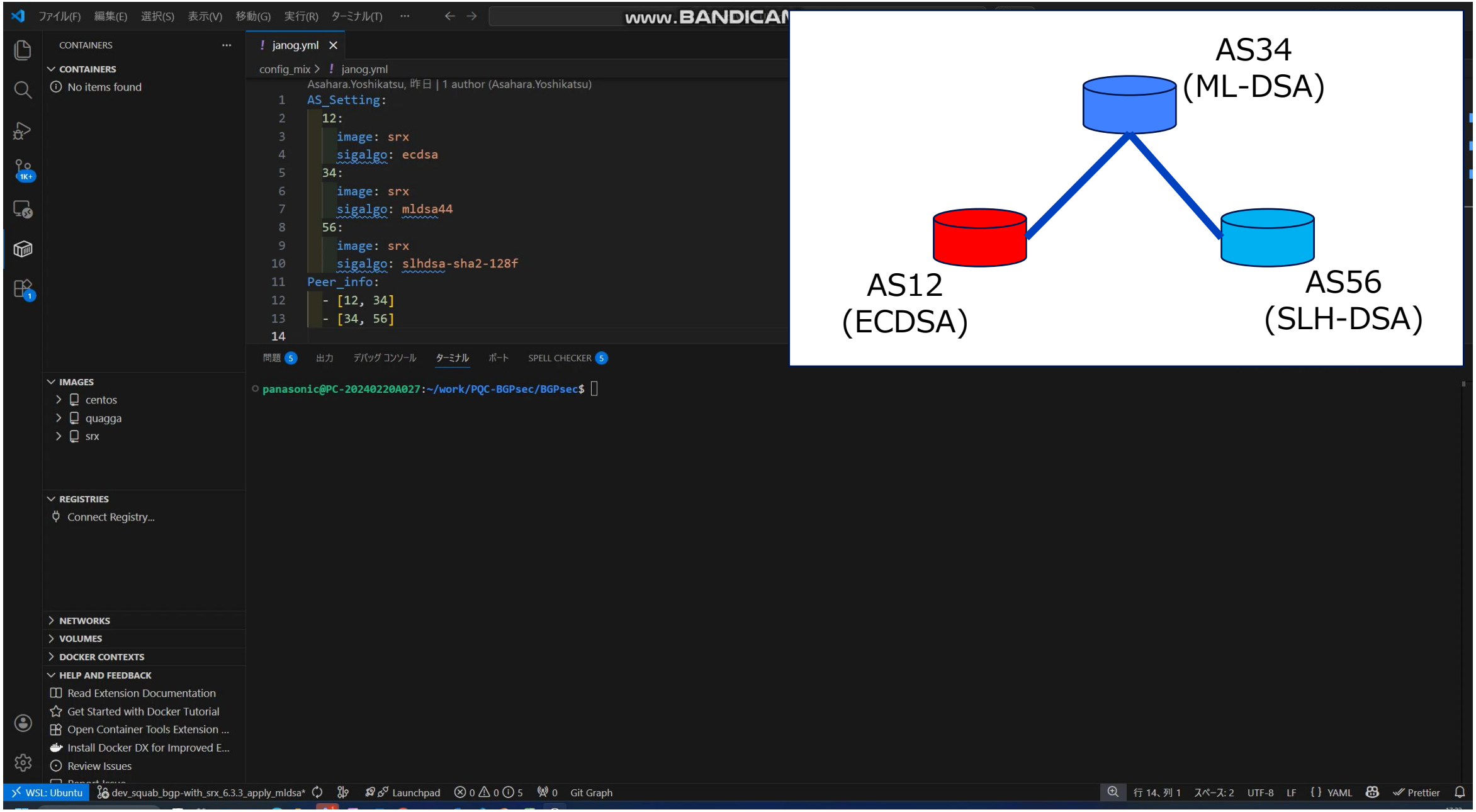
- (1)収束経路が一意でない -> **攻撃者による経路変更攻撃**
- (2)経路が収束しない -> **ルータへの負荷増加**

(2)に対処する導入方法：階層単位でのPQC導入順序

- ネットワークが階層構造の場合、以下のPQC導入順序であれば経路が収束：
  ①任意の階層のAS全てにPQCを導入（これをN層目とする）
  ②N-1層目 or N+1層目のAS全てにPQCを導入、以下これを繰り返す



【動画】PQC対応BGPsecネットワーク構築デモ



【参考】PQC対応BGPsecネットワーク構築デモ実装

リファレンス実装：NIST-BGP-SRx

- BGPの評価実験を行う共通基盤として作られたオープンソースライブラリ(GitHub)
- BGP自動構築にはSQUABを利用
  - DockerコンテナとしてASとRPKIサーバを立ち上げ＆ネットワーク構築

PQC対応のためのBGP-SRx実装修正ポイント

①OpenSSLライブラリアップデート

暗号実装部のコア部分にはOpenSSLを利用 -> PQC対応のv3.5.4にバージョンアップ

②鍵ファイルのバッファ不足対処

ML-DSAは鍵サイズが大きいため、パラメータに合わせてバッファサイズを再設定

③EVP鍵構造体を利用可能に

新たにEVP鍵タイプevp pkey を定義 & 作成したDER形式鍵ファイルをEVP変換するAPIを実装

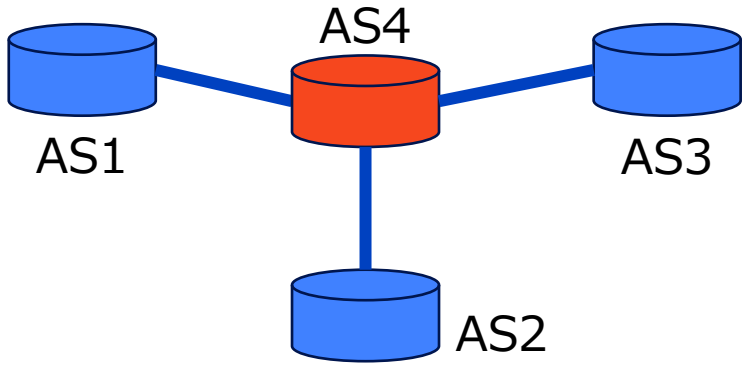
【参考】今後の研究：ネットワークトポロジーの特徴量を利用したPQC導入

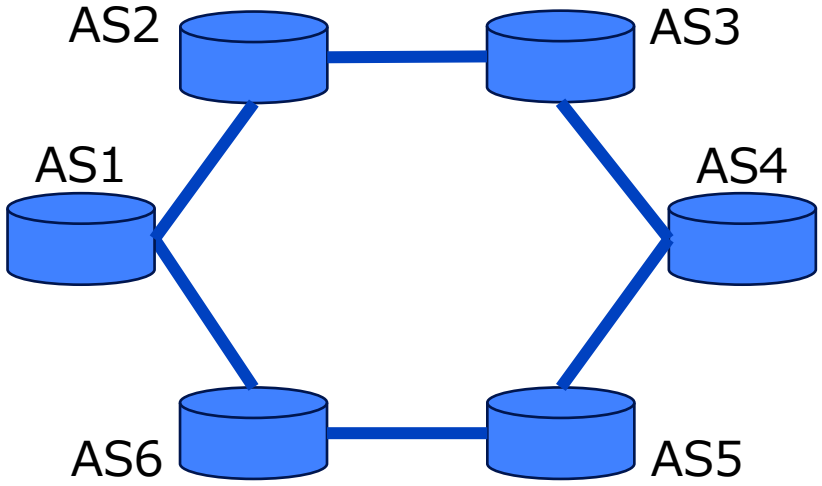
中心性を利用したPQC導入順序

- (媒介)中心性：ノード間最短経路の集合にあるノードが含まれる度合い
- 中心性が大きい＝そのノードを含むASパスが多いと予想されるので、優先的にPQC導入を行う

半径を利用したPQCアルゴリズム選択

- 離心率：あるノードから最遠のノードとの距離
- 半径：グラフの最小離心率（つまり最小の最遠距離）
- 半径が大きい＝ASパスの経路長が長いので、検証回数が多くなる -> 検証が速いFALCONを選択





質疑＆議論

議論ポイント

PQCについて知っていましたか？

2035年までにPQC移行を推奨されていることを知っていましたか？

PQC移行に着手されていますか？

されている　ー＞いつから着手していて、どのくらい移行が進んでいますか？

されていない ー＞PQC動向のキャッチアップはされていますか？

いつから着手するという予定はありますか？

PQC移行において課題になりそうなことは何でしょうか？

例えば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

E-mail：takahashi.yasushi@jp.panasonic.com

幸せの、チカラに。

Panasonic Digital Transformation & Cyber-Physical Systems Division