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 (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移行が必要といわれていることは知っていましたか？**

- **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(5分)
- ネットワークにおける認証・鍵交換、公開鍵暗号
- 量子計算機による危殆化 -> PQC

PQC移行の動向(5分)
- 米国、欧州、日本の動向
- IETF活動動向

弊社のPQC移行に向けた取り組み(10分)
- 改良方式の開発
- PQC対応SSL/TLSライブラリ実装

ネットワークルーティングプロトコルに関するPQC移行状況(5分)
- IETF活動動向、関連論文

弊社のBGPsecに関するPQC移行技術(10分)
- 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

PQC-BGPsecのデモ(5分)

質疑＆議論(20分)

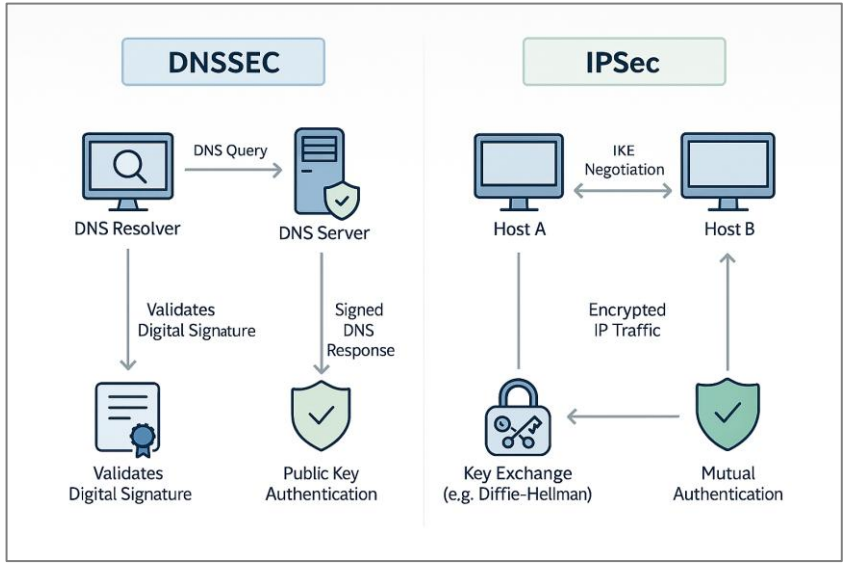
PQCとは何か

ネットワークにおける認証・鍵交換の必要性

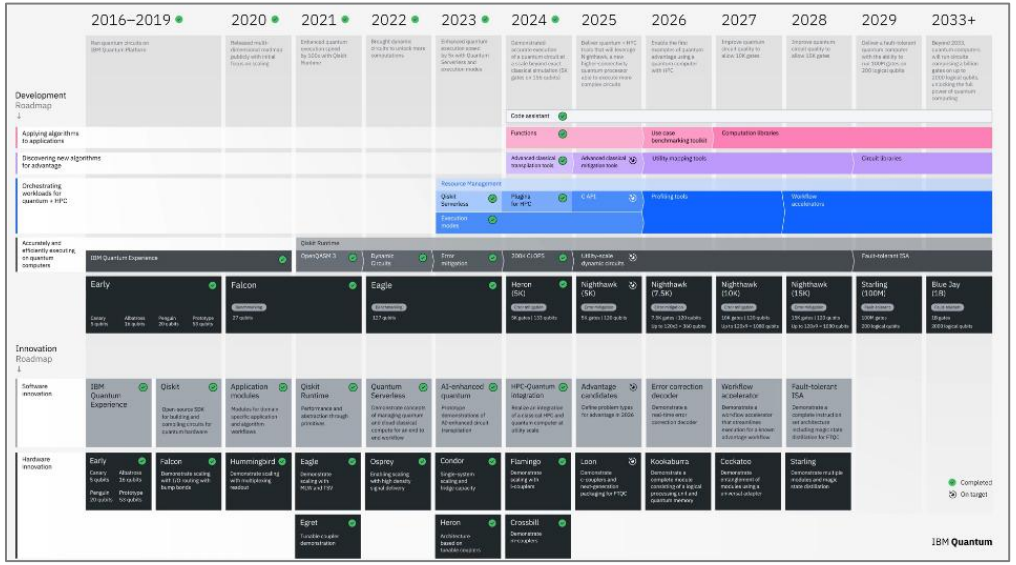
- DNSSEC、IPsecなどで認証・鍵交換が必要 <- **公開鍵暗号**と呼ばれる技術が安全性を保証

量子計算機と公開鍵暗号

- 世界的に量子計算機の開発が活発化（例：1121 qubitをIBMが開発）
- 実用的な量子計算機があれば、現在使用される**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]



DNSSEC･Ipsecにおける認証･鍵交換



2025 IBM Quantum Roadmap update - IBM Mediacenter

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方式
- 各国で標準化が進められている
- 過去の例を見てもシステムの**暗号移行には長期間かかる**
  ⇒ **今の内から**PQCの標準化・移行準備が進む

RSA暗号に対する推奨鍵長の変遷

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

NISTPQC標準方式

議論ポイント

- **PQCについて知っていましたか？**

- **PQCへ（2035年までに）移行しないといけないことは知っていましたか？**

- **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移行の動向

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

現在

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)

▼
2035：米大統領令 PQC移行目標

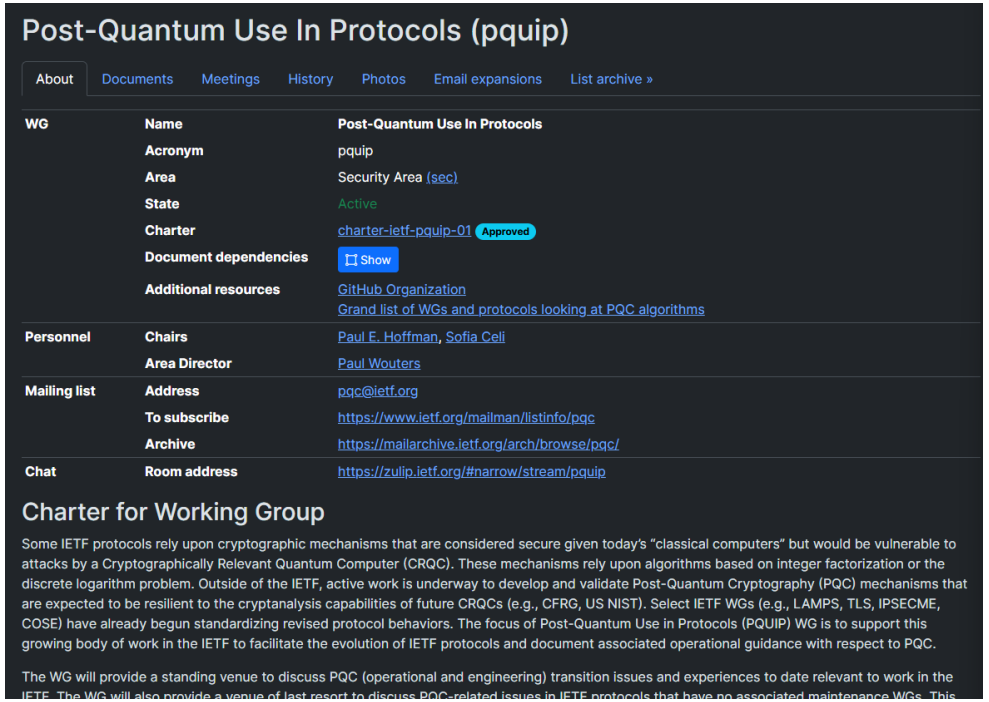
▼
2035：米NSA移行目標

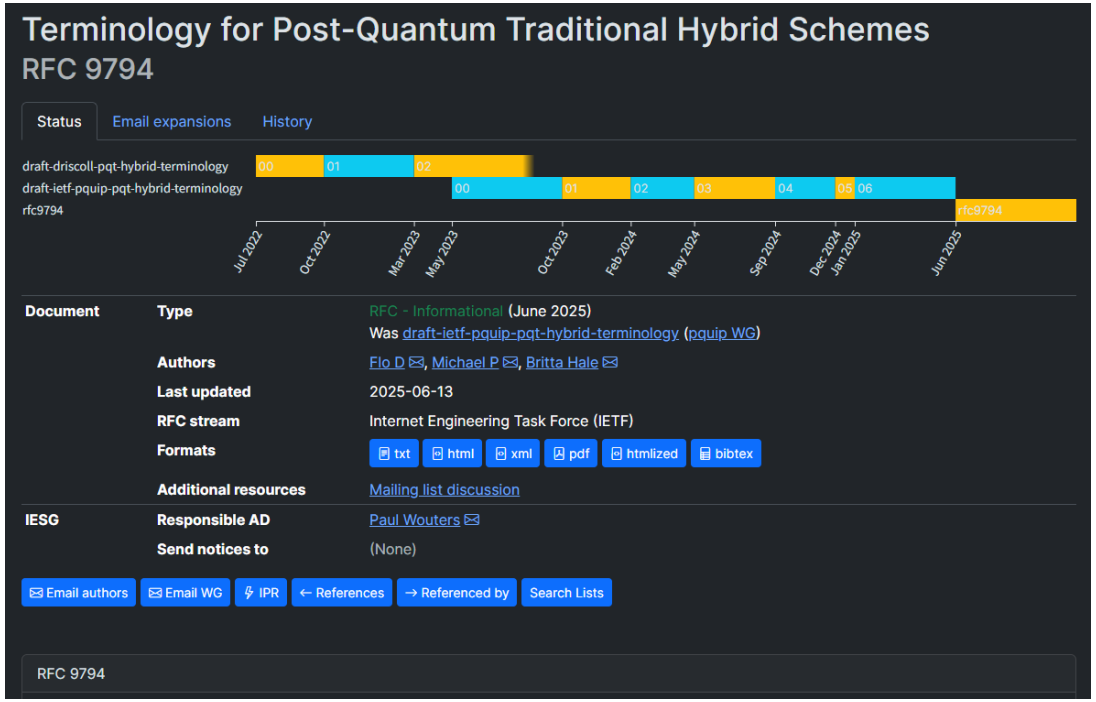
▼
2035：ブラウザ・クラウドサービス移行目標 (CNSA2.0)

PQC移行の動向

IETFの動き

- 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





議論ポイント

- **PQCについて知っていましたか？**

- **PQCへ（2035年までに）移行しないといけないことは知っていましたか？**

- **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？

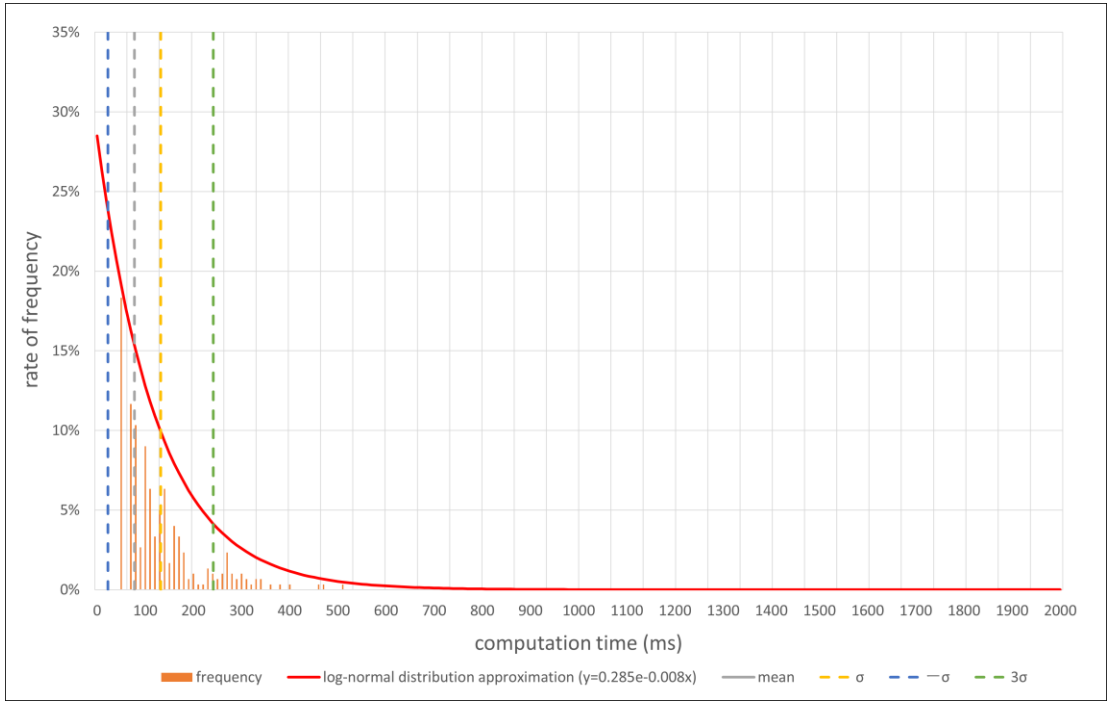
- **PQC移行において課題になりそうなことは何でしょうか？**
  （例えばパケットサイズの増大、次世代ルータの処理性能不足など）

PQC移行に向けた取り組み

宅内IoT機器環境（省リソース）における課題抽出＆解決技術開発

- 【課題抽出】IoT機器は省リソース環境 → **メモリ使用量が大きい**ことが実環境での課題
  - PQC良点：従来暗号と比べて高速（1.5倍~10倍）
  - PQC欠点：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）

ML-DSAの処理時間



ML-DSAのスタック消費量

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

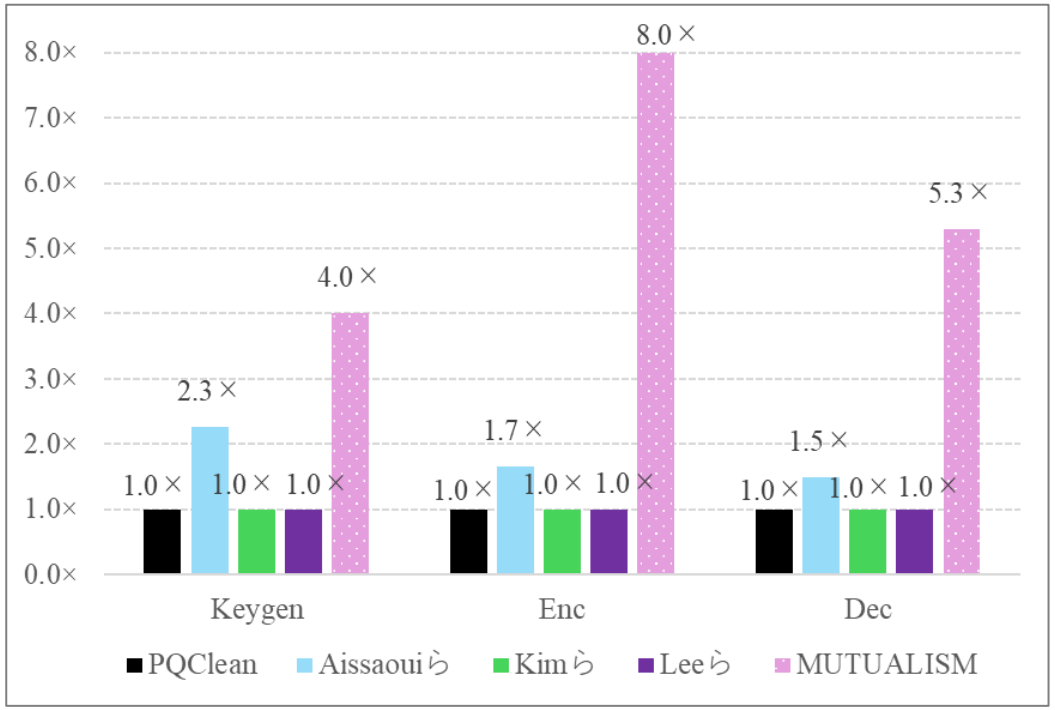
環境：宅内IoT機器向け評価ボード
SiliconLabs EFR32xG24
CPU: ARM® Cortex®-M33, 32bit 78.0MHz
Flash memory: 1,536 kB,
RAM: 256 kB

PQC移行に向けた取り組み

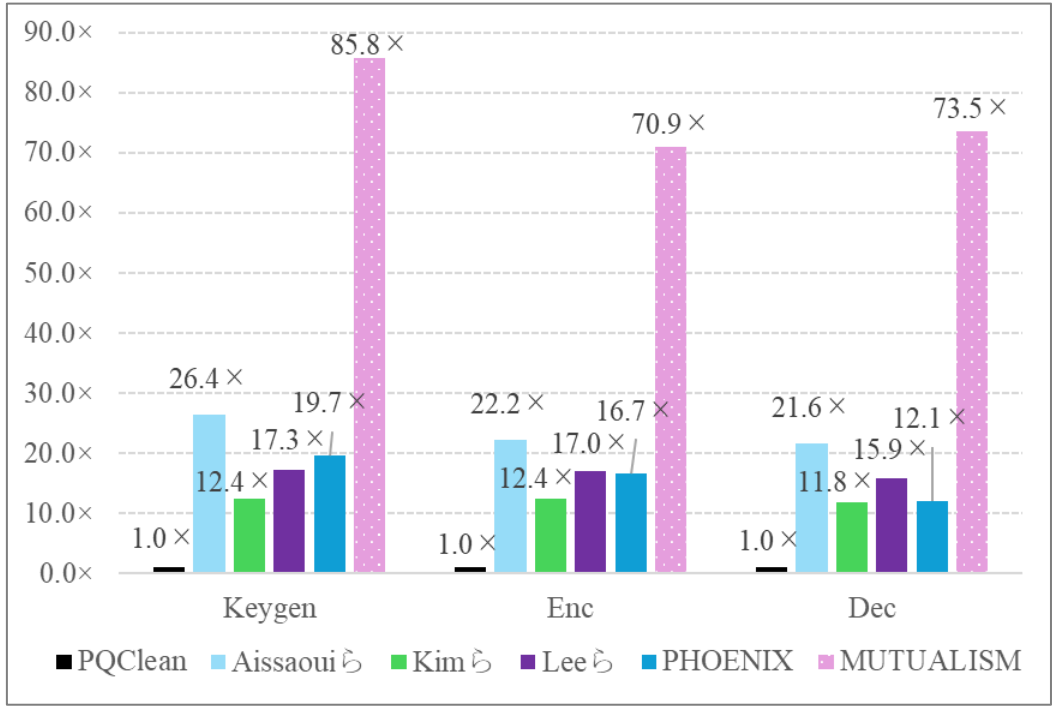
宅内IoT機器環境（省リソース）における課題抽出＆解決技術開発

- 【解決技術】**処理時間とメモリ使用量両方の削減方式**を開発（国内学会発表済）
  - 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), 2F1-1, 2026.

HQCのメモリ改善倍率



HQCの処理時間改善倍率

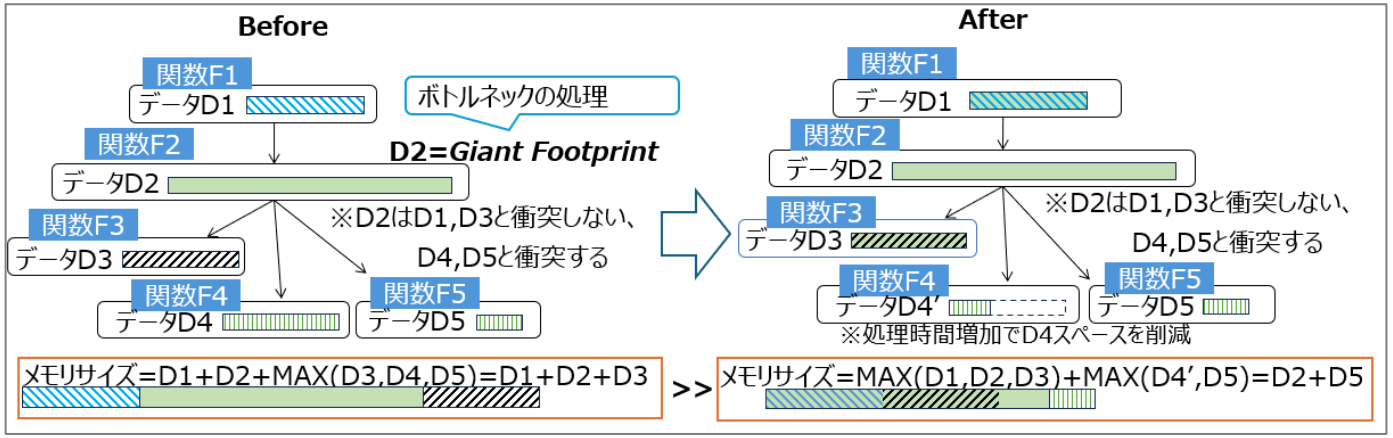


PQC移行に向けた取り組み

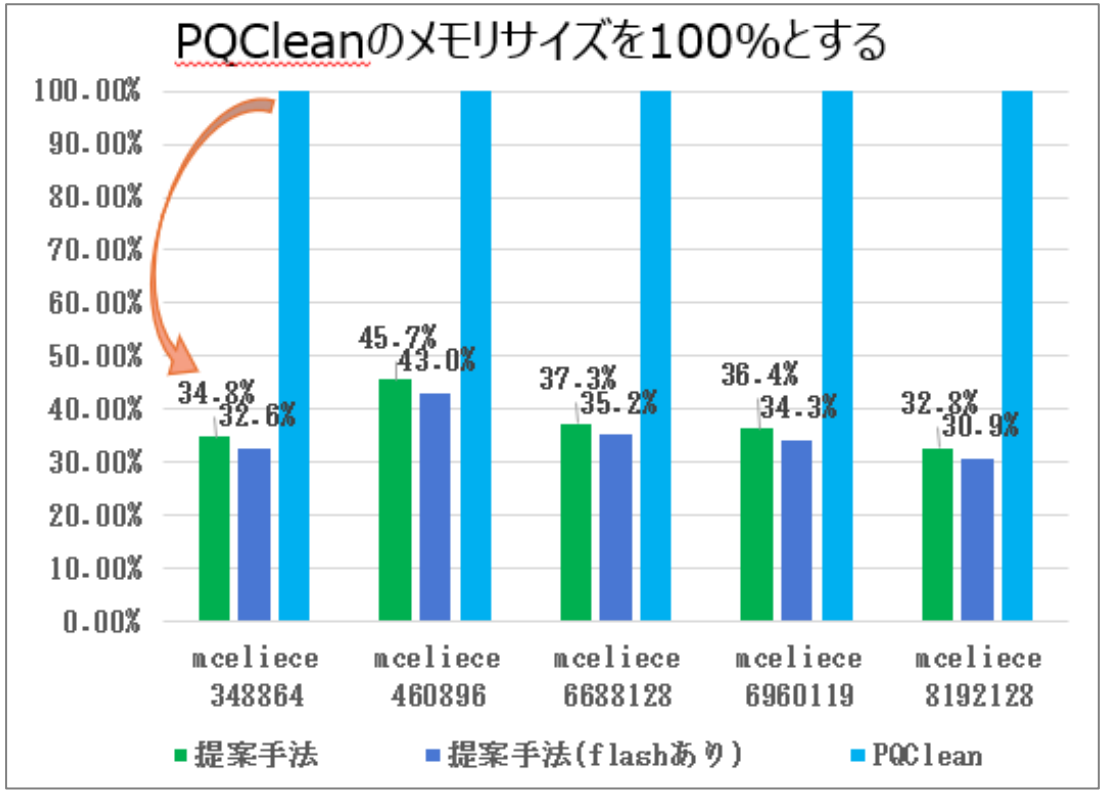
宅内IoT機器環境（省リソース）における課題抽出＆解決技術開発

- 【解決技術】**処理時間メモリ使用量削減方式**を開発（国際論文誌採択済）
  - C. Liu et. al, “Giant Footprint Sharing: A Memory-Efficient Decryption Implementation for Classic McEliece, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2025

McEliece提案アイデア図



McElieceのメモリ削減倍率

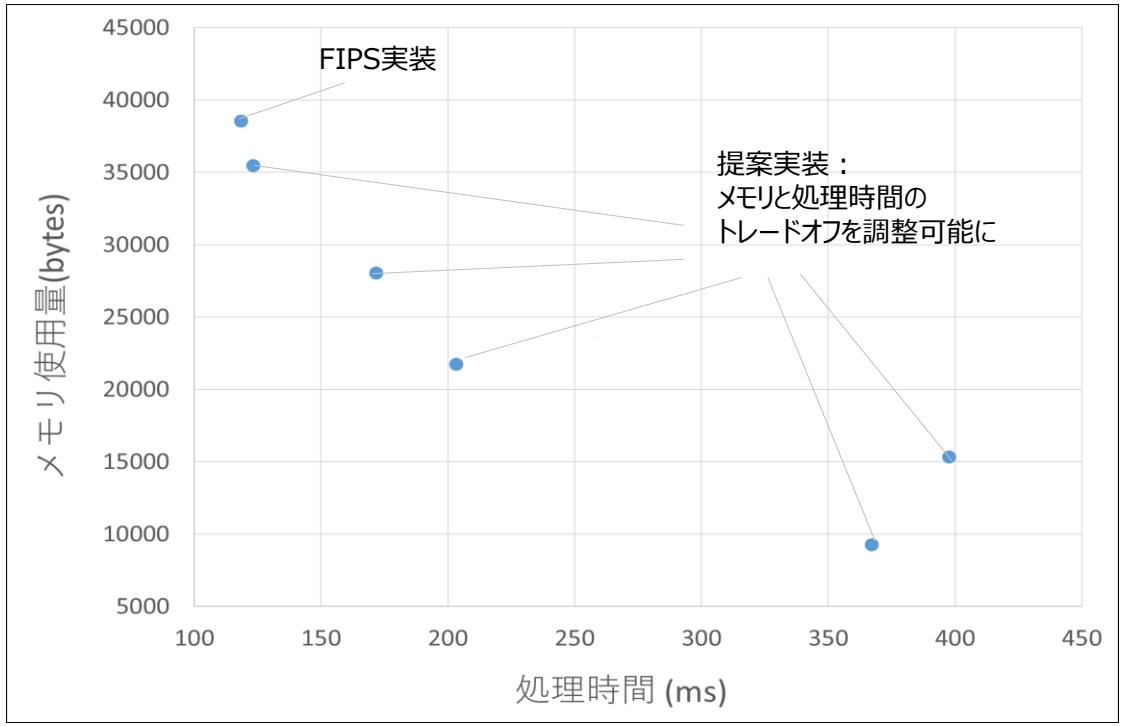


PQC移行に向けた取り組み

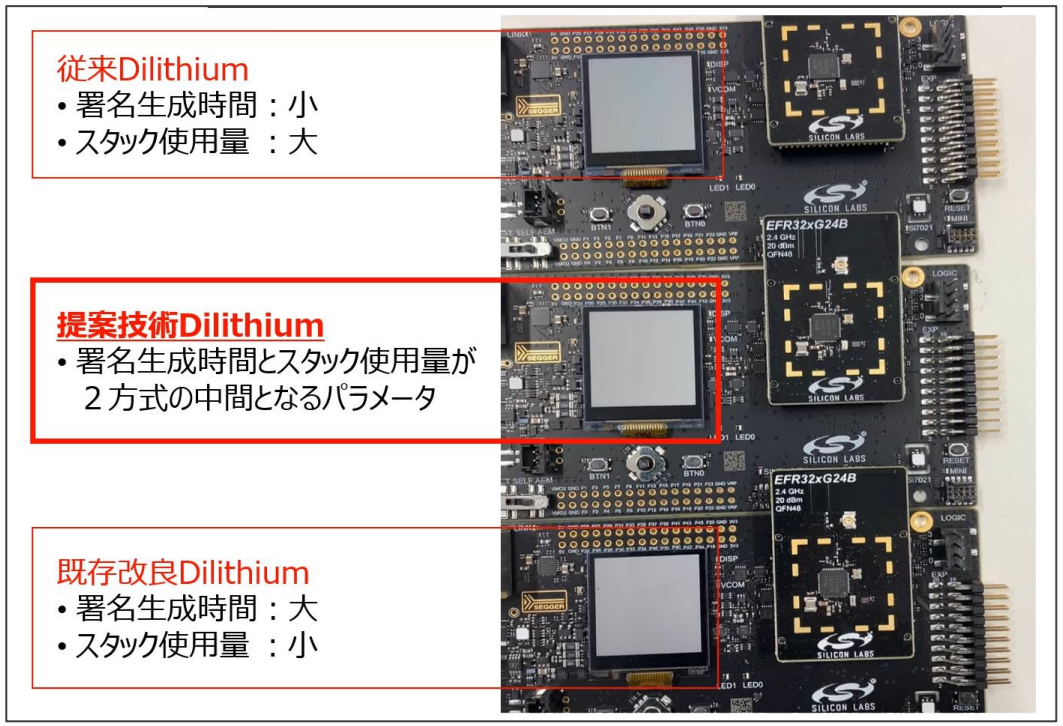
宅内IoT機器環境（省リソース）における課題抽出＆解決技術開発

- 【解決技術】**処理時間スタック使用量パラメトライズ方式**を開発（国際学会発表・国際論文誌採択済）
  - Y. Takahashi et. al, “Parameterizing Time-Memory Trade-off for CRYSTALS-Dilithium and Its Flexible Implementation, IEICE Transactions on Information and Systems, 2025

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



PQC移行に向けた取り組み

IoT機器向けSSL/TLSライブラリ

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

ライブラリへのPQC対応開発

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

省メモリで互換性のあるSSL/TLS通信が可能

軽量・高速

コードサイズ50kB、データサイズ10kB(OpenSSL比1/20)以下でSSL/TLSが高速動作※5。
IoTデバイスのリソースに合わせてソフトウェアのカスタマイズも可能です。

組込み容易

カプセル化されたシンプルなAPIをご提供。簡単かつ安全にSSL/TLSを実装可能です。OpenSSLの置き換えにも対応しています。

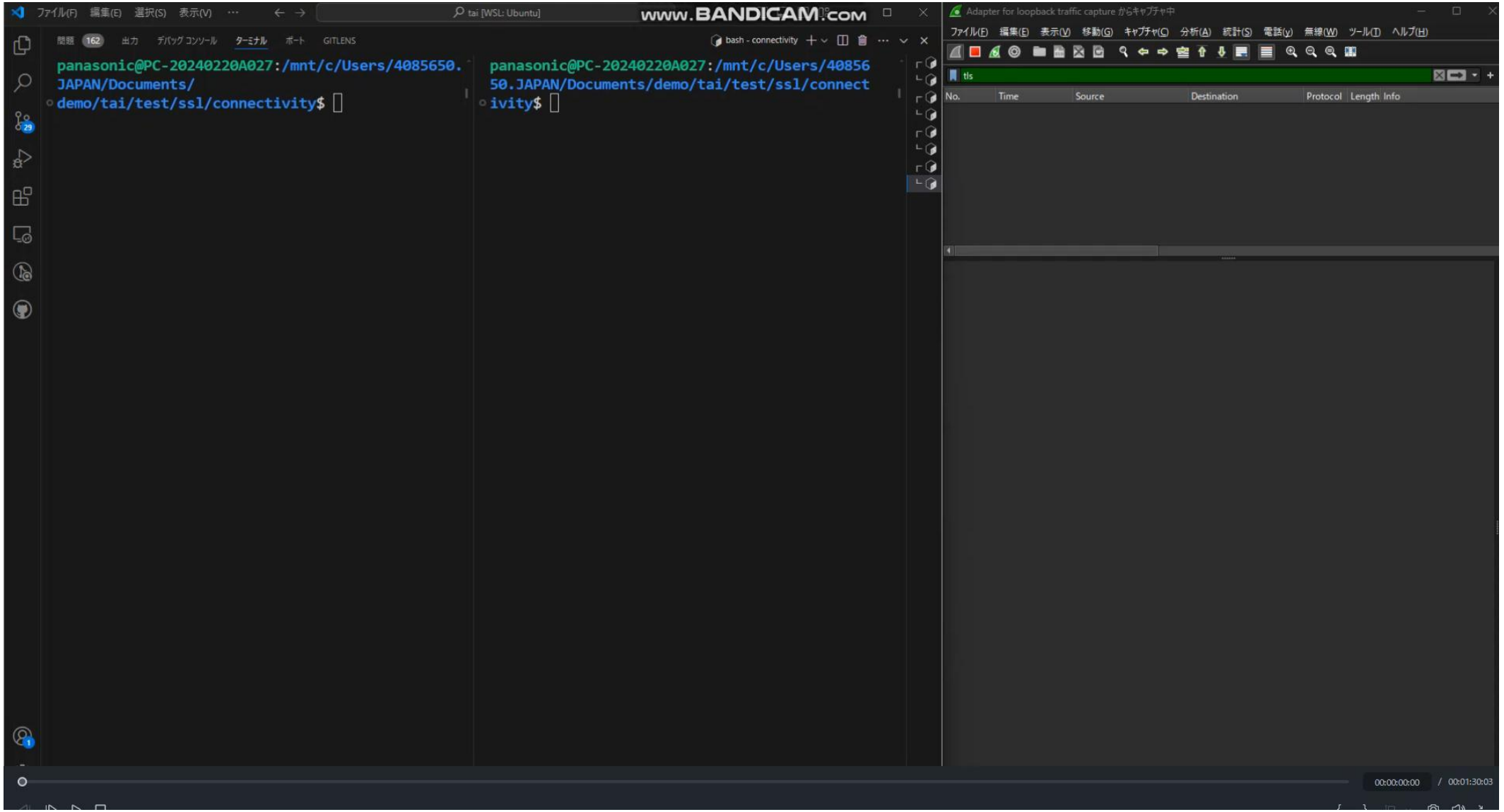
オープンソース不使用

脆弱性が心配なオープンソースソフトウェアは一切不使用。
当社製品で10年以上の搭載実績があり、経験豊富な技術者がメンテナンスしていますので安心です。

※5：当社ソフトウェア最小構成時。OpenSSLデフォルト構成とのメモリサイズ比較において。（2020年3月現在、当社調べ）

PQC移行に向けた取り組み

IoT機器向けSSL/TLSライブラリ（動画）



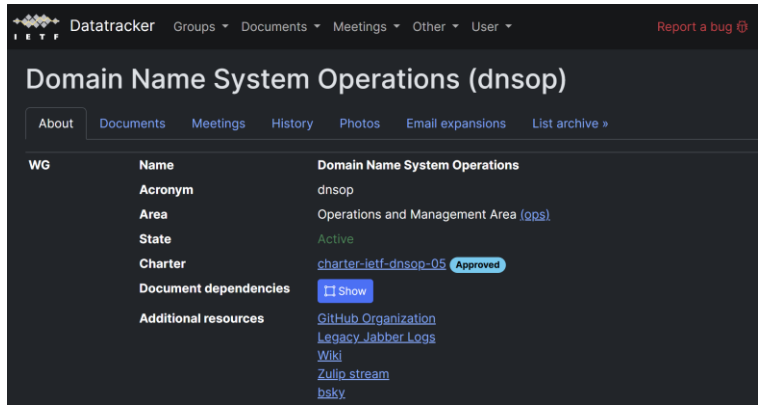
インターネットルーティングプロトコルのPQC移行状況

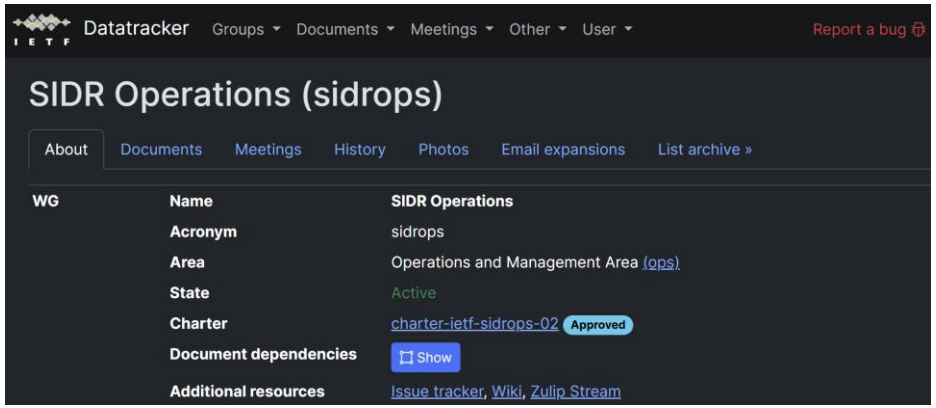
RPKI・BGP

- IETF WG：SIDROPはあるが…
- PQC関連**RFC・IETFドラフトは無い**

DNSSEC

- IETF WG：DNSOP WG (公式), PQ DNSSEC (非公式)はあるが…
- PQC関連**RFC・IETFドラフトは無い**





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移行状況

関連論文：ルーティングプロトコルへのPQC導入

- **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

Response Type	RRs in response	RRs added by DNSSEC (covered RR)	Alexa 1M median TTL (mean)
AAAA	≥ 1 AAAA	1 RRSIG (AAAA)	5 min (0.6 h)
DNSKEY	≥ 1 DNSKEY	1 RRSIG (DNSKEY)	60 min (8.3 h)
Non-existent domain (with NSEC)	SOA	1 RRSIG (SOA) 2 NSEC 2 RRSIG (NSEC)	60 min (2.0 h)
NSEC3 Closest-encloser proof (§5.5 of [33])	SOA	1 RRSIG (SOA) ≥ 3 NSEC3 ≥ 3 RRSIG (NSEC3)	10 min (2.8 h)

Table 1: Records added by DNSSEC and the median time they are cached of the 1M most popular domains [4].

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.

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

議論ポイント

- **PQCについて知っていましたか？**

- **PQCへ（2035年までに）移行しないといけないことは知っていましたか？**

- **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）

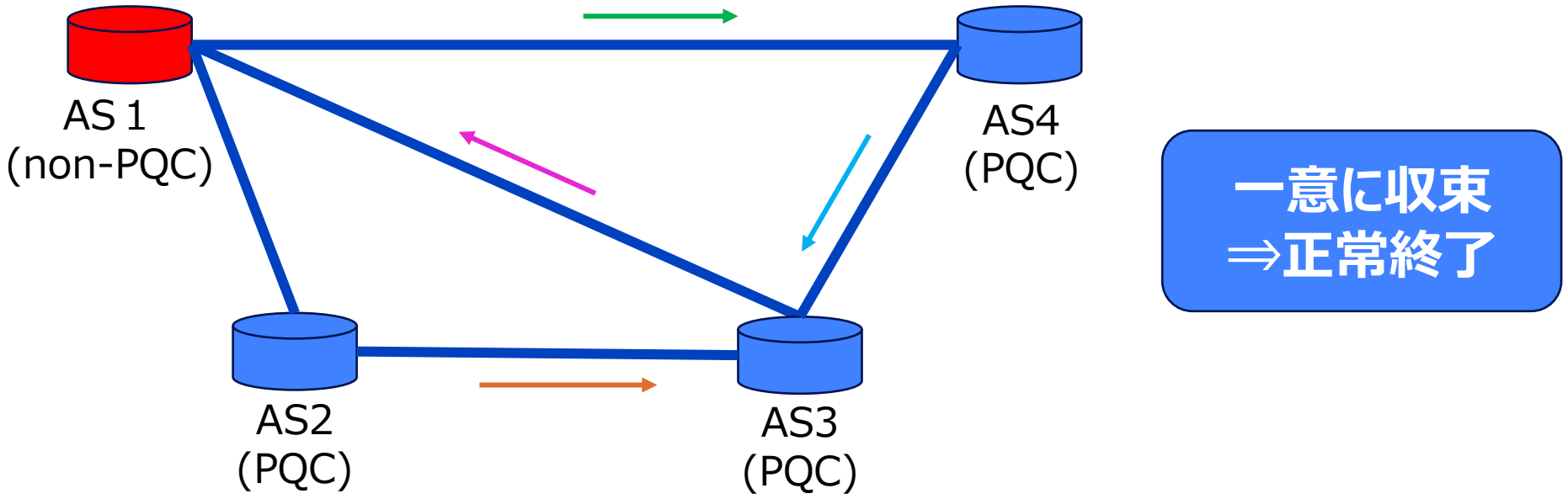
BGPsecに関するPQC移行技術

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

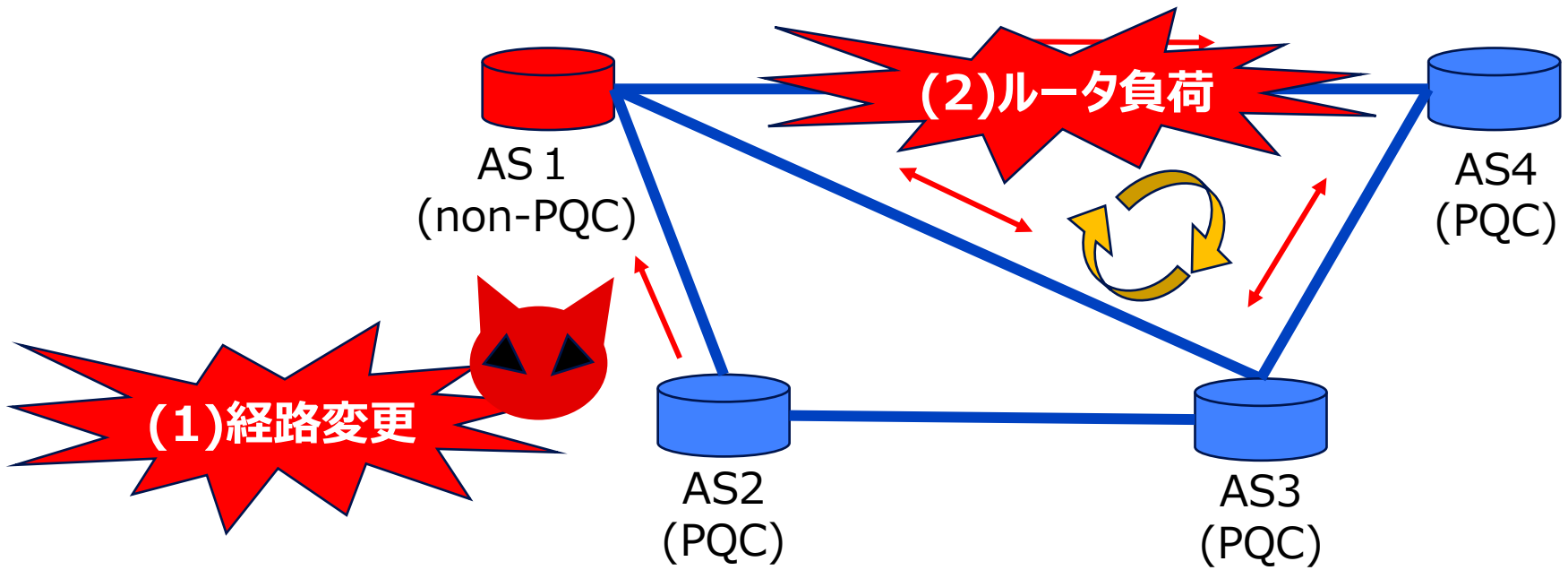


BGPsecに関するPQC移行技術

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]**

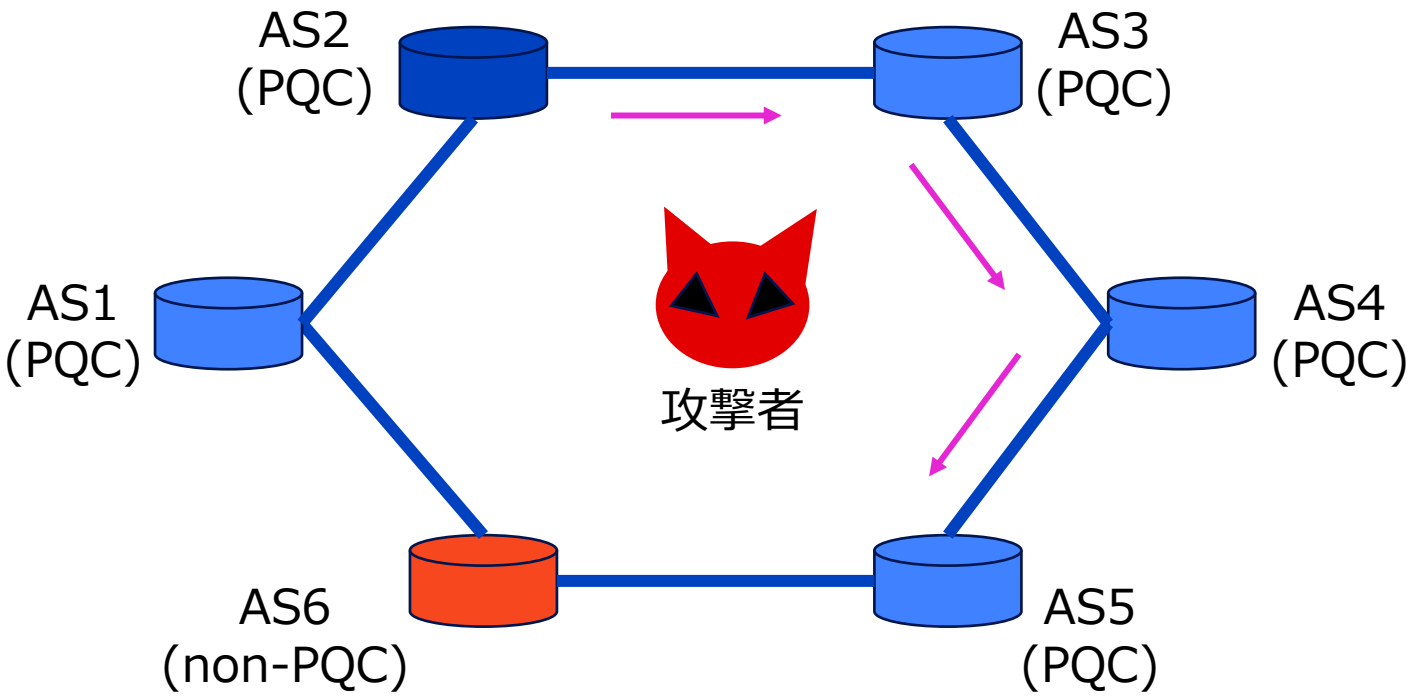
PQC部分導入時に(1)と(2)のそれぞれが起こりうる具体例を発見（今回(1)のみ紹介）



BGPsecに関するPQC移行技術

(1)収束経路が一意でない例＝BGP Wedge

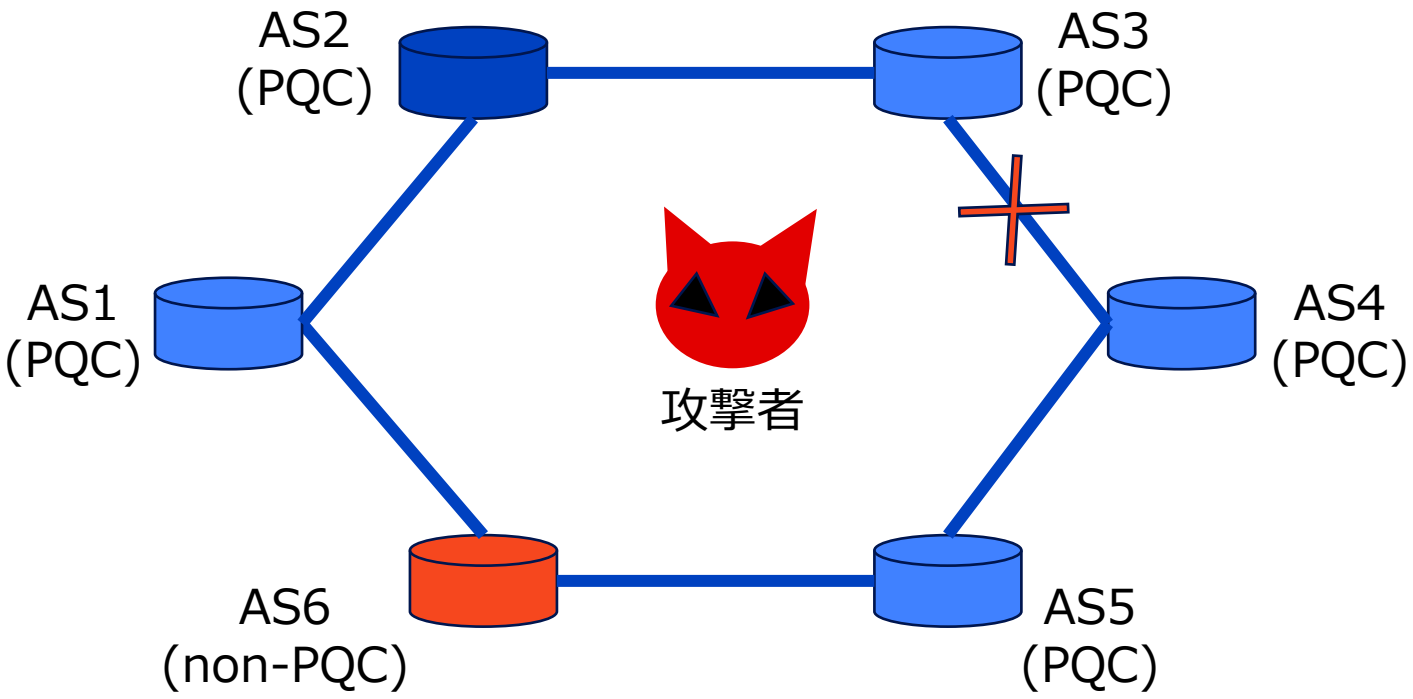
- BGP Wedge[Yang, 2022]：ネットワークが接断した際，意図した安定状態とは別状態に収束する
- PQC部分導入時に、攻撃者は**non-PQCのASを通るような収束経路に変更する攻撃**が可能



BGPsecに関するPQC移行技術

(1)収束経路が一意でない例＝BGP Wedge

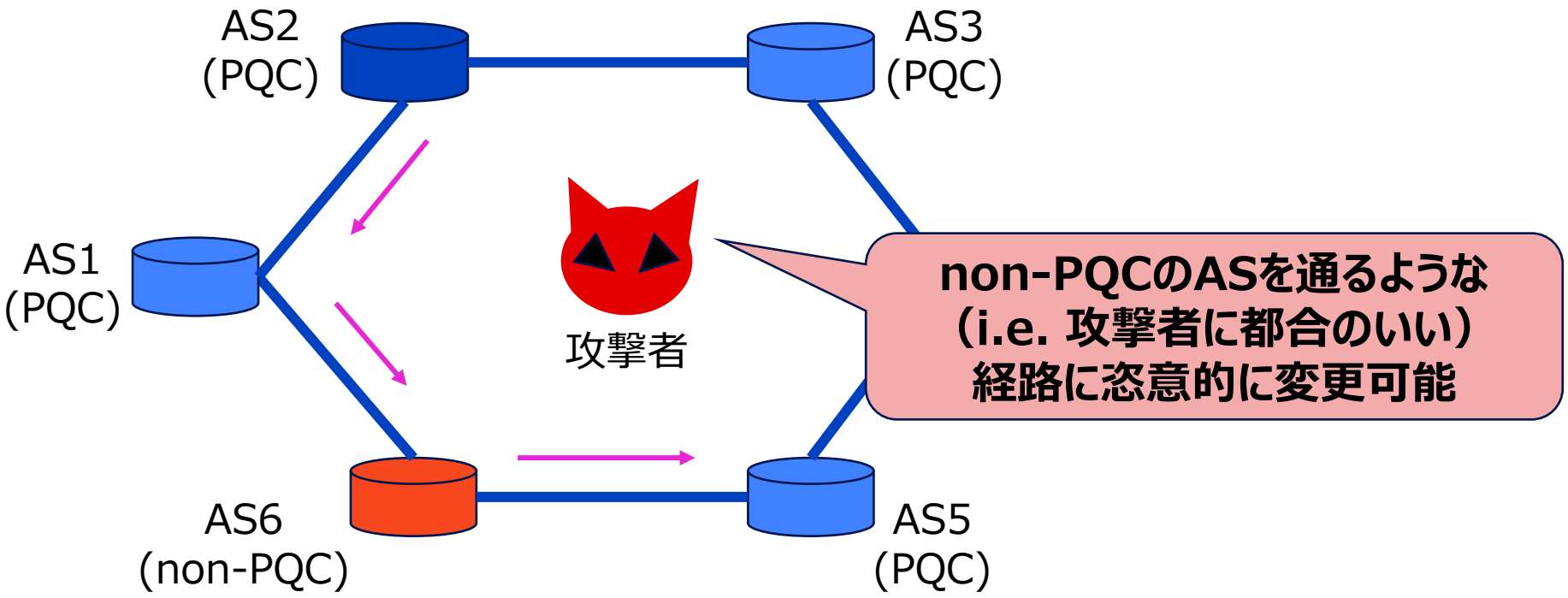
- BGP Wedge[Yang, 2022]：ネットワークが接断した際，意図した安定状態とは別状態に収束する
- PQC部分導入時に、攻撃者は**non-PQCのASを通るような収束経路に変更する攻撃**が可能



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



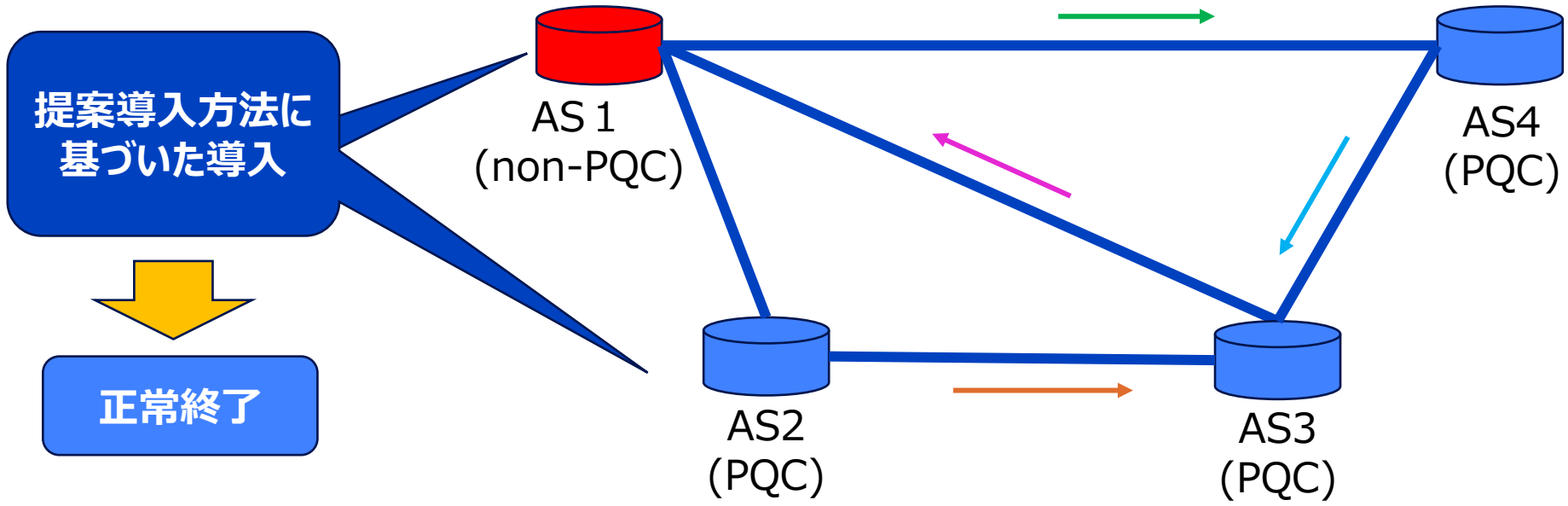
BGPsecに関するPQC移行技術

【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



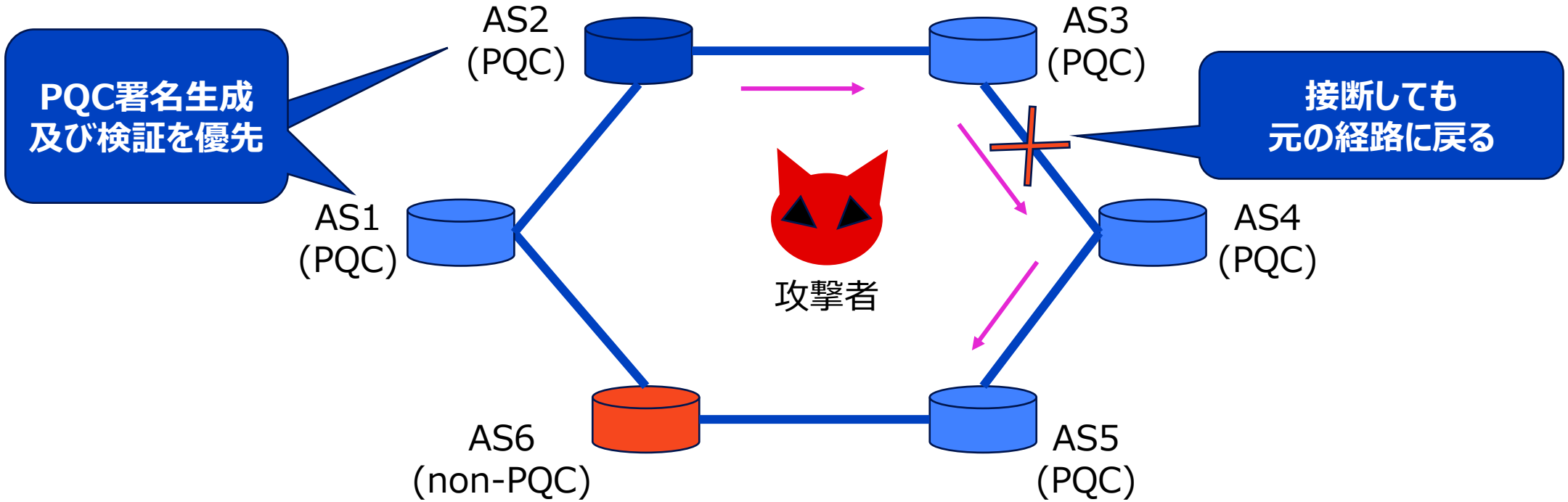
BGPsecに関するPQC移行技術

【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



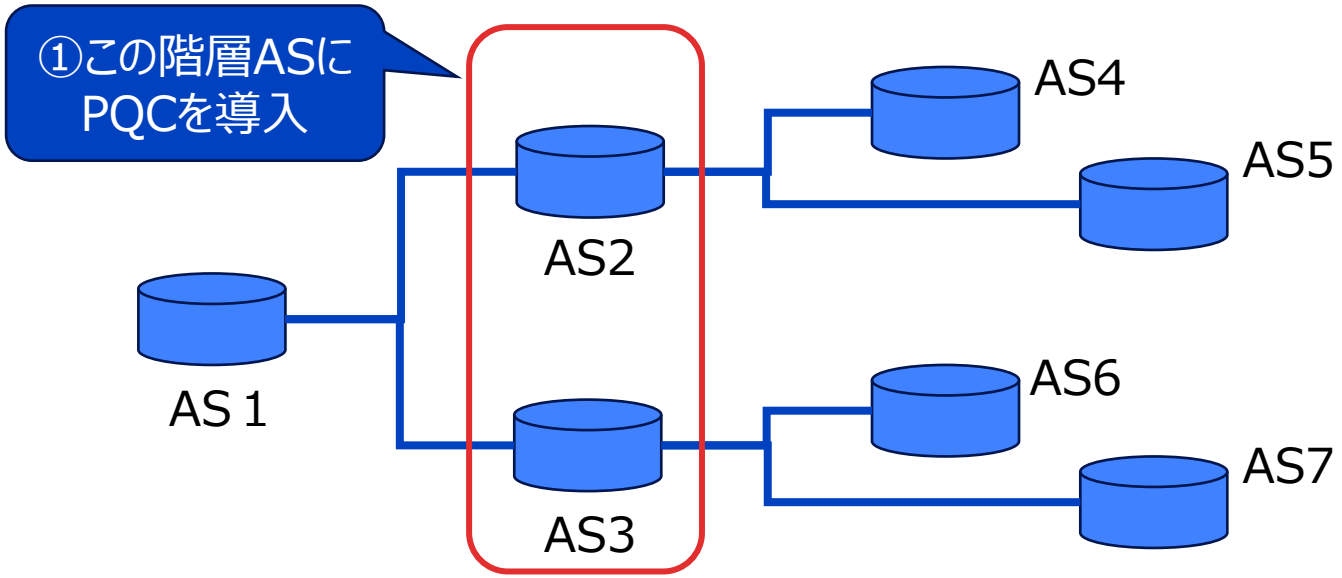
BGPsecに関するPQC移行技術

【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



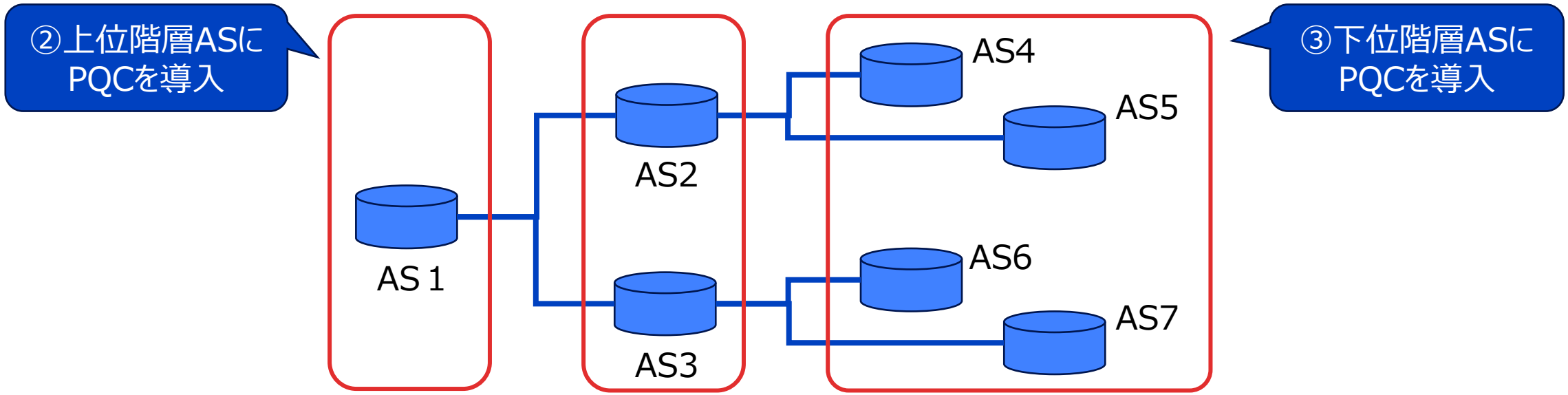
BGPsecに関するPQC移行技術

【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**

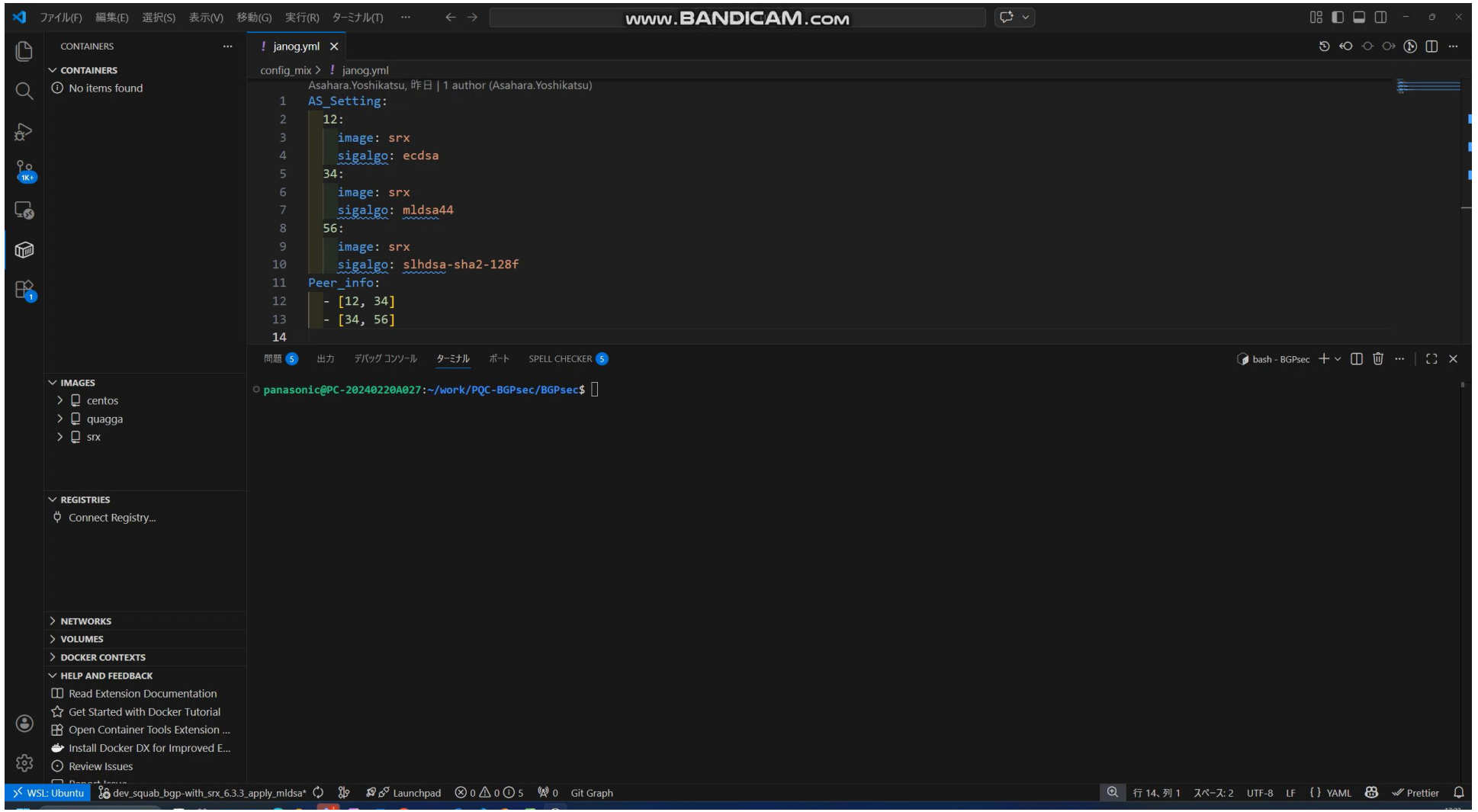
(2)に対処する導入方法：階層単位でのPQC導入順序

- 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



BGPsecに関するPQC移行技術

PQC対応BGPsecネットワーク構築デモ（動画）



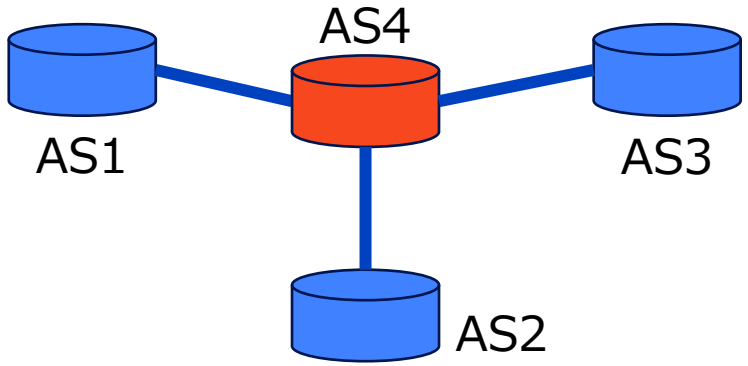
今後の研究：ネットワークトポロジーの特徴量を利用したPQC導入

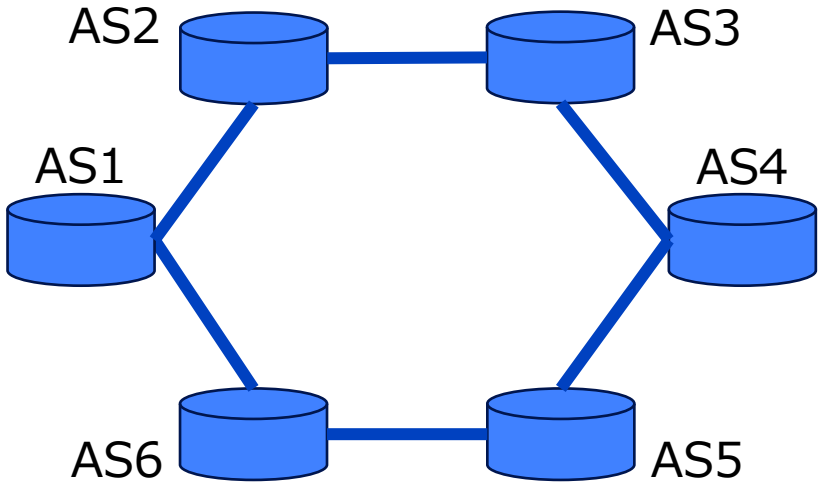
中心性を利用したPQC導入順序

- (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





議論ポイント

- **PQCについて知っていましたか？**

- **PQCへ（2035年までに）移行しないといけないことは知っていましたか？**

- **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）

幸せの、チカラに。

Panasonic Digital Transformation & Cyber-Physical Systems Division