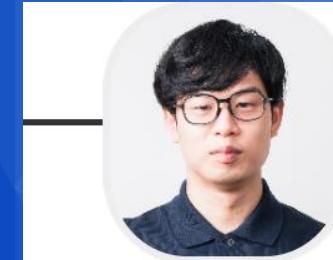


# 量子計算機時代に向けた 安全なネットワークの実現 ～耐量子計算機暗号～

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



高橋 康  
パナソニック ホールディングス株式会社  
Yasushi Takahashi



矢内 直人  
パナソニック ホールディングス株式会社  
Naoto Yanai

# 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

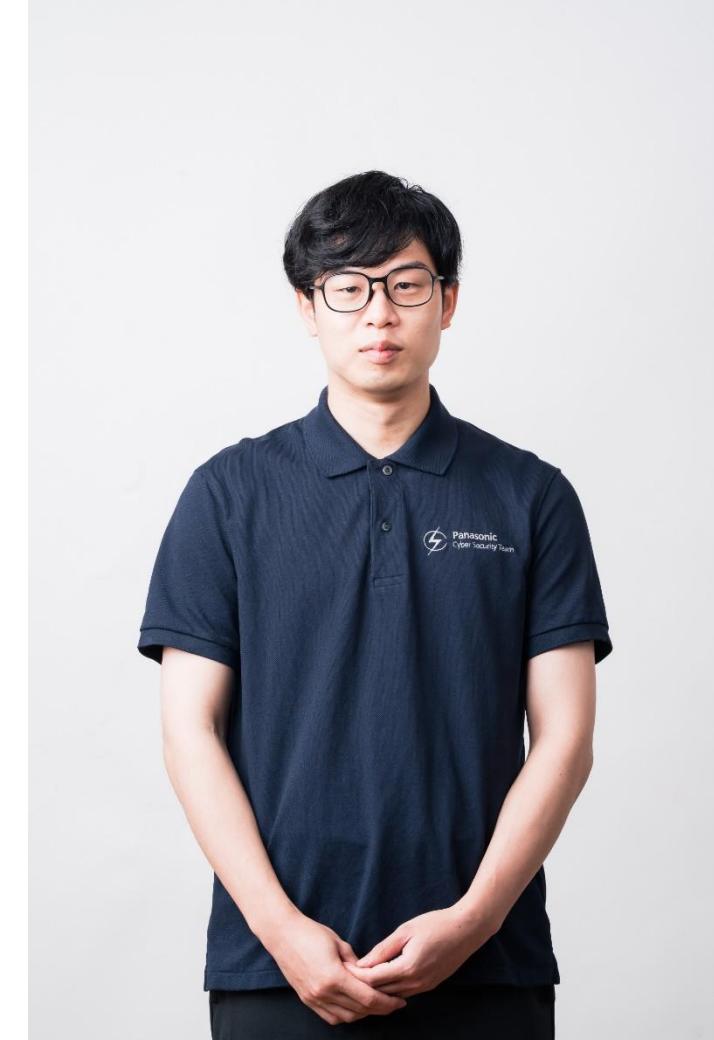
- ・ 2019年-2022年：富士通株式会社
  - ・ 2022年-現在：パナソニックホールディングス株式会社  
一貫して暗号に関するR&D業務を担当（ネットワーク素人です）
- JANOG参加は2回目**（前回が初参加）

## 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

- 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 → 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 → 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険化 -> 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)

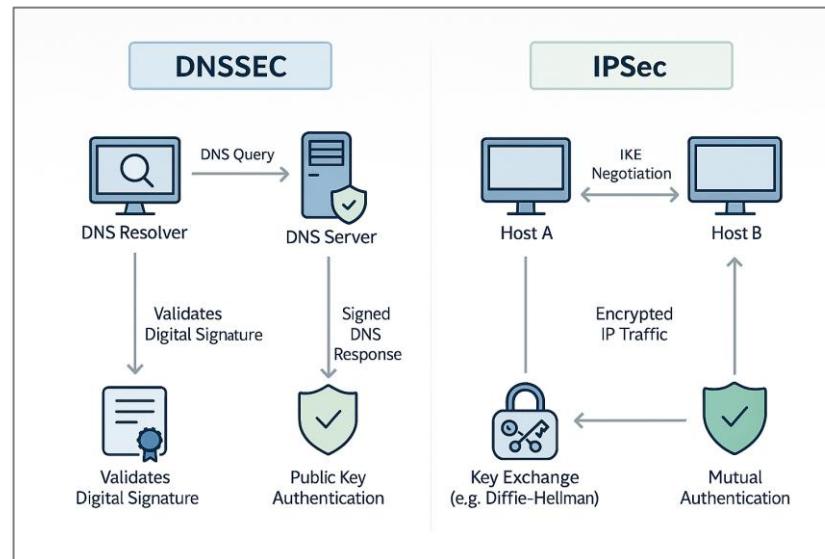
## 質疑＆議論(20分)

## ネットワークにおける認証・鍵交換の必要性

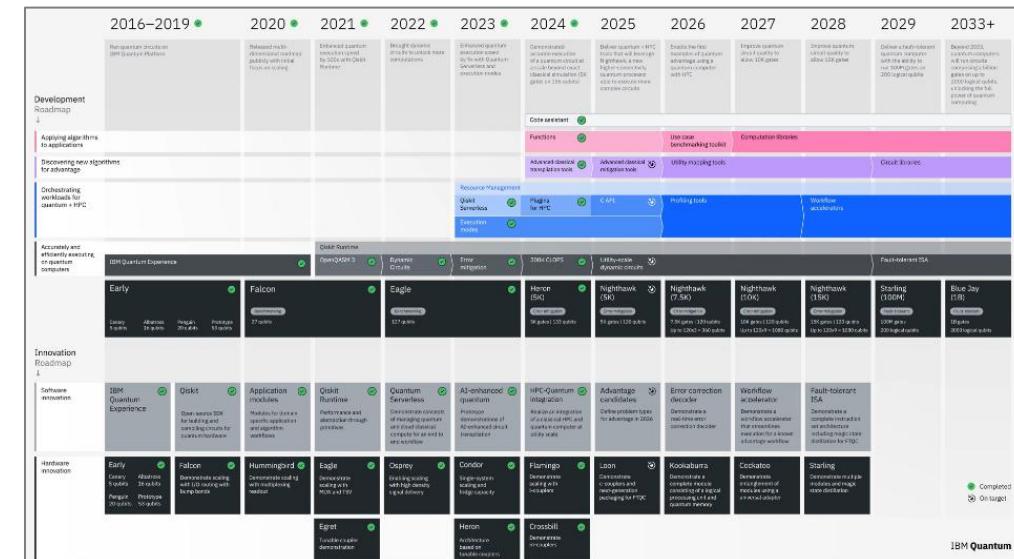
- DNSSEC、IPsecなどで認証・鍵交換が必要 <- 公開鍵暗号と呼ばれる技術が安全性を保証

## 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=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  
⇒ 今之内からPQCの標準化・移行準備が進む



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

- 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 → 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 → 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)

## 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](#)

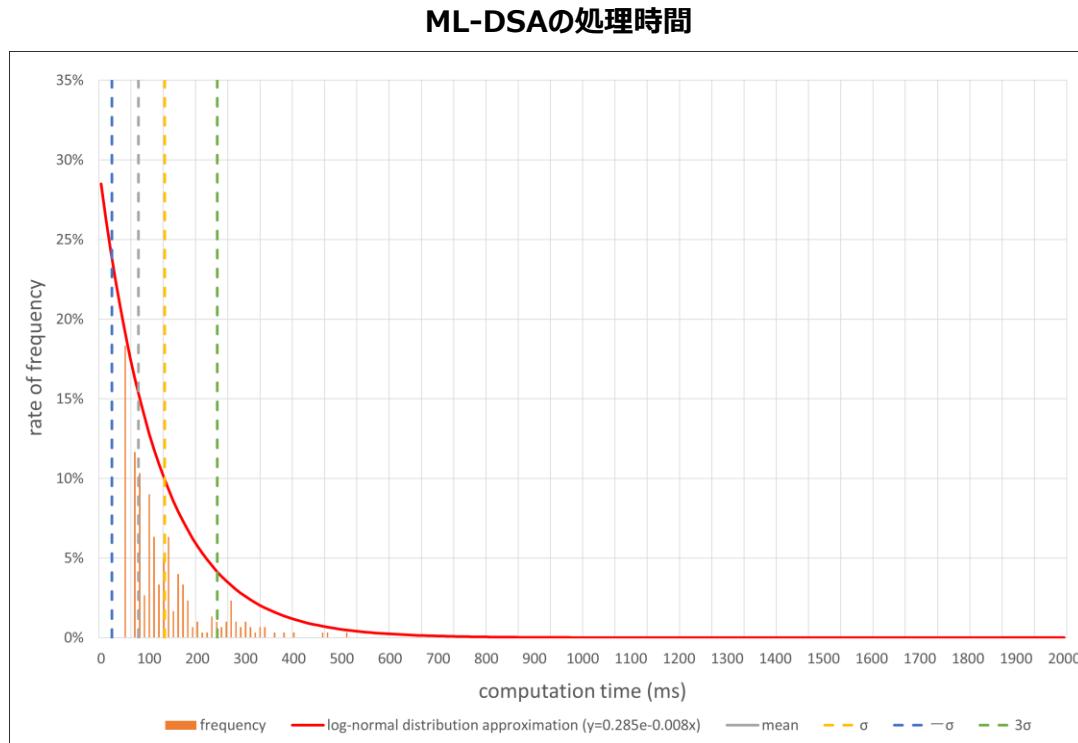
Post-Quantum Use In Protocols (pquip)	
About	
<a href="#">Documents</a>	<a href="#">Meetings</a>
<a href="#">History</a>	<a href="#">Photos</a>
<a href="#">Email expansions</a>	<a href="#">List archive »</a>
<b>WG</b>	<b>Name</b> <a href="#">Post-Quantum Use In Protocols</a>
	<b>Acronym</b> pquip
	<b>Area</b> Security Area ( <a href="#">sec</a> )
	<b>State</b> Active
	<b>Charter</b> <a href="#">charter-ietf-pquip-01</a> <span>Approved</span>
	<b>Document dependencies</b> <a href="#">Show</a>
	<b>Additional resources</b> GitHub Organization <a href="#">Grand list of WGs and protocols looking at PQC algorithms</a>
<b>Personnel</b>	<b>Chairs</b> <a href="#">Paul E. Hoffman</a> , <a href="#">Sofia Cell</a>
	<b>Area Director</b> <a href="#">Paul Wouters</a>
<b>Mailing list</b>	<b>Address</b> <a href="mailto:pqc@ietf.org">pqc@ietf.org</a>
	<b>To subscribe</b> <a href="https://www.ietf.org/mailman/listinfo/pqc">https://www.ietf.org/mailman/listinfo/pqc</a>
	<b>Archive</b> <a href="https://mailarchive.ietf.org/arch/browse/pqc/">https://mailarchive.ietf.org/arch/browse/pqc/</a>
<b>Chat</b>	<b>Room address</b> <a href="https://zulip.ietf.org/#narrow/stream/pquip">https://zulip.ietf.org/#narrow/stream/pquip</a>
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	

Terminology for Post-Quantum Traditional Hybrid Schemes	
RFC 9794	
<a href="#">Status</a> <a href="#">Email expansions</a> <a href="#">History</a>	
<a href="#">draft-driscoll-pqt-hybrid-terminology</a>	00 01 02 03 04 05 06
<a href="#">draft-ietf-pquip-pqt-hybrid-terminology</a>	00 01 02 03 04 05 06
<a href="#">rfc9794</a>	rfc9794
<b>Document</b>	<b>Type</b> <a href="#">RFC - Informational (June 2025)</a> Was <a href="#">draft-ietf-pquip-pqt-hybrid-terminology</a> ( <a href="#">pquip WG</a> )
	<b>Authors</b> <a href="#">Flo D</a> ✉, <a href="#">Michael P</a> ✉, <a href="#">Britta Hale</a> ✉
	<b>Last updated</b> 2025-06-13
	<b>RFC stream</b> Internet Engineering Task Force (IETF)
	<b>Formats</b> <a href="#">txt</a> <a href="#">html</a> <a href="#">xml</a> <a href="#">pdf</a> <a href="#">htmlized</a> <a href="#">bibtex</a>
	<b>Additional resources</b> <a href="#">Mailing list discussion</a>
<b>IESG</b>	<b>Responsible AD</b> <a href="#">Paul Wouters</a> ✉ <b>Send notices to</b> (None)
<a href="#">✉ Email authors</a> <a href="#">✉ Email WG</a> <a href="#">↳ IPR</a> <a href="#">← References</a> <a href="#">→ Referenced by</a> <a href="#">Search Lists</a>	

- 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 → 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 → 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)

## 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）



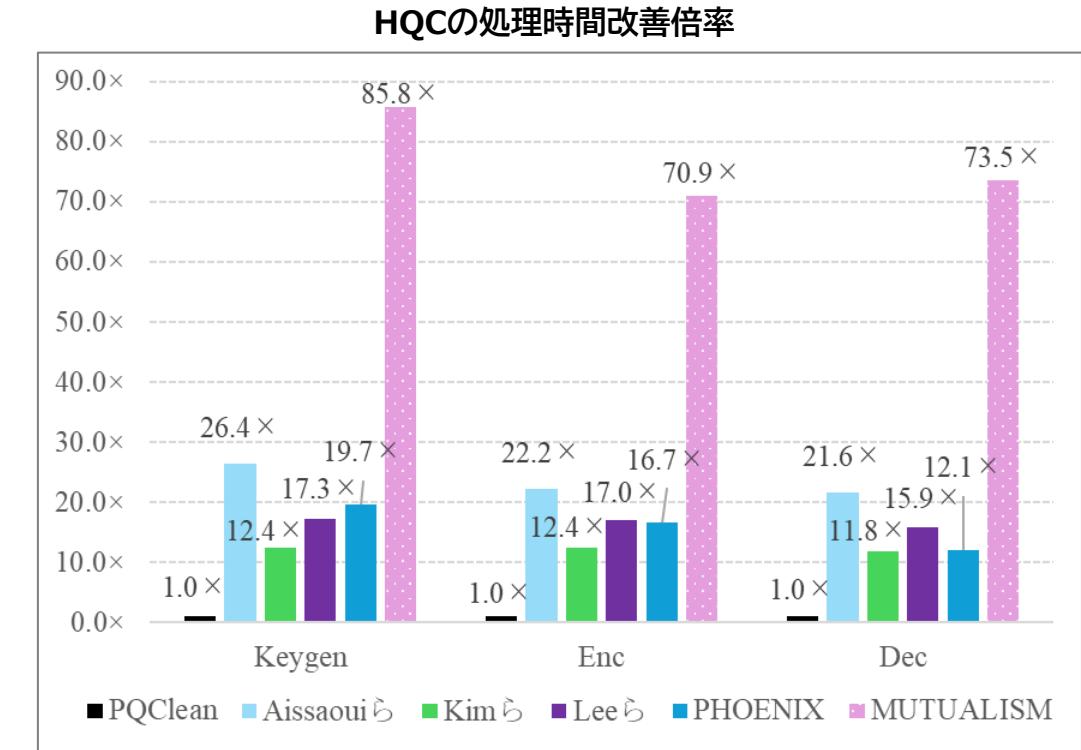
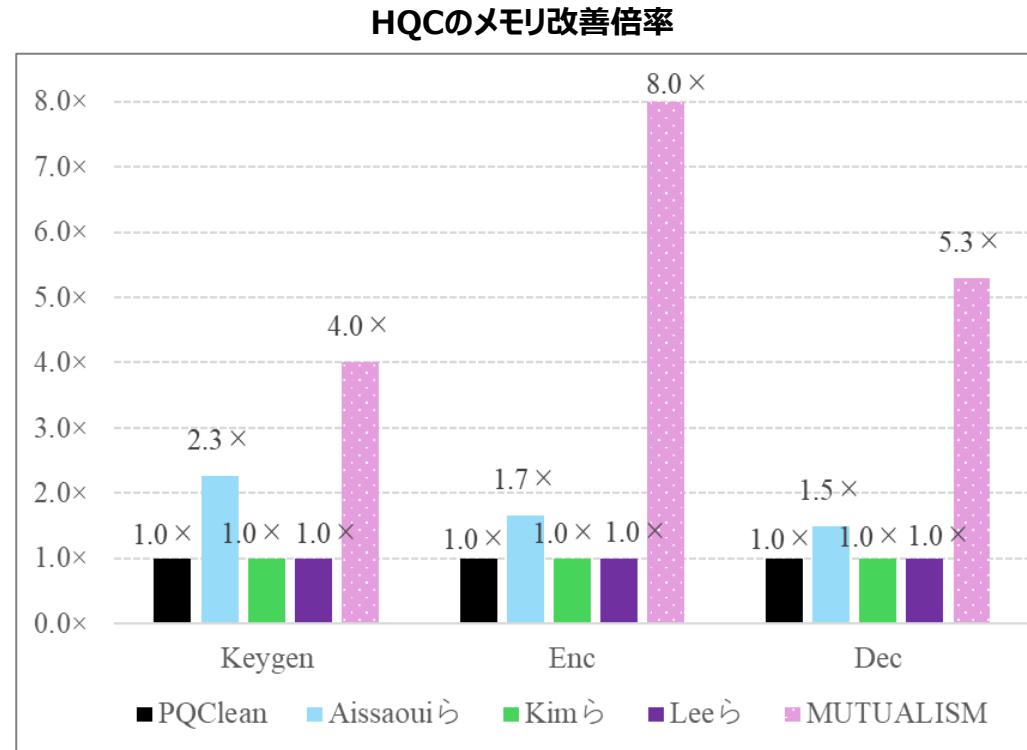
ML-DSAのスタック消費量

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

## 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

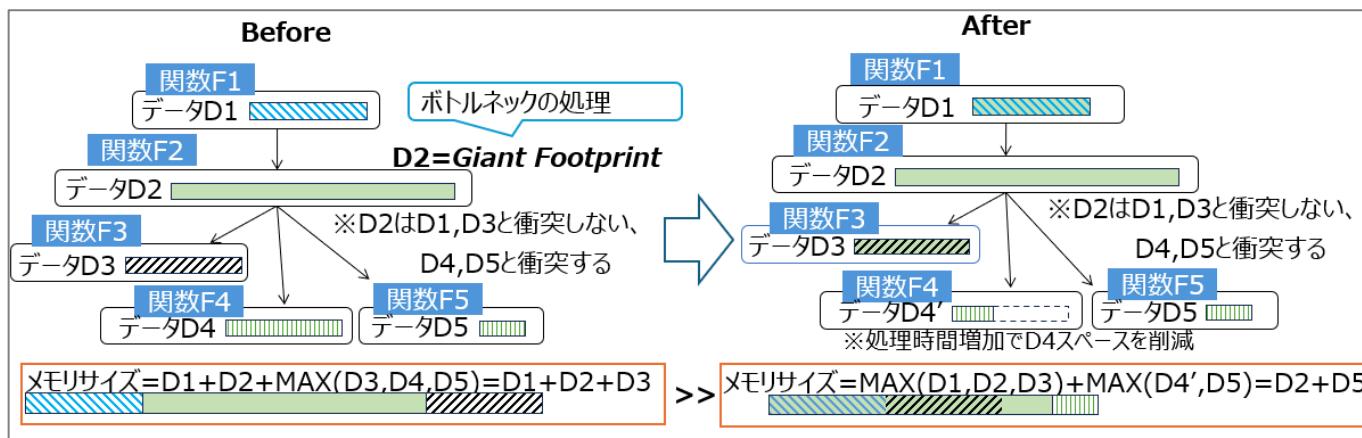
- 【解決技術】処理時間とメモリ使用量両方の削減方式を開発（国内学会発表済）
  - 劉ら，“HQCの省リソース機器向けソフトウェア実装”，暗号と情報セキュリティシンポジウム(SCIS), 2F1-1, 2026.



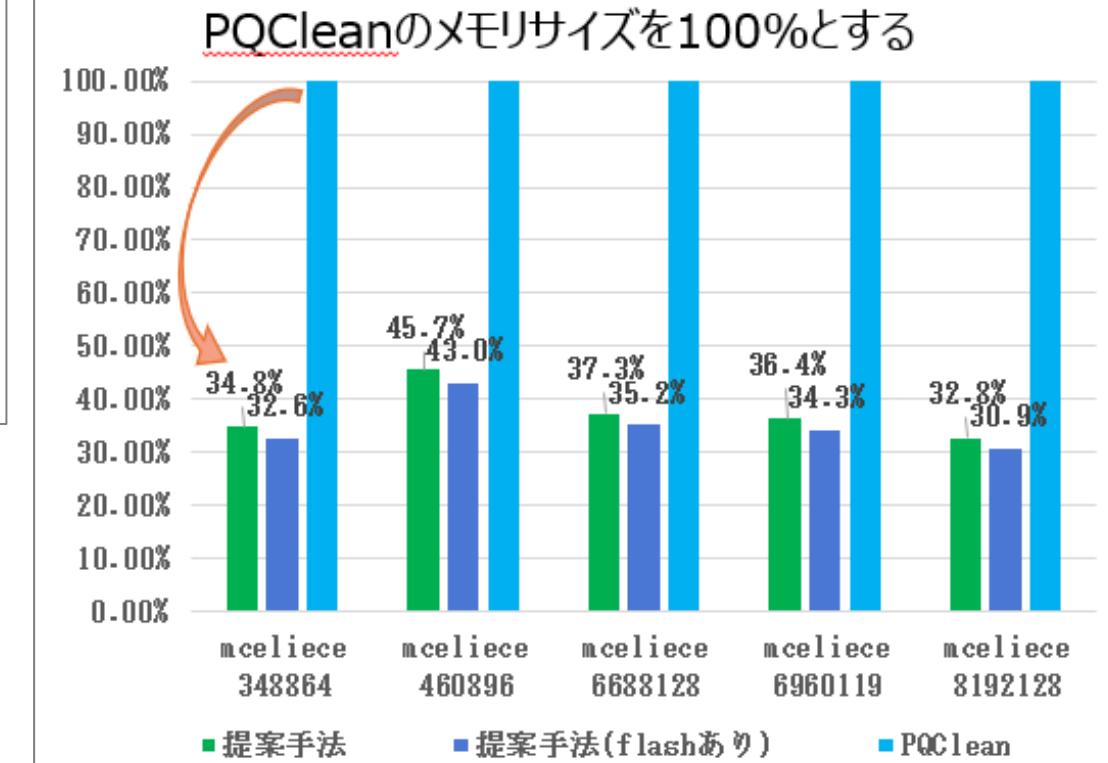
## 宅内IoT機器環境（省リソース）における課題抽出＆解決技術開発

- 【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



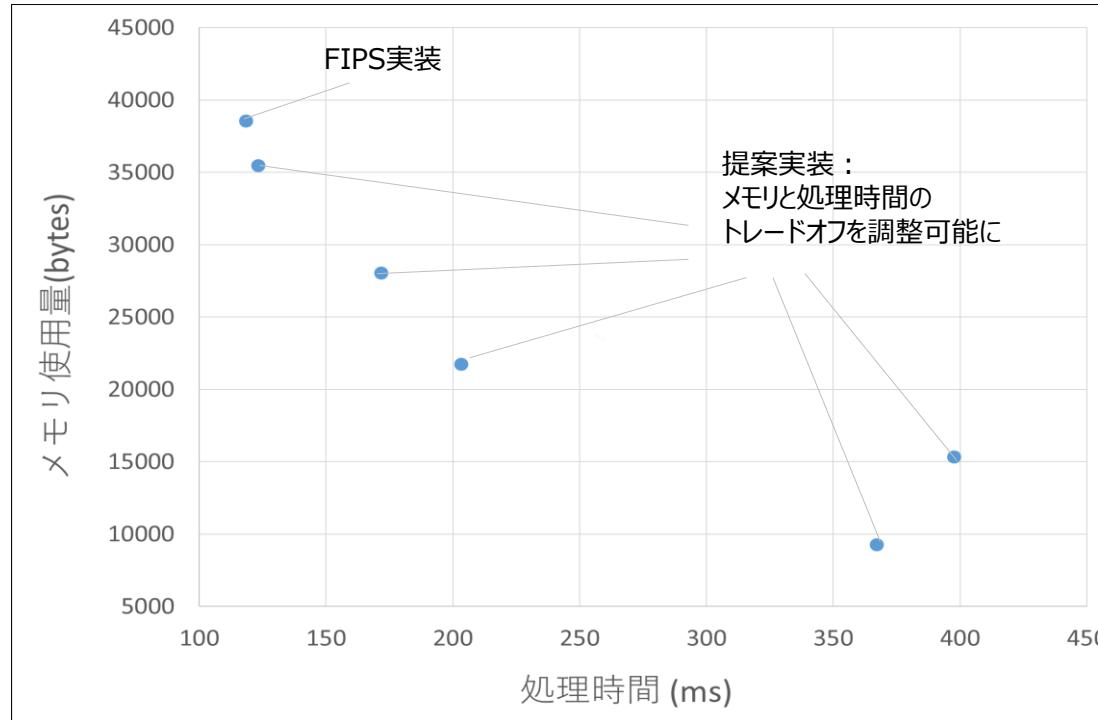
McElieceのメモリ削減倍率



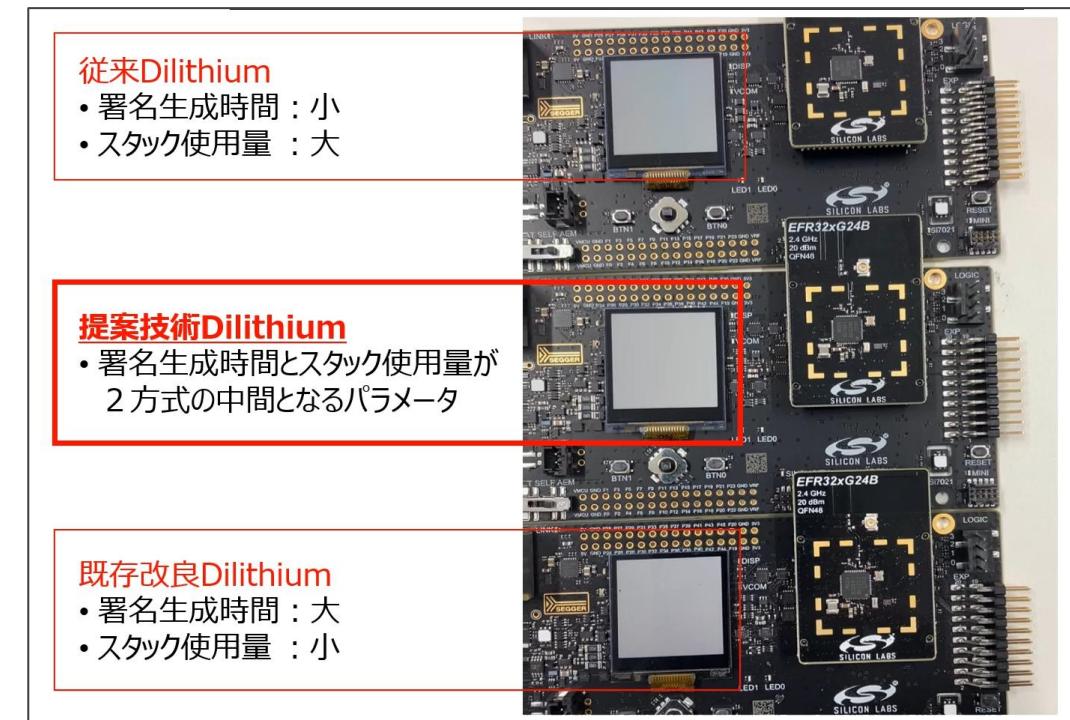
## 宅内IoT機器環境（省リソース）における課題抽出＆解決技術開発

- 【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



## 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

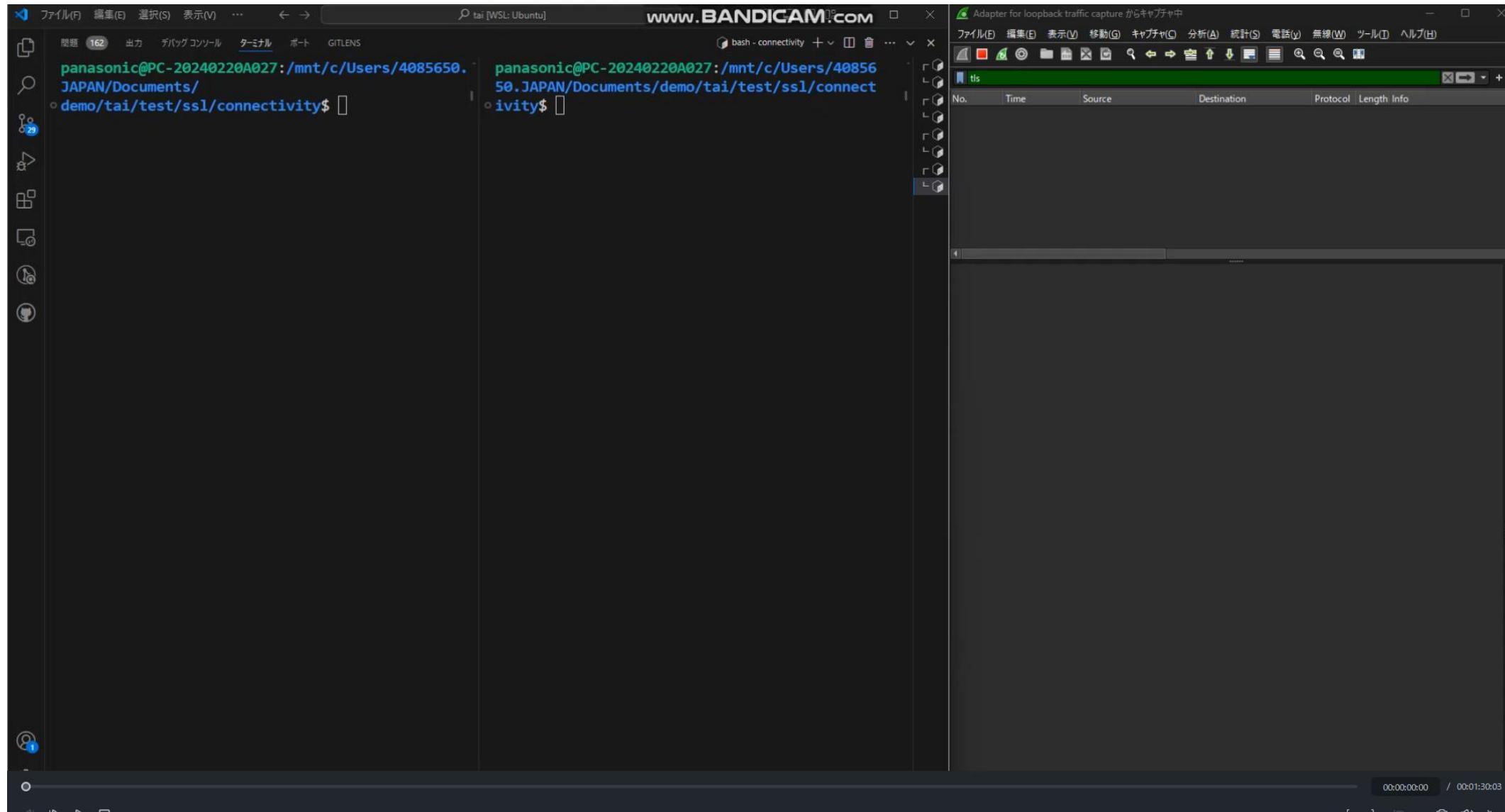
カプセル化されたシンプルなAPIを  
ご提供。簡単かつ安全にSSL/TLSを  
実装可能です。OpenSSLの置き換え  
にも対応しています。



### 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。

## IoT機器向けSSL/TLSライブラリ（動画）

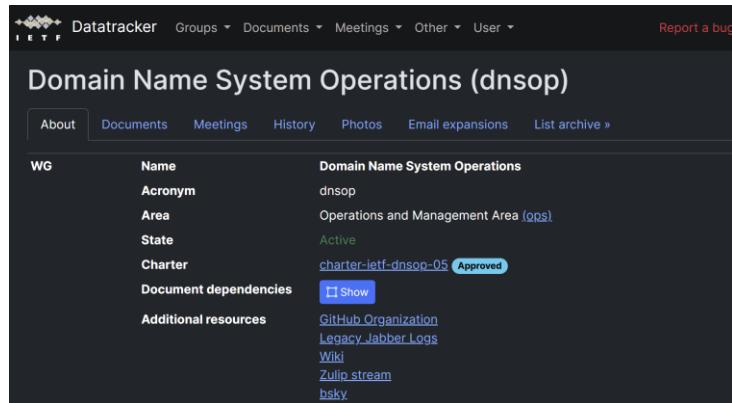


## RPKI・BGP

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

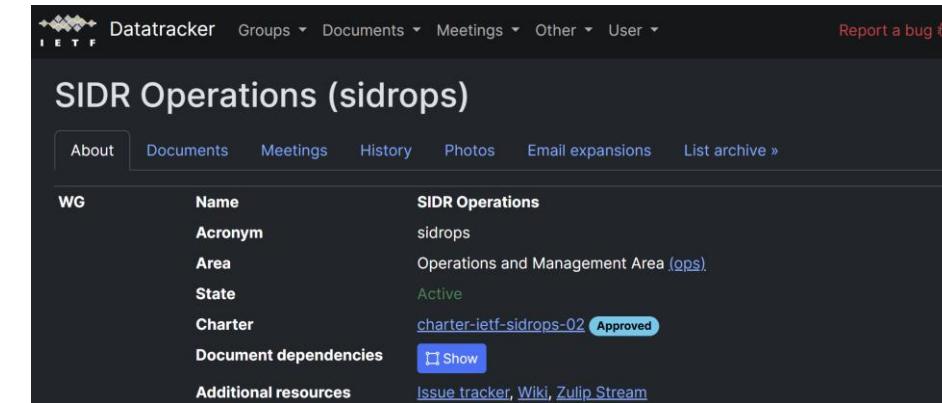
## DNSSEC

- 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



The screenshot shows the IETF Datatracker interface for the Domain Name System Operations (dnsop) Working Group. The page title is "Domain Name System Operations (dnsop)". The "About" tab is selected. Key information displayed includes:

WG	Name	Domain Name System Operations
Acronym	dnsop	
Area	Operations and Management Area	<a href="#">(ops)</a>
State	Active	
Charter	<a href="#">charter-ietf-dnsop-05</a>	<span>Approved</span>
Document dependencies	<a href="#">Show</a>	
Additional resources	<a href="#">GitHub Organization</a> <a href="#">Legacy Jabber Logs</a> <a href="#">Wiki</a> <a href="#">Zulip stream</a> <a href="#">bsky</a>	



The screenshot shows the IETF Datatracker interface for the SIDR Operations (sidrops) Working Group. The page title is "SIDR Operations (sidrops)". The "About" tab is selected. Key information displayed includes:

WG	Name	SIDR Operations
Acronym	sidrops	
Area	Operations and Management Area	<a href="#">(ops)</a>
State	Active	
Charter	<a href="#">charter-ietf-sidrops-02</a>	<span>Approved</span>
Document dependencies	<a href="#">Show</a>	
Additional resources	<a href="#">Issue tracker</a> , <a href="#">Wiki</a> , <a href="#">Zulip Stream</a>	

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

## 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 <sup>+</sup> -Haraka-128s [11]	Candidate	Hash	64B	32B	8kB		
Picnic-L1-F5 [17]	Candidate	Hash	16B	32B	34kB		
Picnic2-L1-F5 [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.

**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**

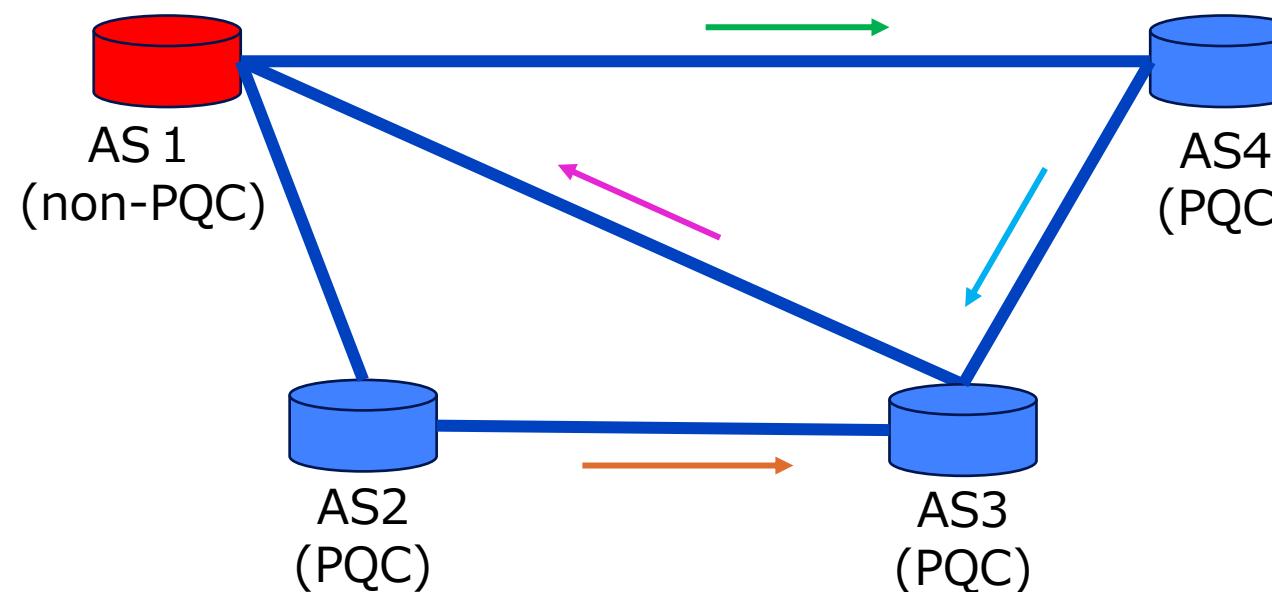
- PQCについて知っていましたか？
- PQCへ（2035年までに）移行しないといけないことは知っていましたか？
- PQC移行に着手されていますか？
  - されている → いつから着手していて、どのくらい移行が進んでいますか？
  - されていない → PQC動向のキャッチアップはされていますか？  
いつから着手するという予定はありますか？
- PQC移行において課題になりそうなことは何でしょうか？  
(例えばパケットサイズの増大、次世代ルータの処理性能不足など)

## 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

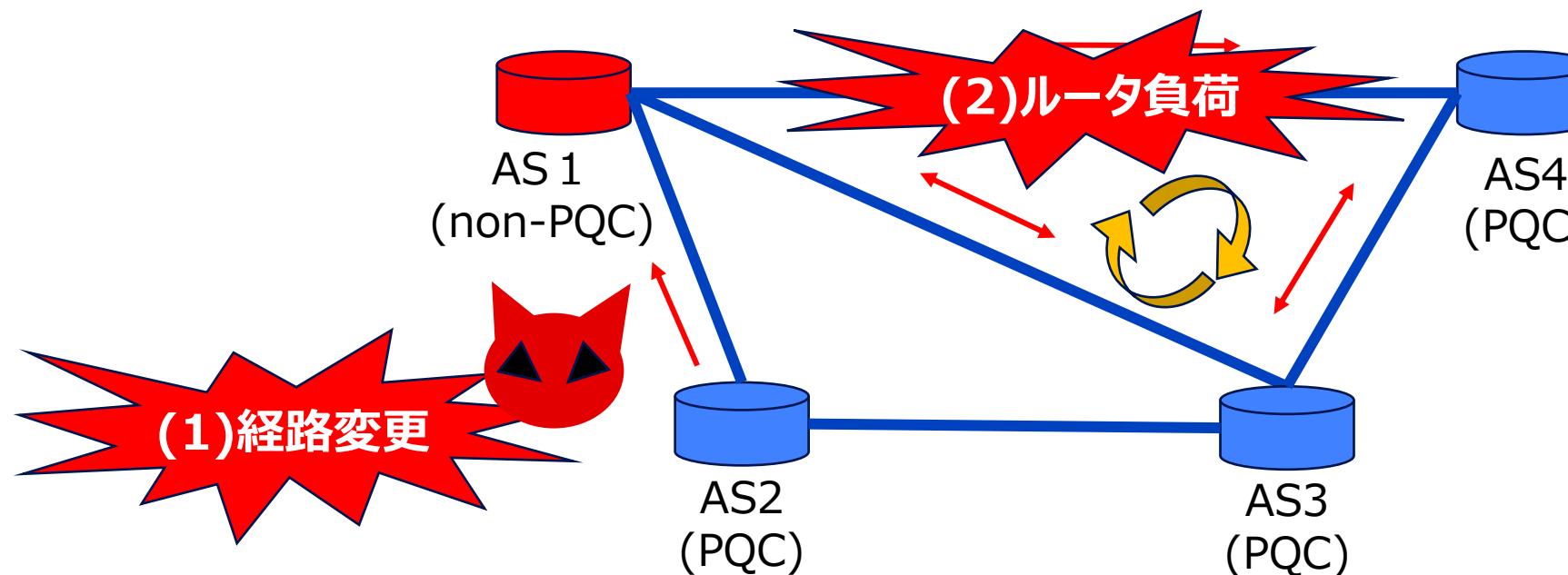
- この性質が満たされると、BGPは安全かつ正常に実行終了



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

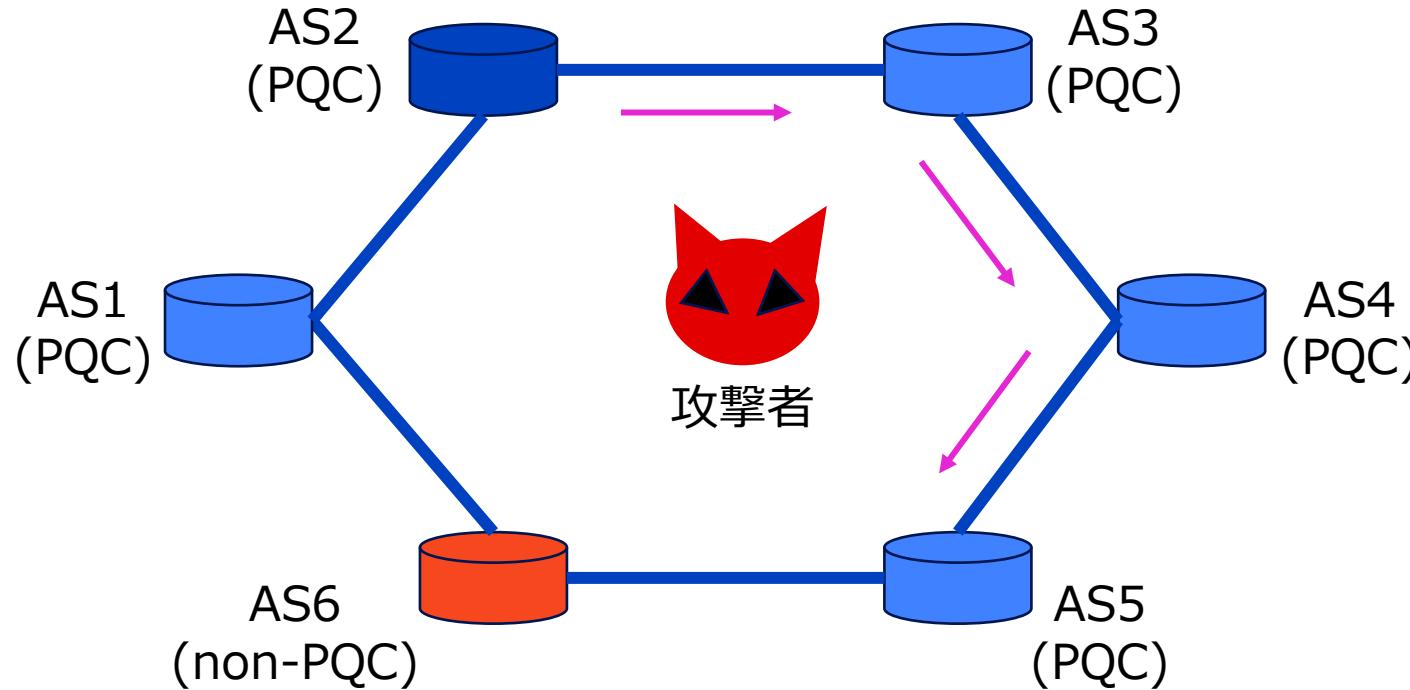
- ・ (1) 収束経路が一意でない -> 攻撃者による経路変更攻撃 [Maria, 2017]
- ・ (2) 経路が収束しない -> ルータへの負荷増加 [Yang, 2022]

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）



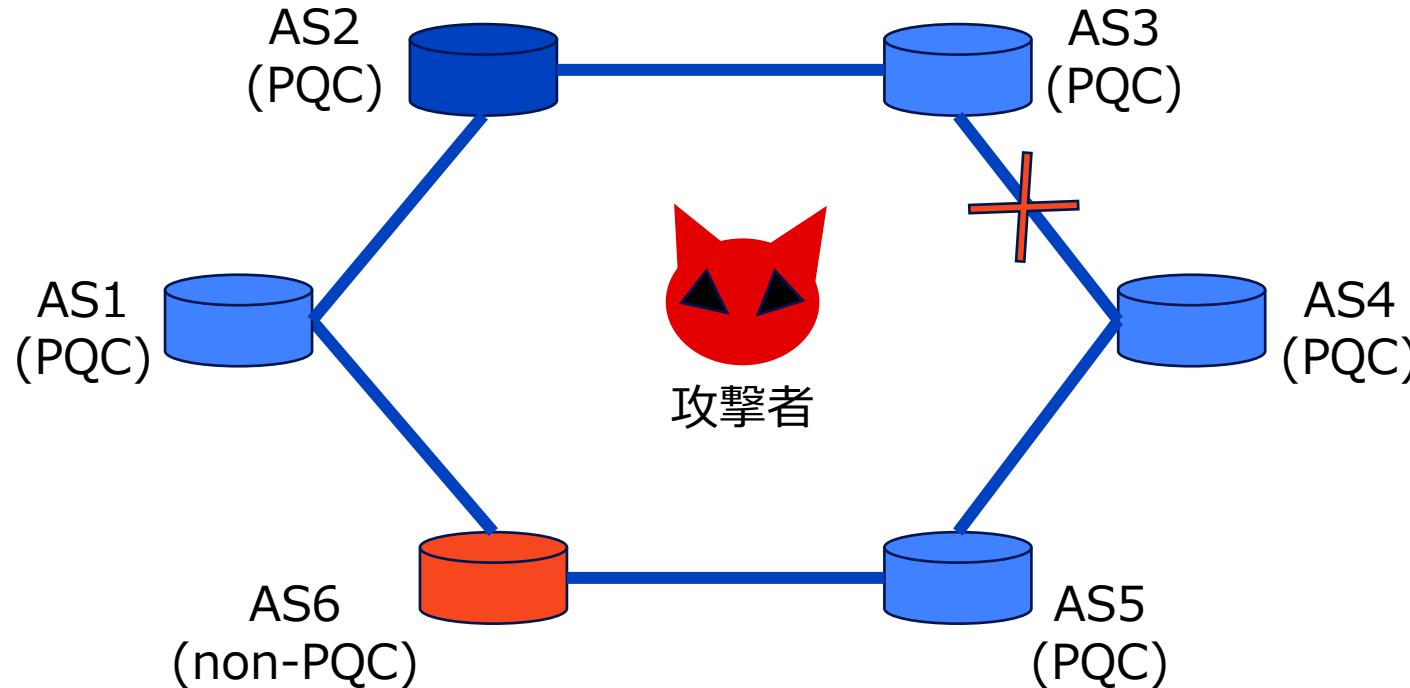
## (1) 収束経路が一意でない例 = BGP Wedge

- BGP Wedge[Yang, 2022] : ネットワークが接続した際, 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



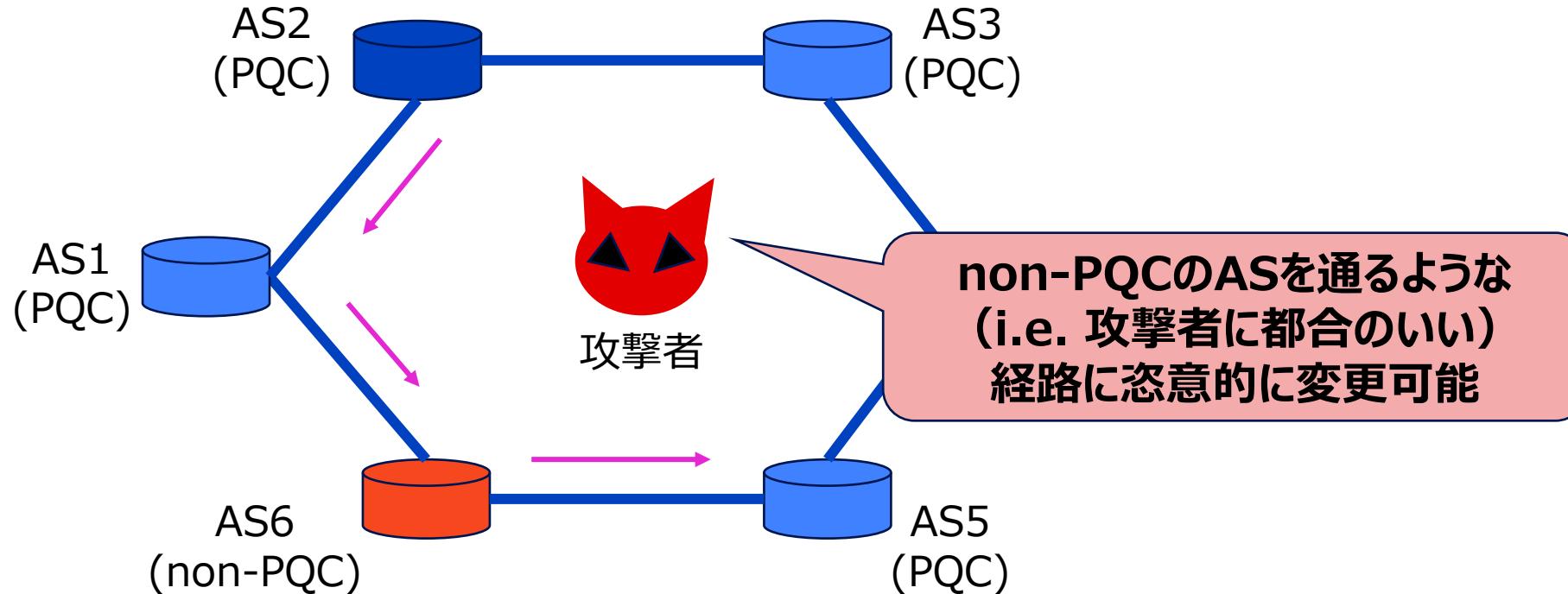
## (1) 収束経路が一意でない例 = BGP Wedge

- BGP Wedge[Yang, 2022] : ネットワークが接続した際, 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] : ネットワークが接続した際, 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

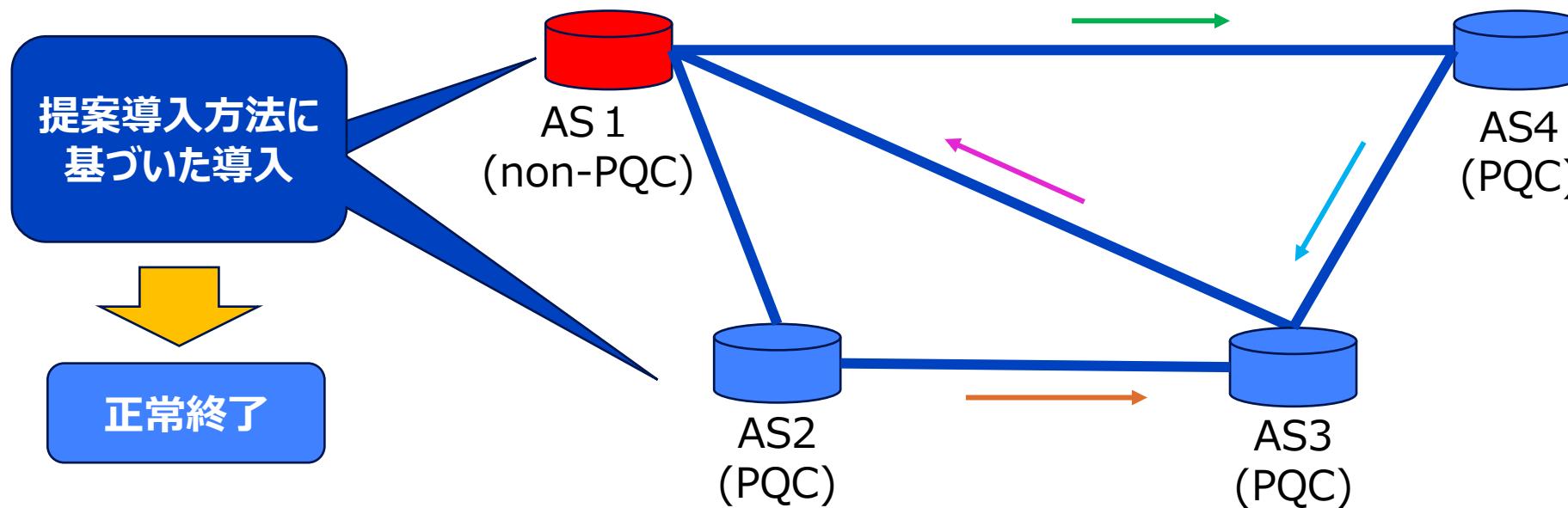


【再掲】経路収束性が満たされていない場合：以下 2 つのパターンが考えられる

- ・ (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

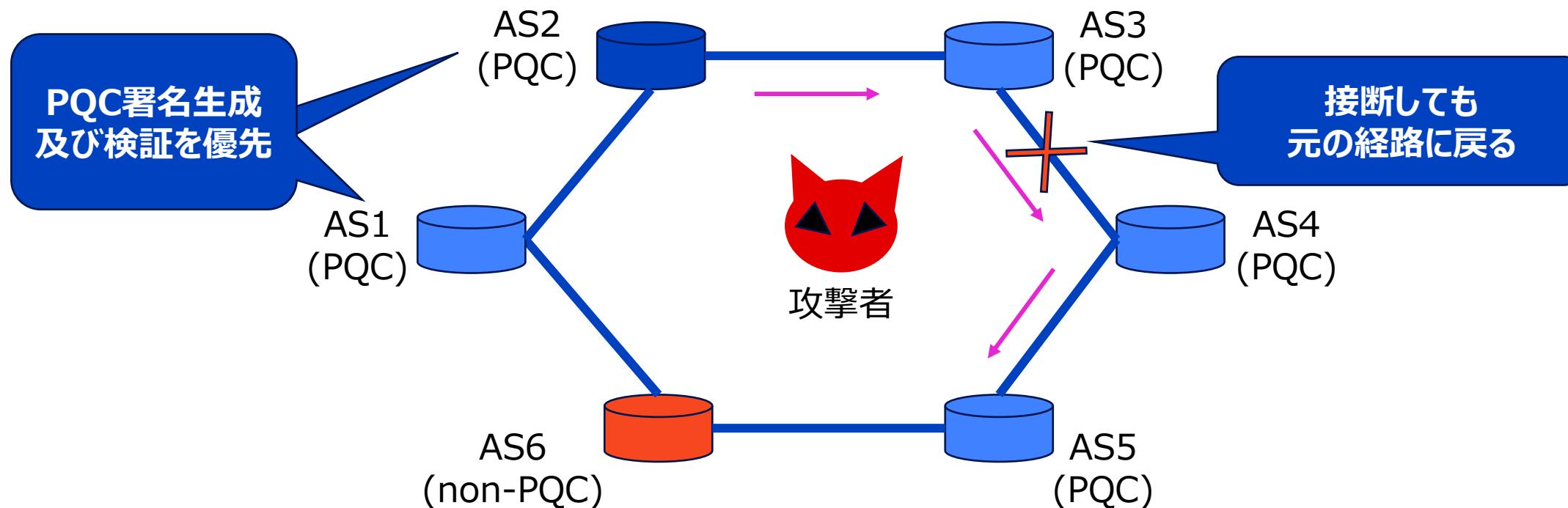


【再掲】経路収束性が満たされていない場合：以下 2 つのパターンが考えられる

- ・ (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

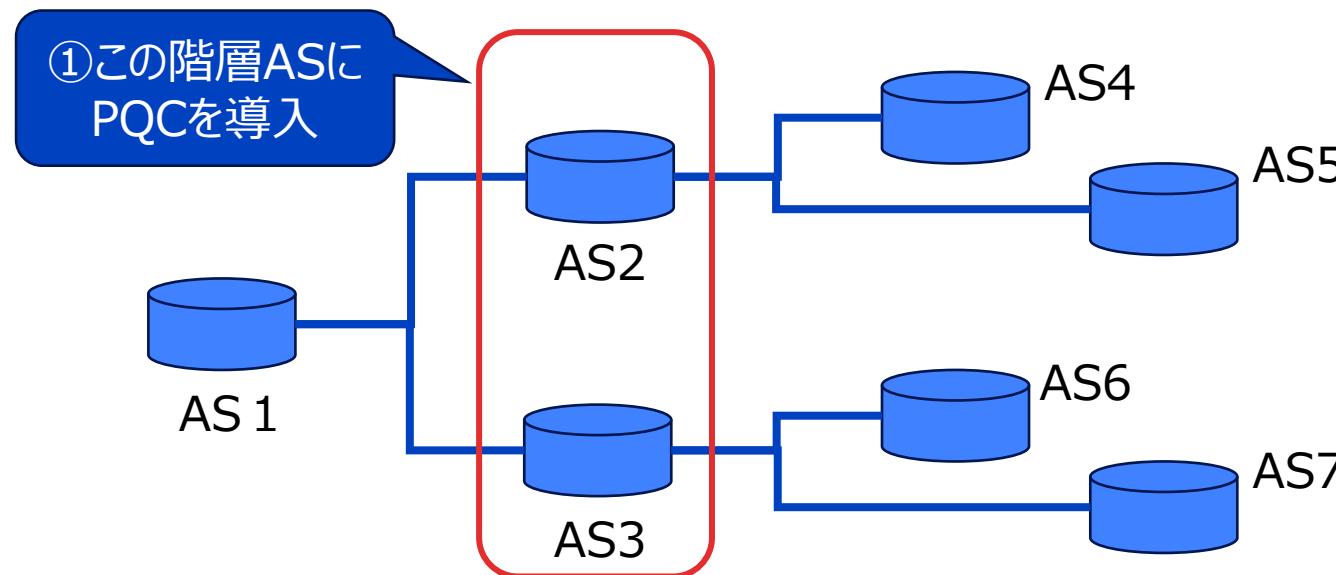


【再掲】経路収束性が満たされていない場合：以下 2 つのパターンが考えられる

- ・ (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) 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

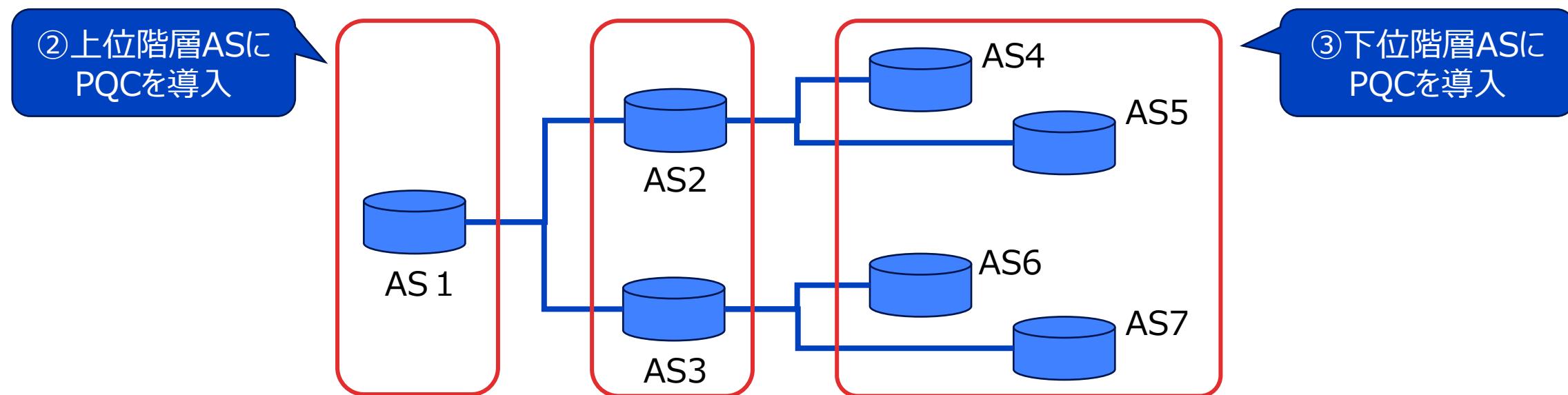


【再掲】経路収束性が満たされていない場合：以下 2 つのパターンが考えられる

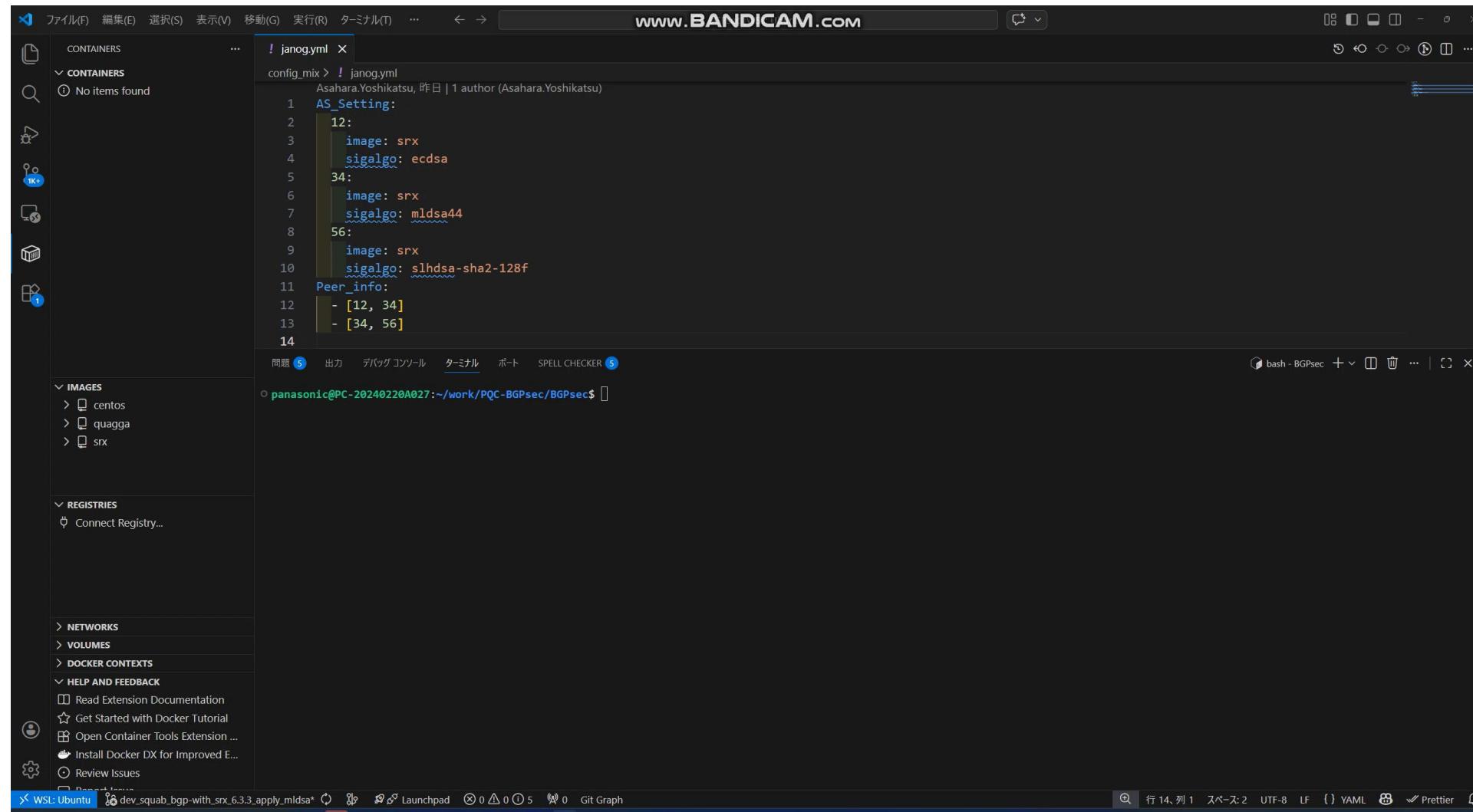
- ・ (1)収束経路が一意でない -> 攻撃者による経路変更攻撃
- ・ (2)経路が収束しない -> ルータへの負荷増加

(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



## PQC対応BGPsecネットワーク構築デモ（動画）

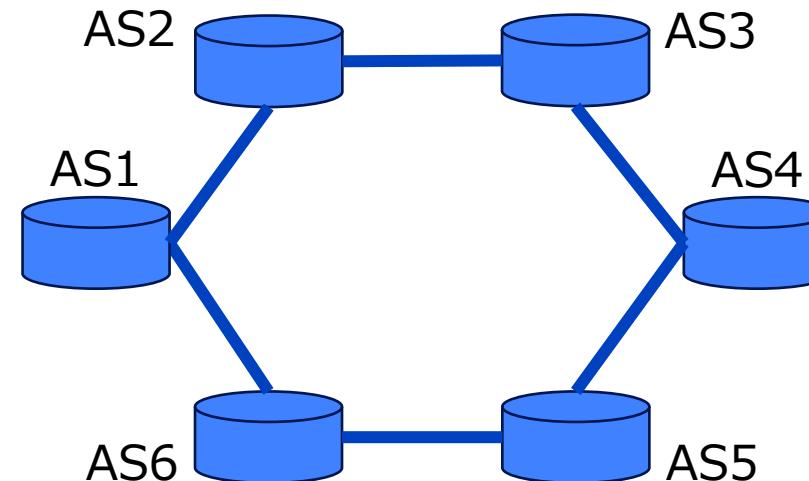
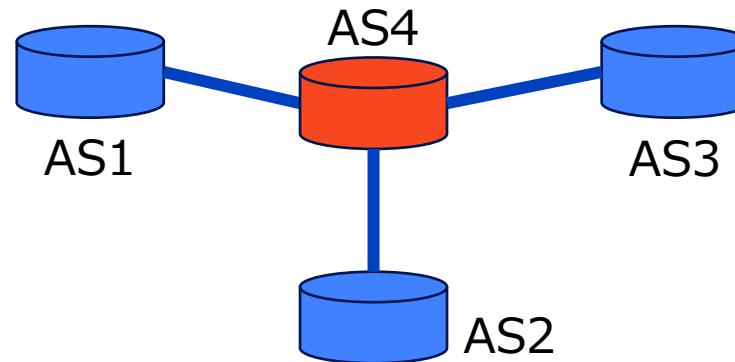


## 中心性を利用したPQC導入順序

- ・ (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



- 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 → 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 → 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