

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

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

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（前回は初参加）

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 → 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

- ・ 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

- ・ PQC改良技術開発
- ・ 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

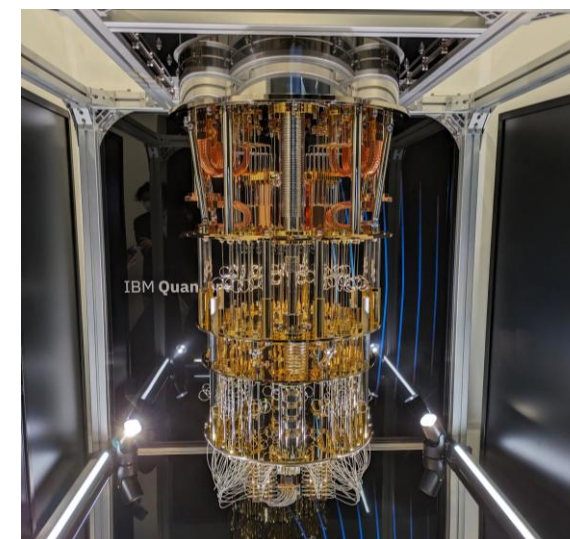
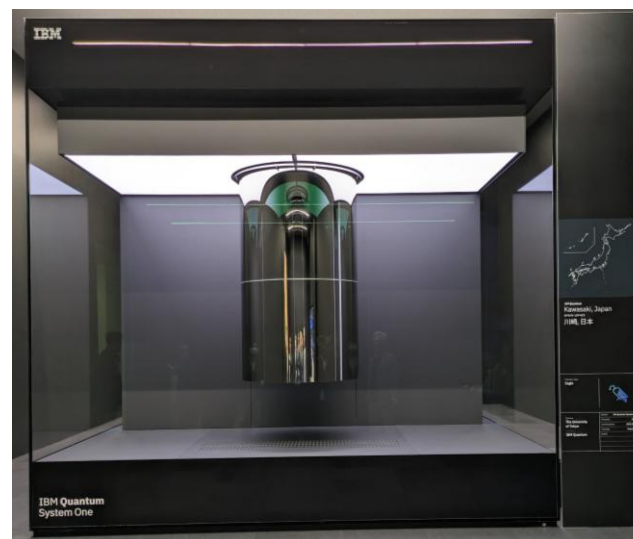
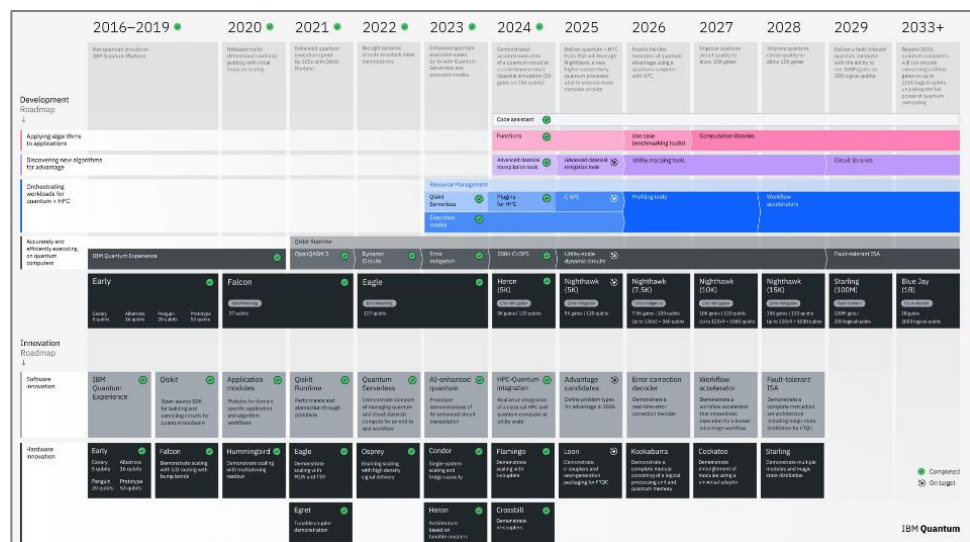
PQCとは何か

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](#)]



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る公開鍵暗号
- 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

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

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

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 → 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

A decorative background on the left side of the slide, consisting of a solid blue vertical bar and a pattern of overlapping, semi-transparent blue triangles of various sizes and shades, creating a modern, geometric look.

PQC移行動向

- **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)													
▼													
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)													
現在													

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](#)

Post-Quantum Use In Protocols (pquip)

About Documents Meetings History Photos Email expansions List archive »

WG	Name	Post-Quantum Use In Protocols
	Acronym	pquip
	Area	Security Area (sec)
	State	Active
	Charter	charter-ietf-pquip-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 Celi
	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/pquip

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

Terminology for Post-Quantum Traditional Hybrid Schemes

RFC 9794

Status Email expansions History

draft-driscoll-pqt-hybrid-terminology

00 01 02

draft-ietf-pquip-pqt-hybrid-terminology

00 01 02 03 04 05 06

rfc9794

Jul 2022

Oct 2022

Mar 2023

May 2023

Oct 2023

Feb 2024

May 2024

Sep 2024

Dec 2024

Jan 2025

Jun 2025

Document	Type	RFC - Informational (June 2025) Was draft-ietf-pquip-pqt-hybrid-terminology (pquip WG)
	Authors	Flo D ✉, Michael P ✉, Britta Hale ✉
	Last updated	2025-06-13
	RFC stream	Internet Engineering Task Force (IETF)
	Formats	txt html xml pdf htmlized bibtex
	Additional resources	Mailing list discussion
IESG	Responsible AD	Paul Wouters ✉
	Send notices to	(None)

[✉ Email authors](#)
[✉ Email WG](#)
[🔗 IPR](#)
[← References](#)
[→ Referenced by](#)
[Search Lists](#)

RFC 9794

RFC9794

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 → 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

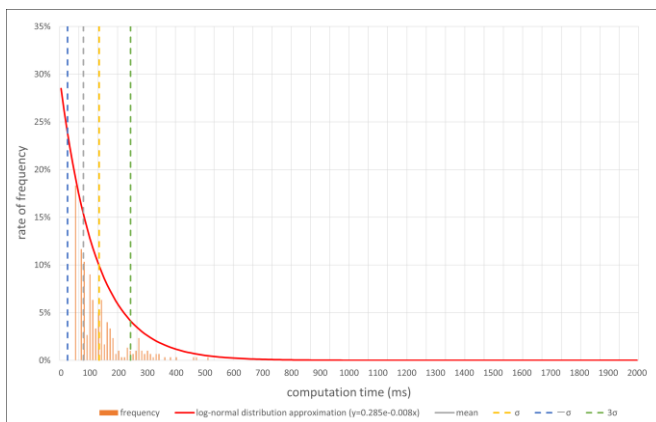
パナソニックのPQC技術開発

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



ML-DSAの処理時間

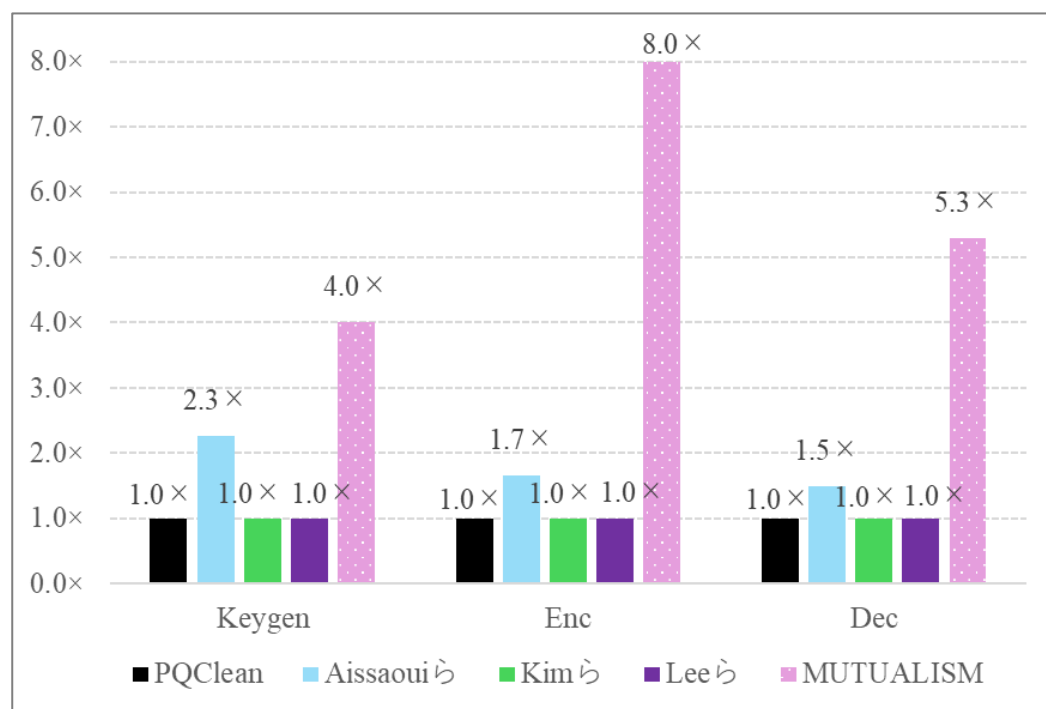
署名アルゴリズム	Stack Usage
ECDSA (従来暗号)	1584 byte
ML-DSA (PQC)	38320 byte

ML-DSAのスタック消費量

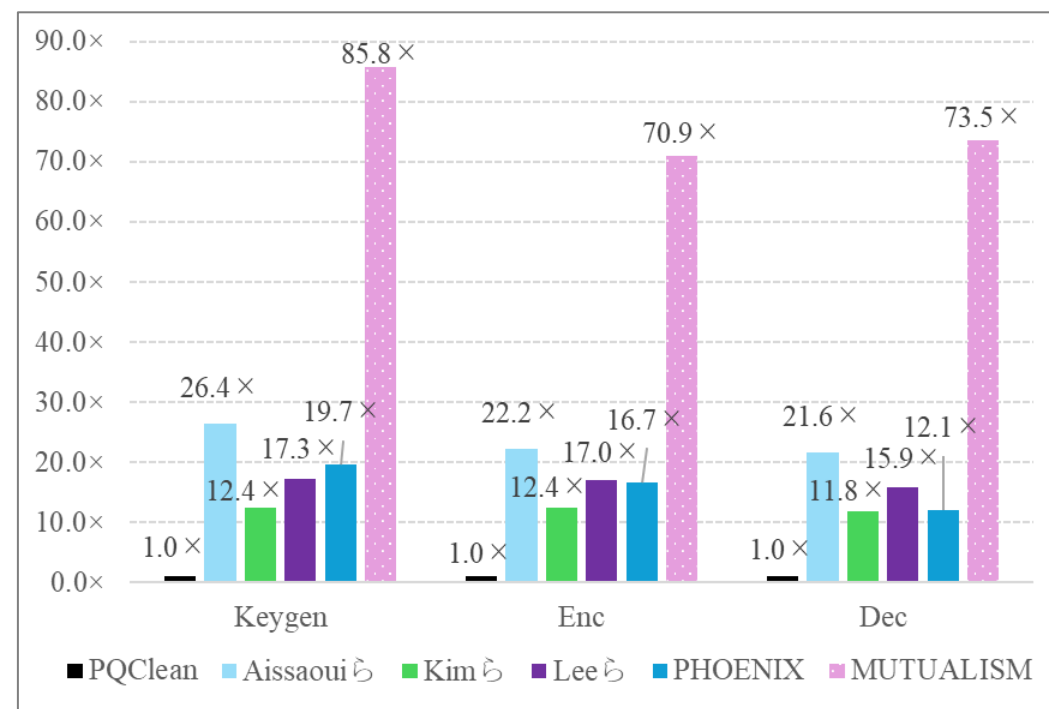
【パナソニックの取り組み】
宅内IoT機器に対するPQC移行に向けた課題抽出・解決技術開発

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



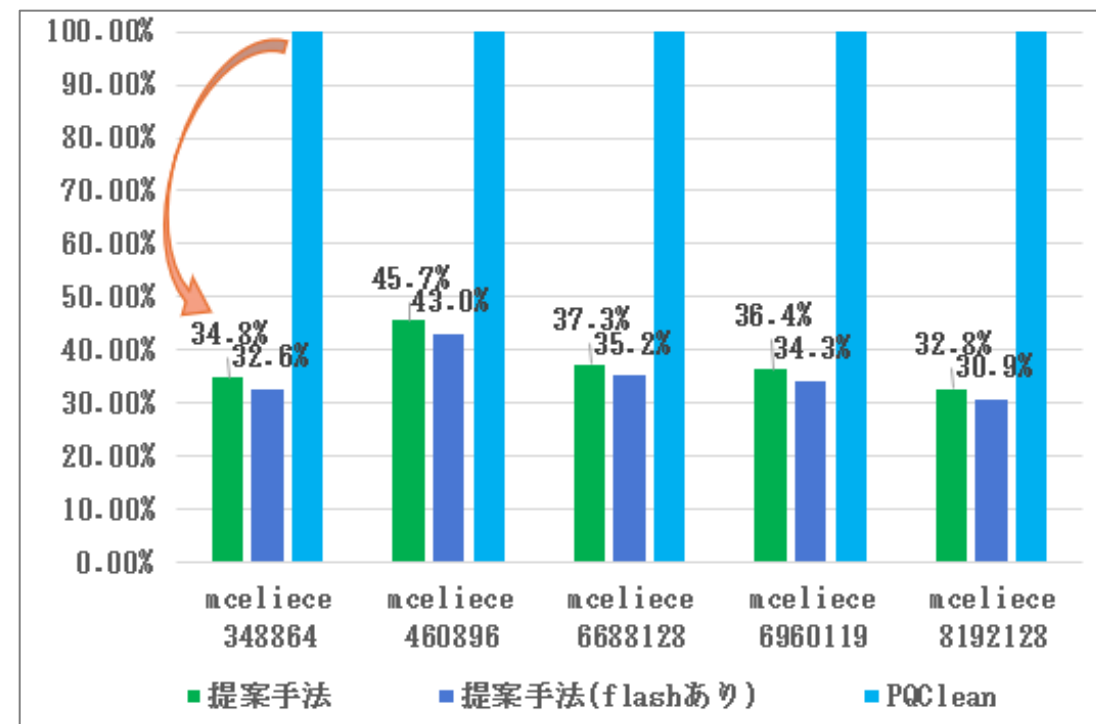
提案方式HQCの処理時間改善倍率

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. of 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)

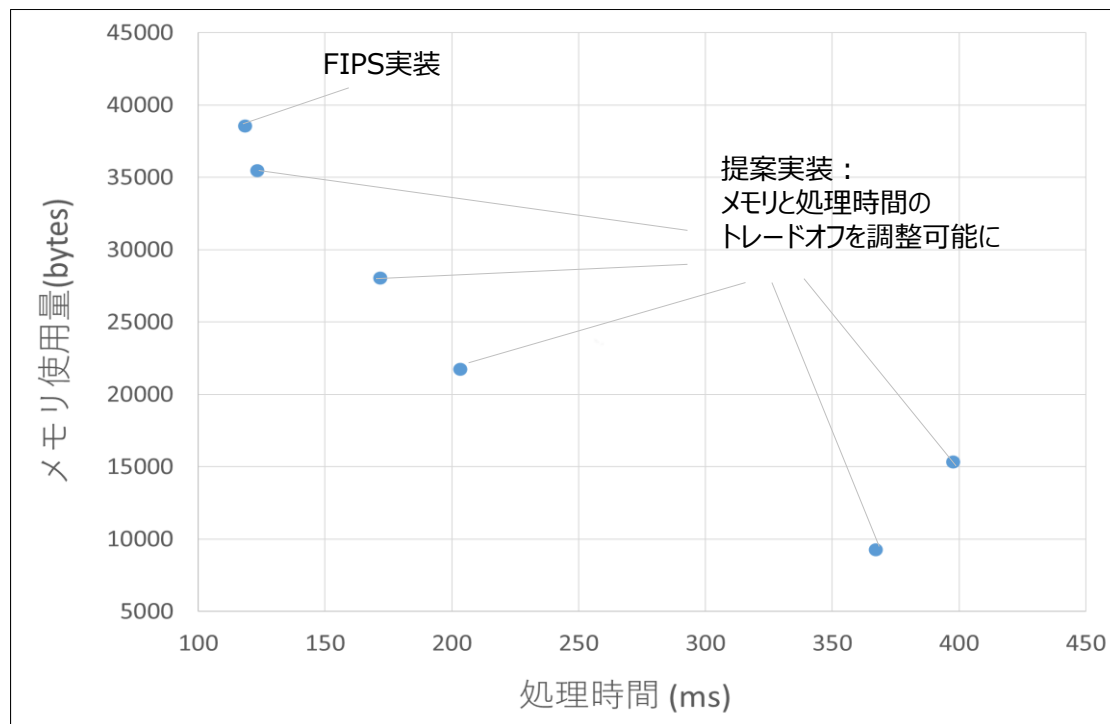
提案方式McElieceの処理時間



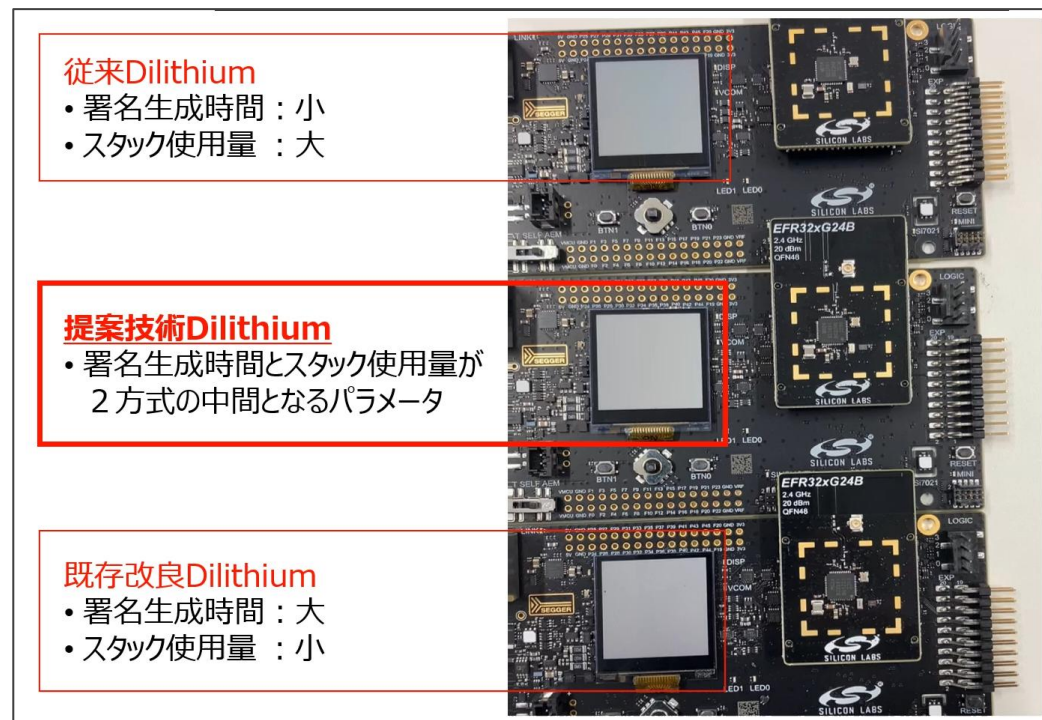
提案方式McElieceのメモリ改善倍率

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. on 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



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。



組み込み容易

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

20/16

The screenshot displays a video player interface with a dark theme. The main content area is split into two panels. The left panel shows a terminal window with the following text:

```
panasonic@PC-20240220A027:/mnt/c/Users/4085650.JAPAN/Documents/  
demo/tai/test/ssl/connectivity$
```

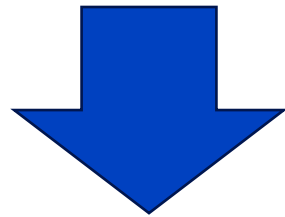
The right panel shows a Wireshark interface with the title bar "Adapter for loopback traffic capture からキャプチャ中". The interface includes a menu bar, a toolbar, and a packet list table. The table has columns for "No.", "Time", "Source", "Destination", "Protocol", "Length", and "Info". The "tls" filter is applied to the packet list.

At the bottom of the video player, a progress bar is visible, showing a duration of 00:00:00:00 / 00:01:30:03.

ネットワーク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**



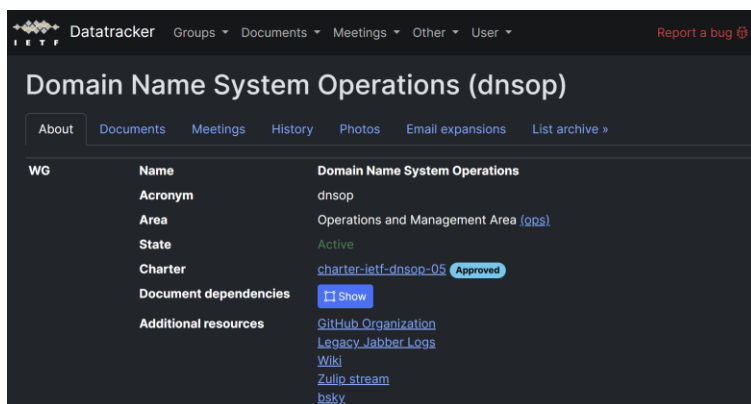
ネットワーク業界はどうだろうか？

RPKI・BGP

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

DNSSEC

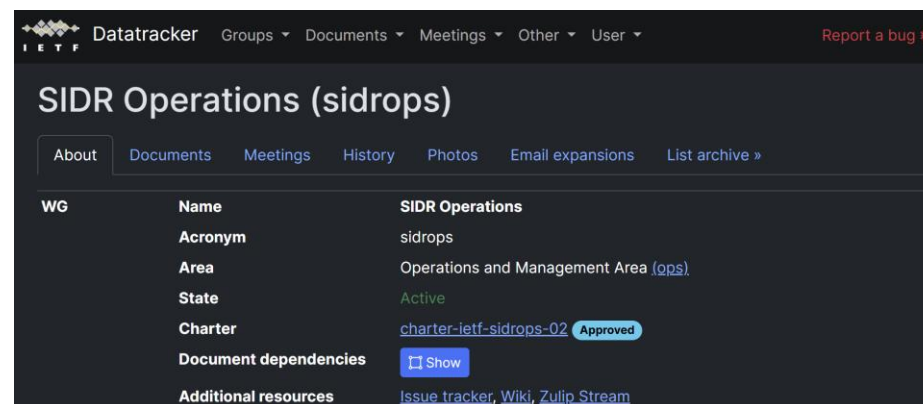
- IETF WG : DNSOP WG (公式), PQ DNSSEC (非公式)
- ドラフト: draft-sheth-pqc-dnssec-strategy-00, draft-fregly-research-agenda-for-pqc-dnssec-01
- PQC関連**RFCは未確認**



The screenshot shows the IETF Datatracker page for the Domain Name System Operations (dnsop) Working Group. The page includes a navigation bar with links for Groups, Documents, Meetings, Other, and User. The main content area displays the group's name, acronym (dnsop), area (Operations and Management Area), state (Active), and charter (charter-ietf-dnsop-05, Approved). It also lists document dependencies and additional resources such as GitHub Organization, Legacy Jabber Logs, Wiki, Zulip stream, and bsky.

WG	Name	Domain Name System Operations
	Acronym	dnsop
	Area	Operations and Management Area (ops)
	State	Active
	Charter	charter-ietf-dnsop-05 Approved
	Document dependencies	Show
	Additional resources	GitHub Organization Legacy Jabber Logs Wiki Zulip stream bsky

DNSOP WG



The screenshot shows the IETF Datatracker page for the SIDR Operations (sidrops) Working Group. The page includes a navigation bar with links for Groups, Documents, Meetings, Other, and User. The main content area displays the group's name, acronym (sidrops), area (Operations and Management Area), state (Active), and charter (charter-ietf-sidrops-02, Approved). It also lists document dependencies and additional resources such as Issue tracker, Wiki, Zulip Stream.

WG	Name	SIDR Operations
	Acronym	sidrops
	Area	Operations and Management Area (ops)
	State	Active
	Charter	charter-ietf-sidrops-02 Approved
	Document dependencies	Show
	Additional resources	Issue tracker , Wiki , Zulip Stream

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

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

- 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

- 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

- 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

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ので、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

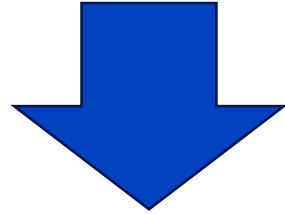
Table 2: A comparison between SL-DNSSEC and signature-based DNSSEC methods. SD : Standard DNS (TCP Fallback).

	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

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！**

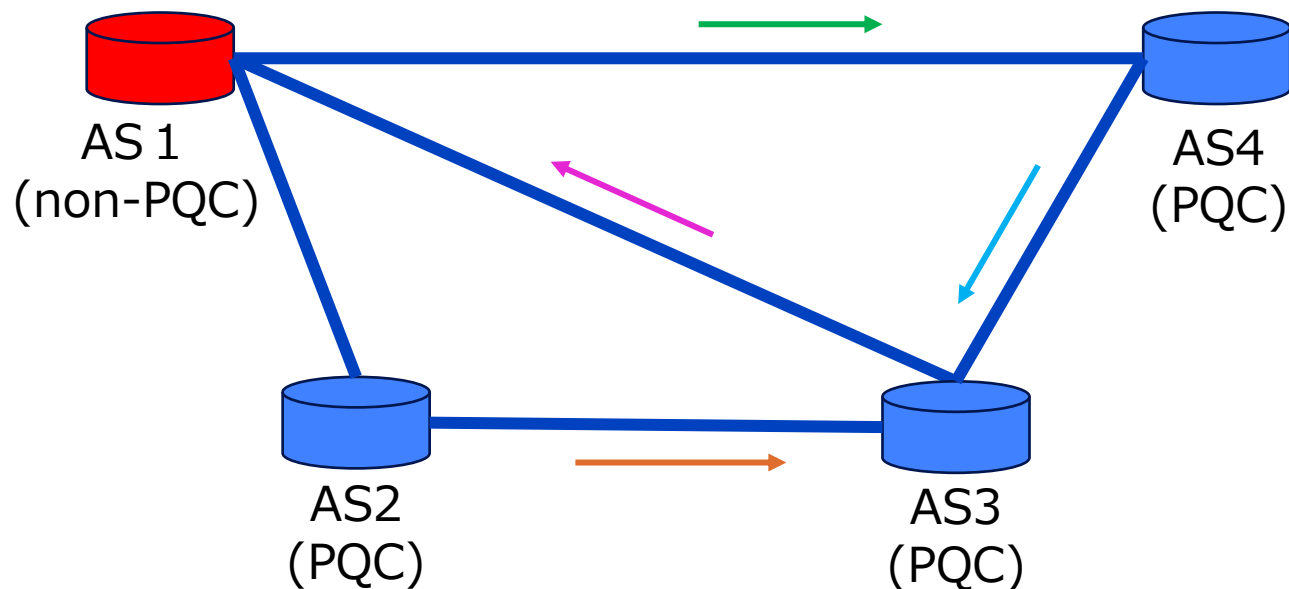
パナソニックのBGPsecに関する PQC移行技術

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

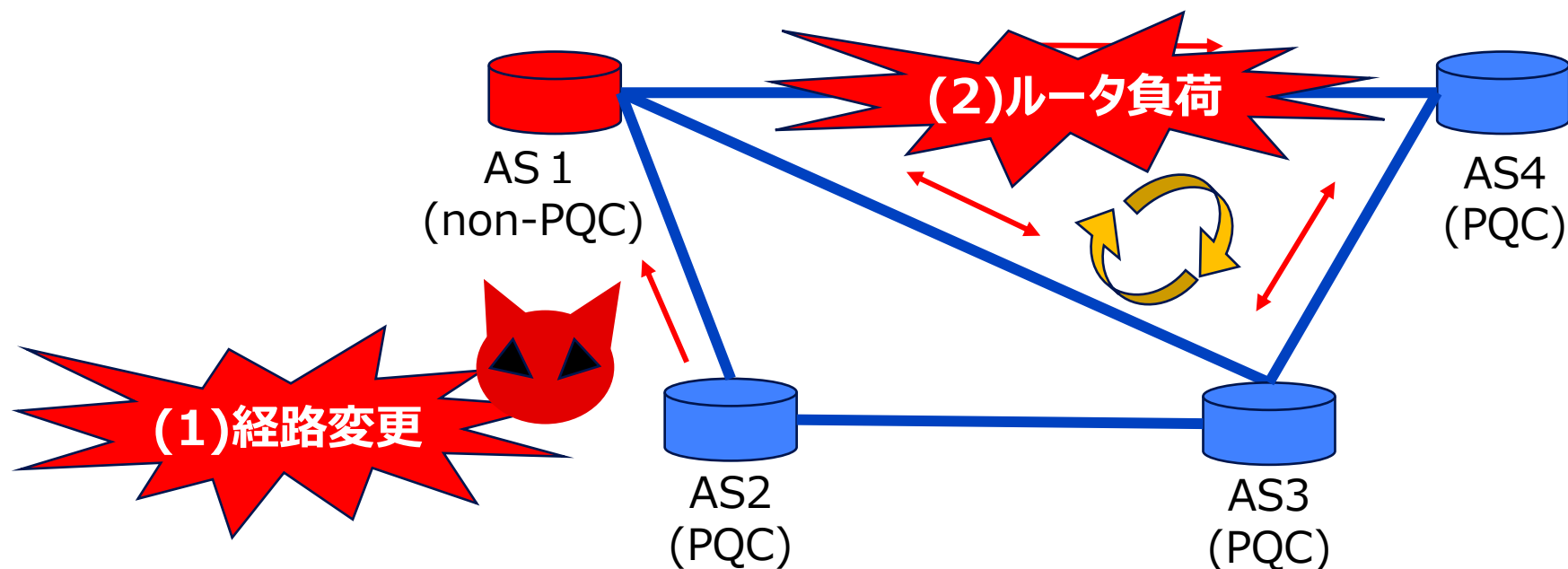


一意に収束
⇒正常終了

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

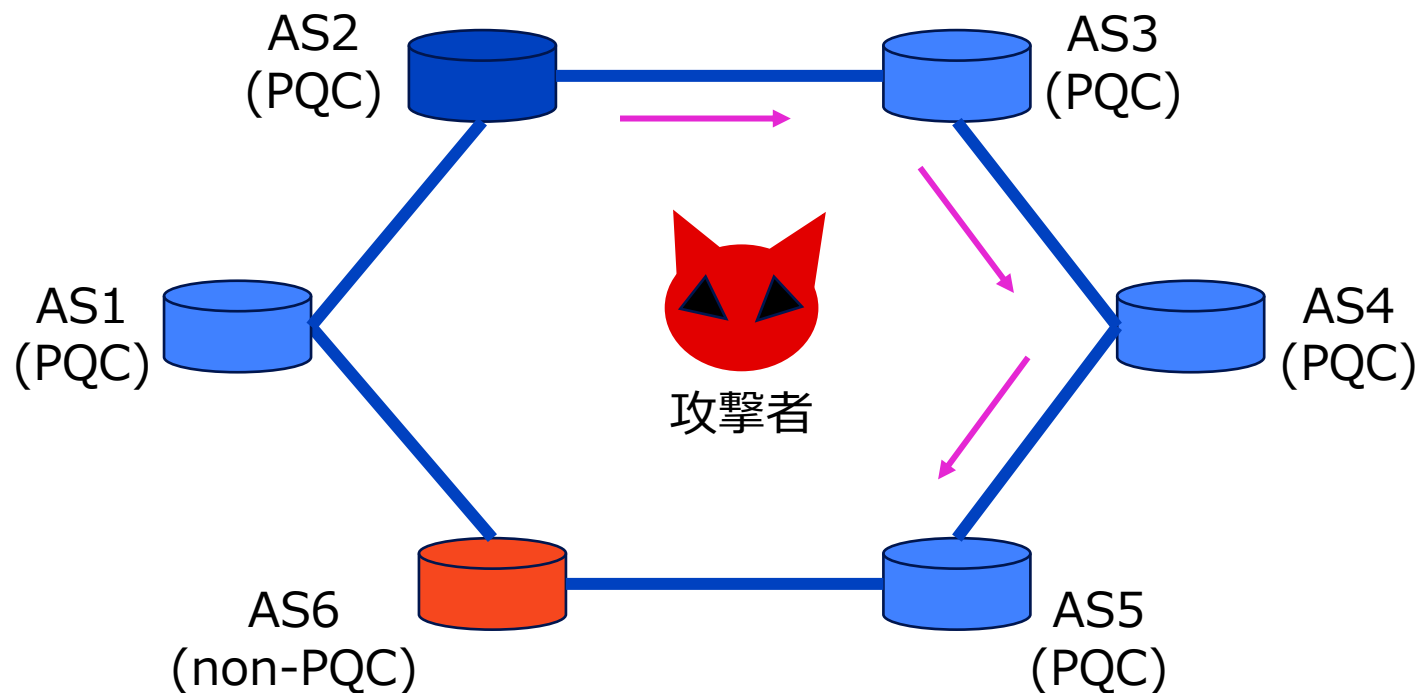
- (1)収束経路が一意でない -> 攻撃者による経路変更攻撃[Maria,2017]
- (2)経路が収束しない -> ルータへの負荷増加[Yang,2022]

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）



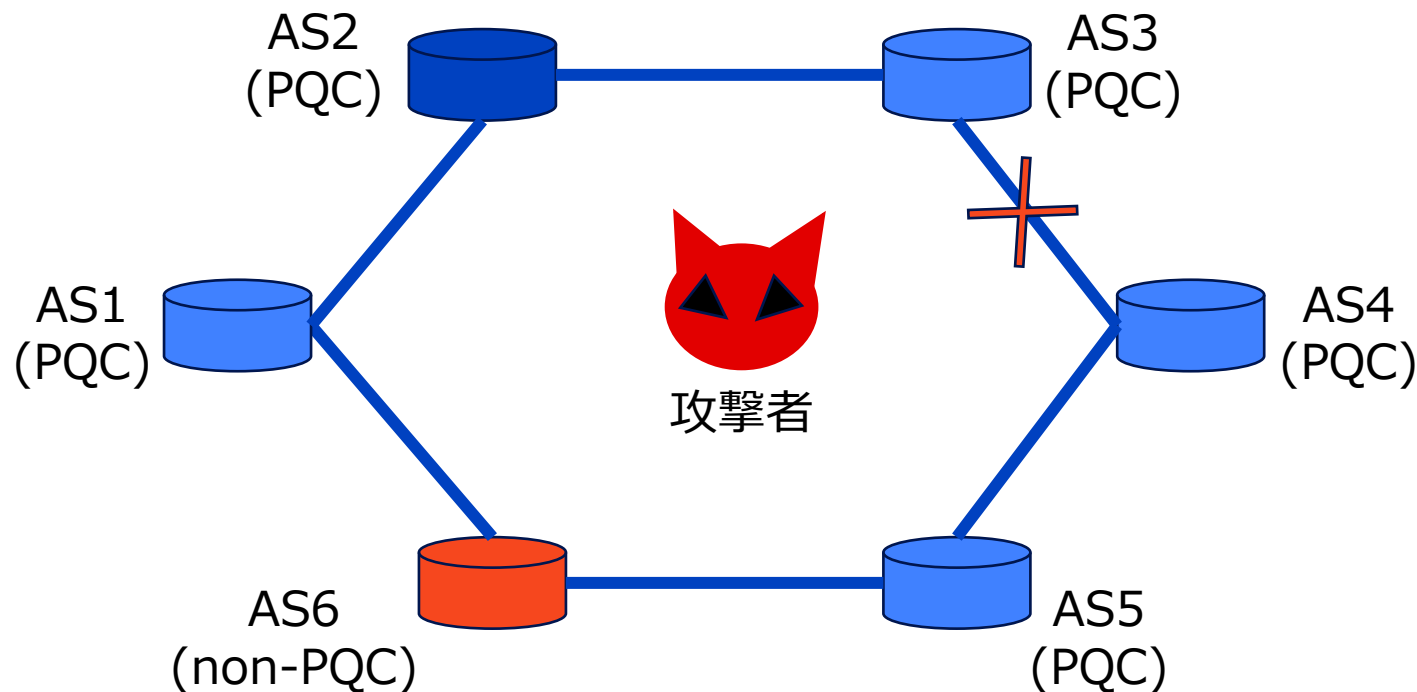
(1)収束経路が一意でない例 = BGP Wedge

- 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



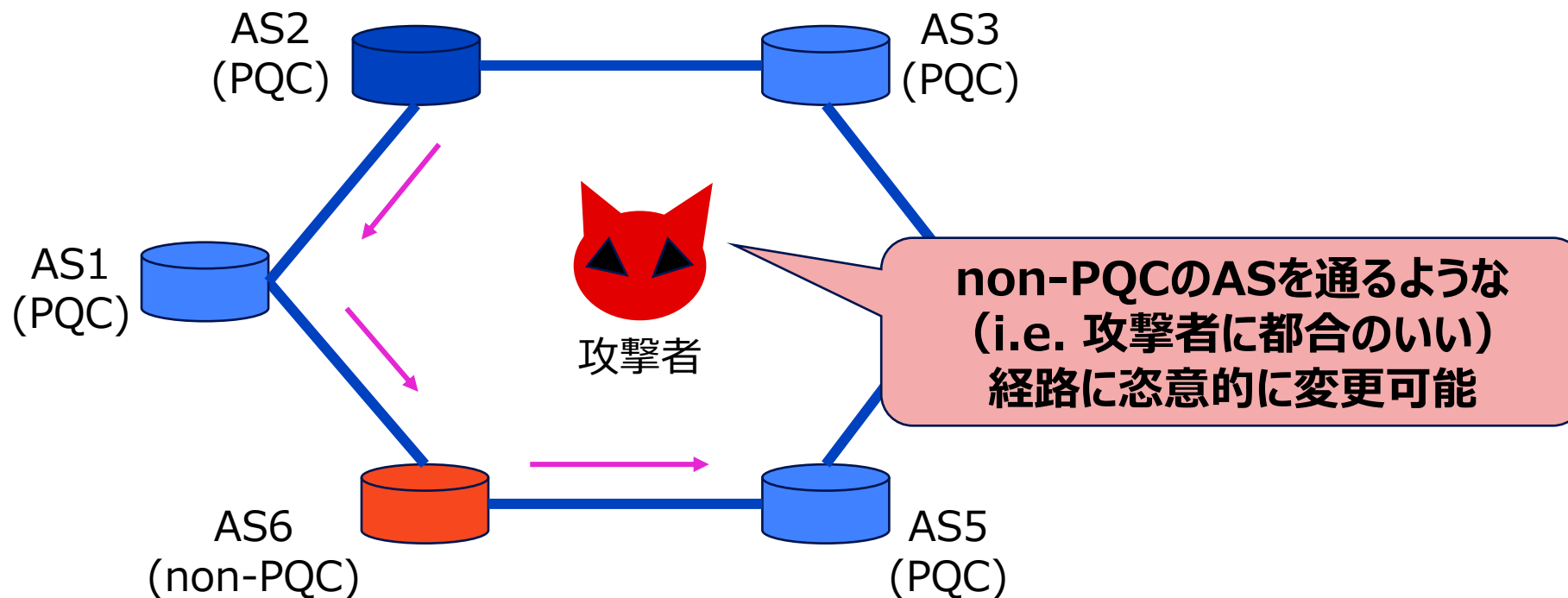
(1)収束経路が一意でない例 = BGP Wedge

- 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

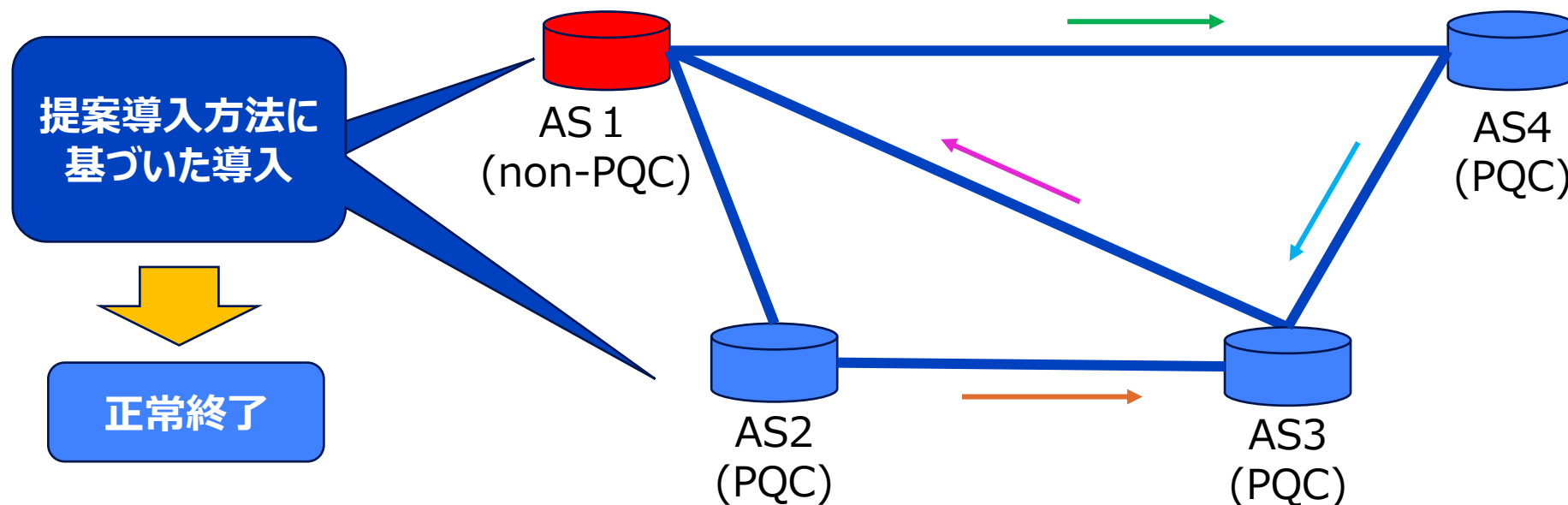


【再掲】経路収束性が満たされていない場合：以下2つのパターンが考えられる

- (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

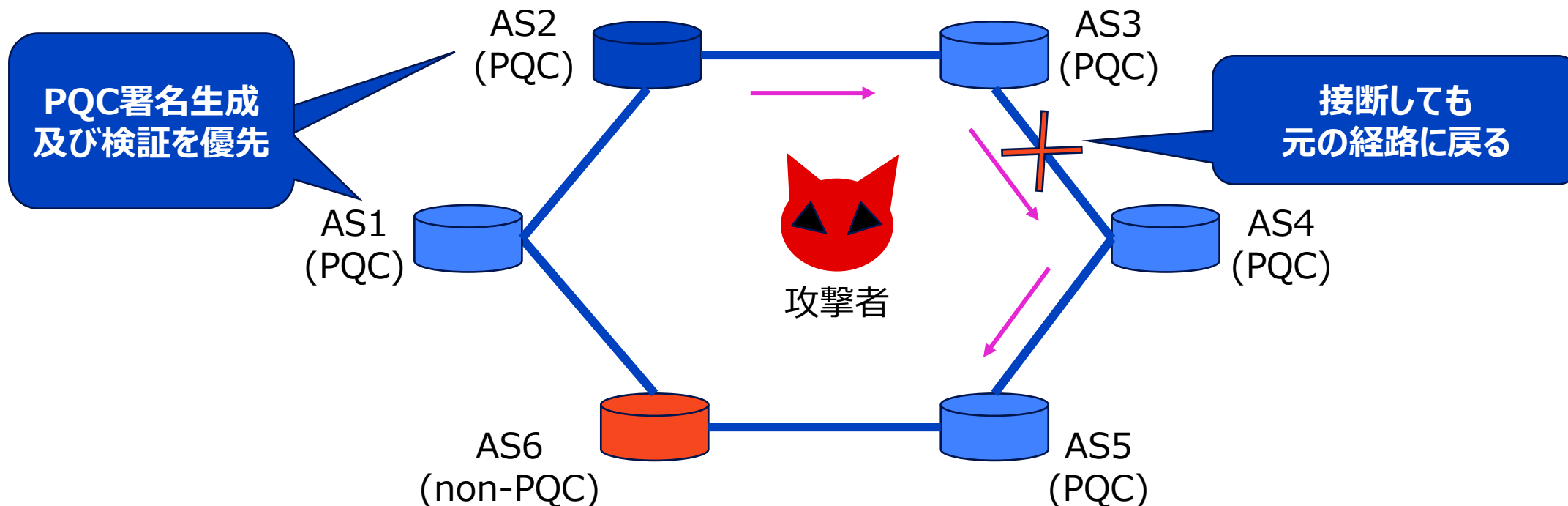


【再掲】経路収束性が満たされていない場合：以下2つのパターンが考えられる

- (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

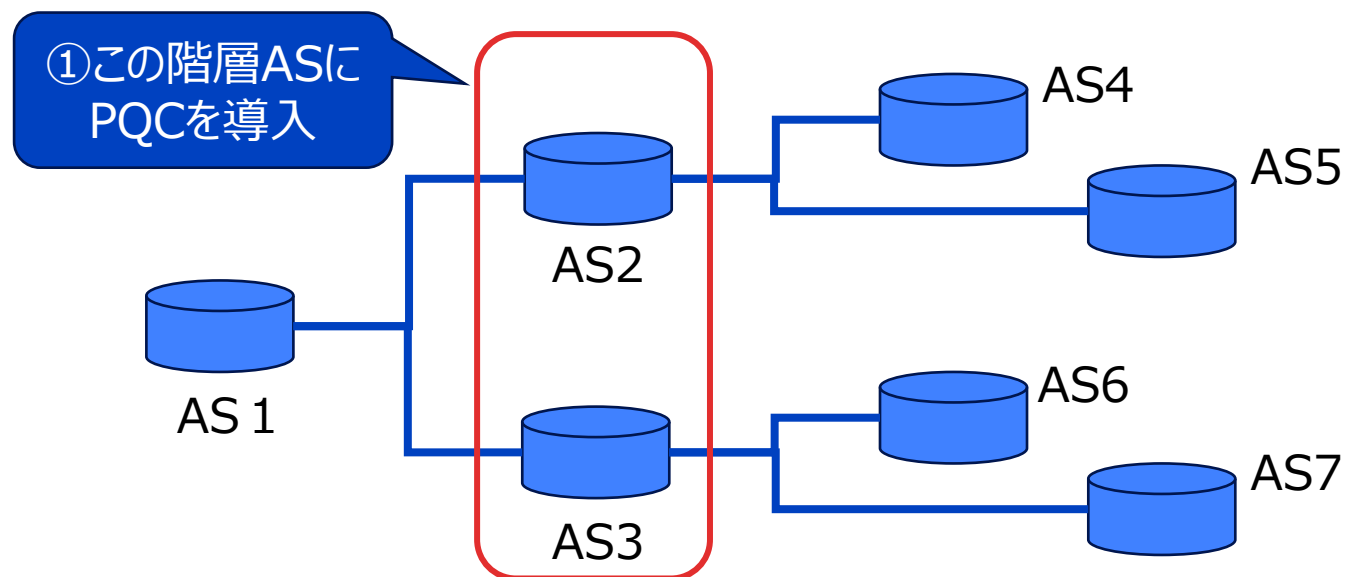


【再掲】経路収束性が満たされていない場合：以下2つのパターンが考えられる

- (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)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



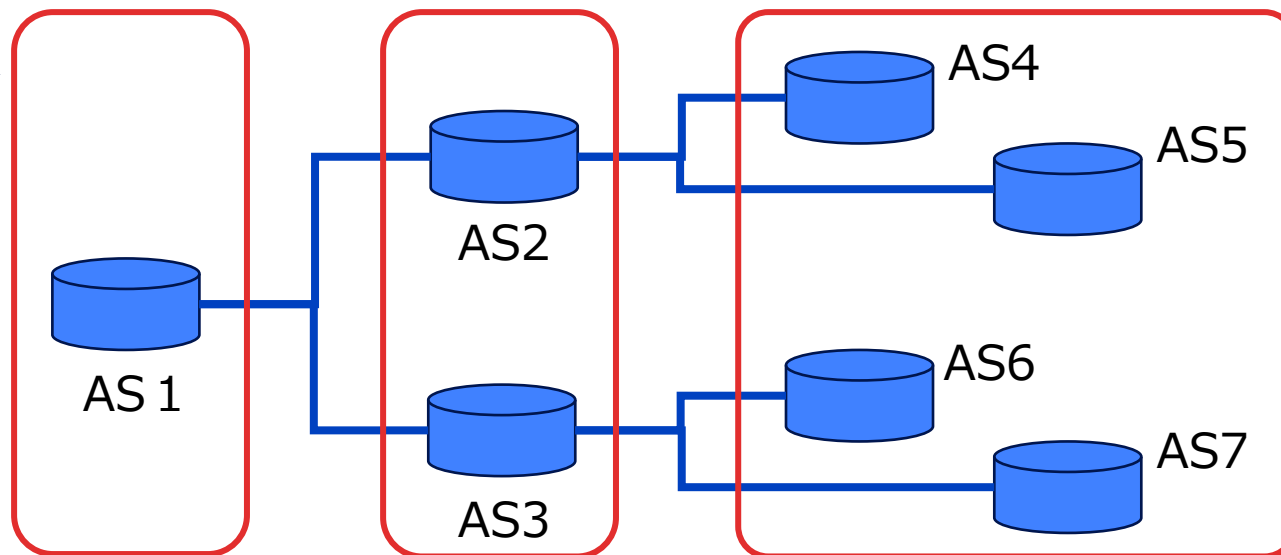
【再掲】経路収束性が満たされていない場合：以下2つのパターンが考えられる

- (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

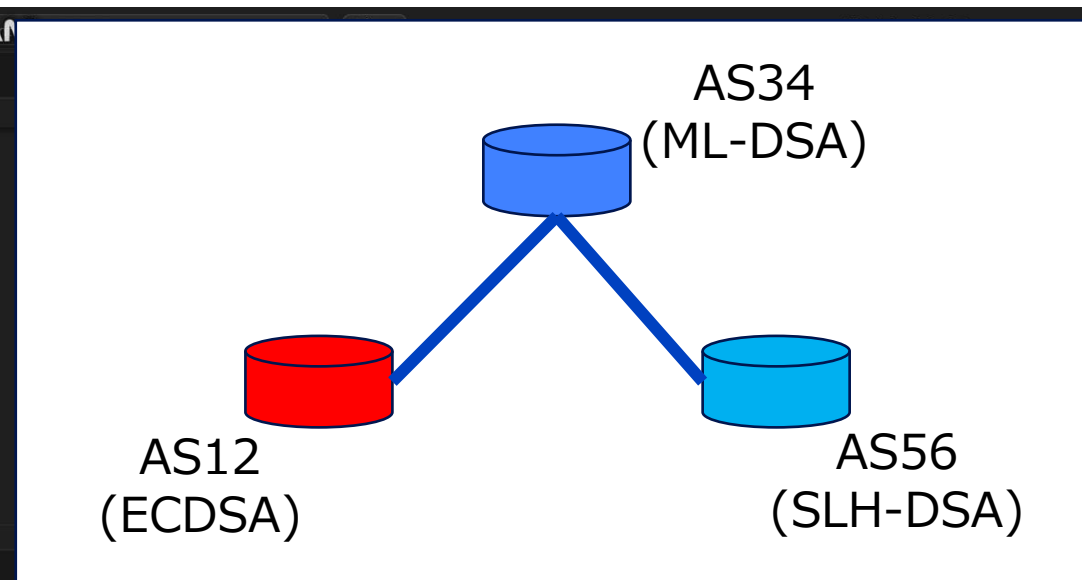
②上位階層ASに
PQCを導入



③下位階層ASに
PQCを導入

```
! janog.yml X
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$
```



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

① OpenSSL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いため、パラメータに合わせてバッファサイズを再設定

③ EVP鍵構造体を利用可能に

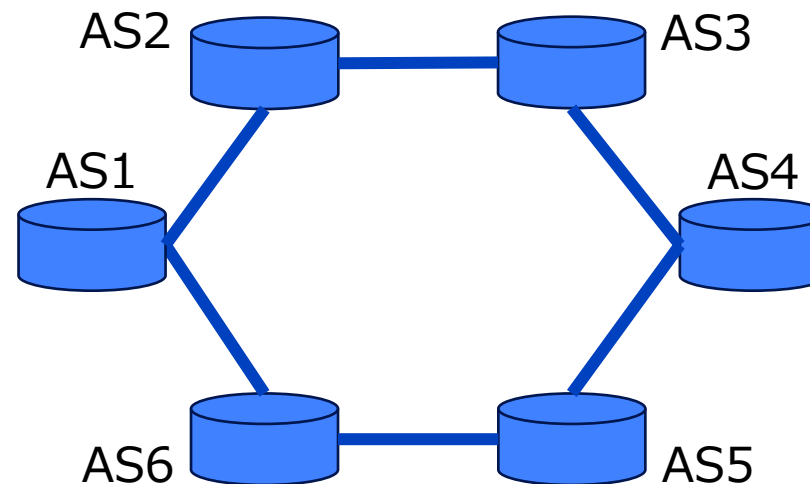
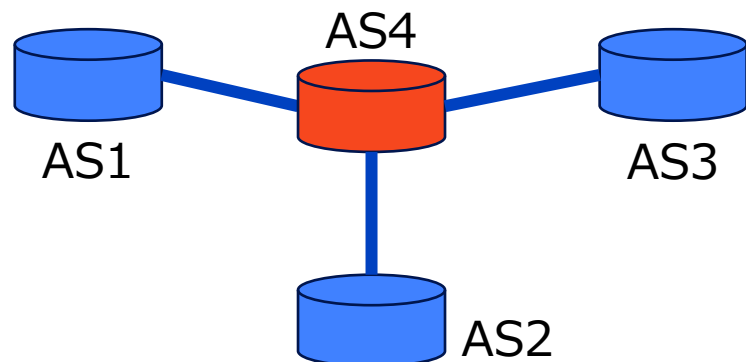
新たにEVP鍵タイプevp_pkey を定義 & 作成したDER形式鍵ファイルをEVP変換するAPIを実装

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
- 中心性が高い＝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、検証回数が増える -> 検証が速いFALCONを選択



A decorative background on the left side of the slide, featuring a solid blue vertical bar and a pattern of overlapping, semi-transparent blue triangles of various sizes and orientations.

質疑&議論

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 → 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。

