D1-3

耐量子計算機暗号(PQC)暗号移行と「暗号の2030年問題」：DNSの現状と未来

菅野　哲（かんの さとる）
GMOコネクト株式会社

2025年11月26日

15:45-16:30

この人、誰？

GMOコネクト株式会社

- 名前
  - 菅野 哲（かんの さとる）
- 所属
  - GMOコネクト株式会社(2025年7月1日～)
    - 執行役員 CTO
  - 公正取引委員会
    - デジタルアナリスト（2024年5月1日 ～）
- どんなことやっていた／やっているの？
  - 学生時代
    - 暗号プロトコルの研究開発、セキュリティベンチャーで技術/営業担当
  - 社会人時代（NTTテクノクロス時代）
    - 暗号ライブラリや情報セキュリティ関連システム開発
    - IETFなどでCamellia関連の標準化活動
  - ここ最近
    - もっぱら会社経営と研究開発支援＆開発プロジェクト実施（生涯現役）

本日のお題を振り返る

GMOコネクト株式会社

15:45-16:30

D1-3 耐量子計算機暗号(PQC)暗号移行と「暗号の2030年問題」：DNSの現状と未来

概要

量子計算機の登場による「暗号の2030年問題」が迫り、PQCへの移行が喫緊の課題です。

本講演ではDNSに焦点を当て、PQC移行がDNSSECに与える影響を解説。署名サイズの増大など、避けては通れない「現状」の技術的課題を具体的に取り上げます。

講演者

- 菅野 哲(GMOコネクト株式会社)

対象者

- 5年後の暗号やDNSSECに関心がある人

https://internetweek.jp/2025/archives/program/d1

Agenda

GMOコネクト株式会社

- 導入・講師紹介（済み）
  - 登壇している菅野とは？
- 暗号の2030年問題
  - 128bit安全性への移行
  - PQCへの移行
- DNSを取り巻く現状と技術動向
  - 顕在化している移行に向けた課題
  - DNSのPQC対応に向けた検討状況
  - PQCを含めた実装状況
- まとめ

暗号の2030年問題

「暗号の2030年問題」とは？

GMOコネクト株式会社

「暗号の2030年問題」は2つの側面がある

「暗号の2030年問題」の背景

将来的な「暗号解読の進展」や
「計算機環境の変化」を考慮し
112bit安全な暗号の移行計画

※ 「NIST SP 800-57」に記述

1つ目

128bit安全な暗号への移行

CRQCによる現行暗号への
リスクが許容できない

2つ目

PQCへの移行

暗号の2030年問題

128bit安全への移行

暗号の2030年問題： 128bit安全性への移行

- 128bit安全なアルゴリズム　⇨「**RSA-3072**」や「**RSA-4096**」
  - RSA暗号だとデータサイズが大きい・・・。
    - DKIMからの視点だと「 DNS の UDPパケット (512 byte) 」の制約あり
  - データサイズが大きい際には「楕円曲線暗号/ECC」が活用

この制約が厳しい…

Internet Engineering Task Force (IETF)　　J. Levine
Request for Comments: 8463　　Taughannock Networks
Updates: 6376　　September 2018
Category: Standards Track
ISSN: 2070-1721

A New Cryptographic Signature Method for DomainKeys Identified Mail (DKIM)

Abstract

This document adds a new signing algorithm, Ed25519-SHA256, to "DomainKeys Identified Mail (DKIM) Signatures" (RFC 6376). DKIM verifiers are required to implement this algorithm.

EdDSA
※ ECDSAでないことに注意

https://datatracker.ietf.org/doc/html/rfc8463

暗号の2030年問題： 128bit安全性への移行（まとめ）

- DNSSECに視点を移して影響を整理すると・・・

どこに影響？

- ルート／TLD／大規模ゾーン
- 権威サーバ／リゾルバ
- 監視・可観測性（メトリクスの再設計）

何が変わるの？

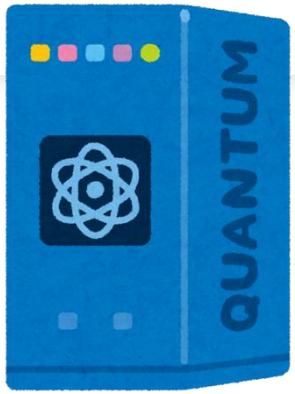
- 署名サイズの増加
- キャッシュへの負荷増加（ストレージ・帯域）
- 検証コスト（CPU時間）の上昇

暗号の2030年問題

PQCへの移行

CRQCが与える現行暗号への影響度

GMOコネクト株式会社



- 特に暗号技術に影響のある量子計算機は何か？

  誤り訂正機能を有する量子ゲート型量子計算機
  → CRQC: **C**ryptographically **R**elevant **Q**uantum **C**omputer
  暗号解読可能な量子計算機

No	暗号の種類	現行暗号例	脅威となる量子アルゴリズム	効率的に解ける問題	暗号への脅威	望ましい対策
1	共通鍵暗号	AES	Grover's Alg	データ探索問題	限定的	鍵長の伸長/暗号利用モードの変更
2			Simon's Alg	周期探索問題	限定的	
3	公開鍵暗号	RSA	Shor's Alg	素因数分解	非常に大きい	PQCへの移行
4		DSA/ECDSA	Shor's Alg	離散対数問題		
5		PQC	（現状）未発見	ー	現在なし	ー

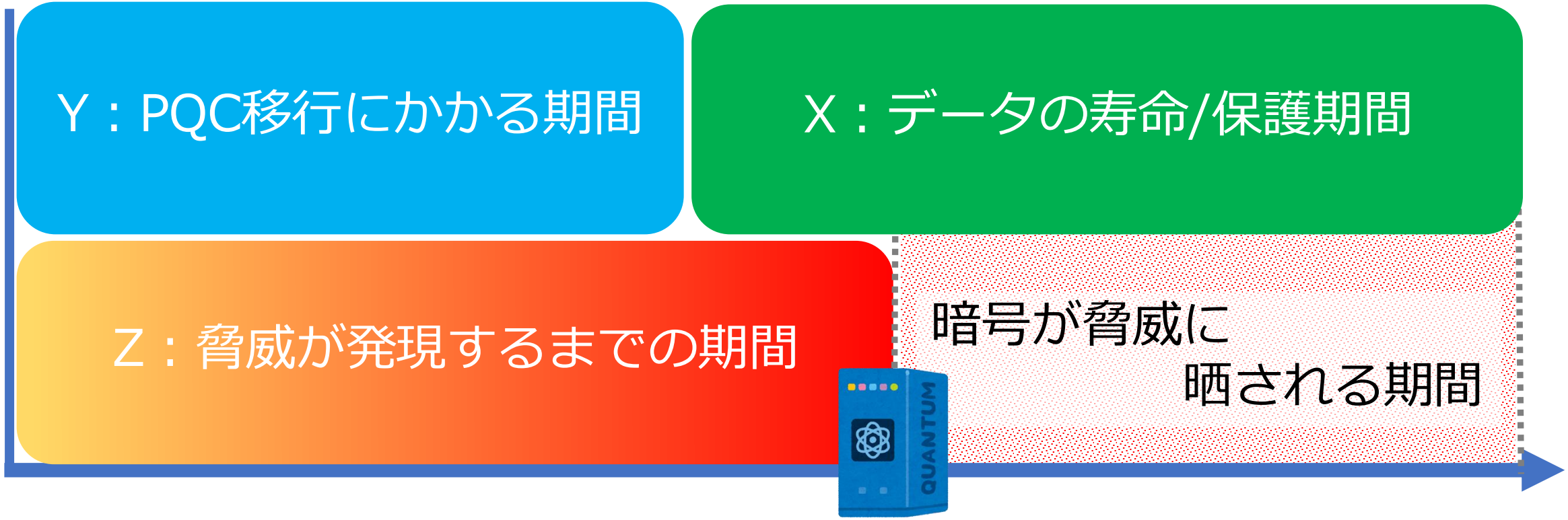
現行暗号における安全性の根拠となる数学的問題が簡単に解ける

既知の脅威が未発見な「PQC」への移行という流れ

Moscaの定理でPQC移行のタイミングを把握

GMOコネクト株式会社

- 暗号が安全でためには「X ＋ Y ＜ Z」を満たす必要ある
  - 例：X ＝ 5年、Y ＝ 10年、Z ＝ 10年（CRQCの発現: 2035年）
    - → X ＋ Yが15となるため、５年間は脅威に晒されることに...



CRQCの発現はいつ頃？？

- 諸説ありますがCRQCの発現は「2035年前後」が妥当ライン？

2030年代
後半

Quantum computers are progressing quickl… …first demonstrations of quantum advantage within the next five years. Most experts agreed in a poll that a quantum computer capable of breaking 2048-bit encryption is likely by the late 2030s.

https://www.ibm.com/think/topics/quantum-safe-cryptography

2030年

https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

2034年以内

The three new standards are built for the future. Quantum computing technology is developing rapidly, and some experts predict that a device with the capability to break current encryption methods could appear within a decade, threatening the security and privacy of individuals, organizations and entire nations.

https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

特定の技術が社会で利用されるまでの道のり

- 一般的な技術が浸透するまで非常**に長い年月**がかかる…
  - 仕様確定がスタートラインで「製品/商品化」が踏ん張り時！

1. 基礎研究
期間：5-10年
- 新しい理論等を大学や研究機関で行われる
- 特定の応用は考慮しない

2. 応用研究
期間：3-7年
- 基礎研究で得られた知見を実用化に向けて応用
- 可用性・実現可能性を調査

3. 技術標準化
期間：2-5年
- 相互運用のための仕様策定
- 標準化団体による技術使用の統一化

4. 試作・実証
期間：1-3年
- プロト開発と実証実験
- 実用性と市場性を検証
- フィードバックを基に改良

5. 製品/商用化
期間：1-2年
- 量産体制の構築と市場投入
- 初期の限定的な市場でのテスト販売

6. 市場普及
期間：5- 15年
- 技術採用のライフサイクルに従い普及
- イノベータから始まり、ラガード層へ

【結論】

CRQCの発現タイミング次第では
PQC移行って赤信号？

現行暗号からPQC移行への始まり

GMOコネクト株式会社

- 2022年5月発行されたNSM-10 第3条でPQC移行の大方針
  - → PQCへの移行の期限「2035年」というゴールが設定された

THE WHITE HOUSE

Administration The Record Briefing Room Visit Español MENU

MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

BRIEFING ROOM › STATEMENTS AND RELEASES

NATIONAL SECURITY MEMORANDUM/NSM-10

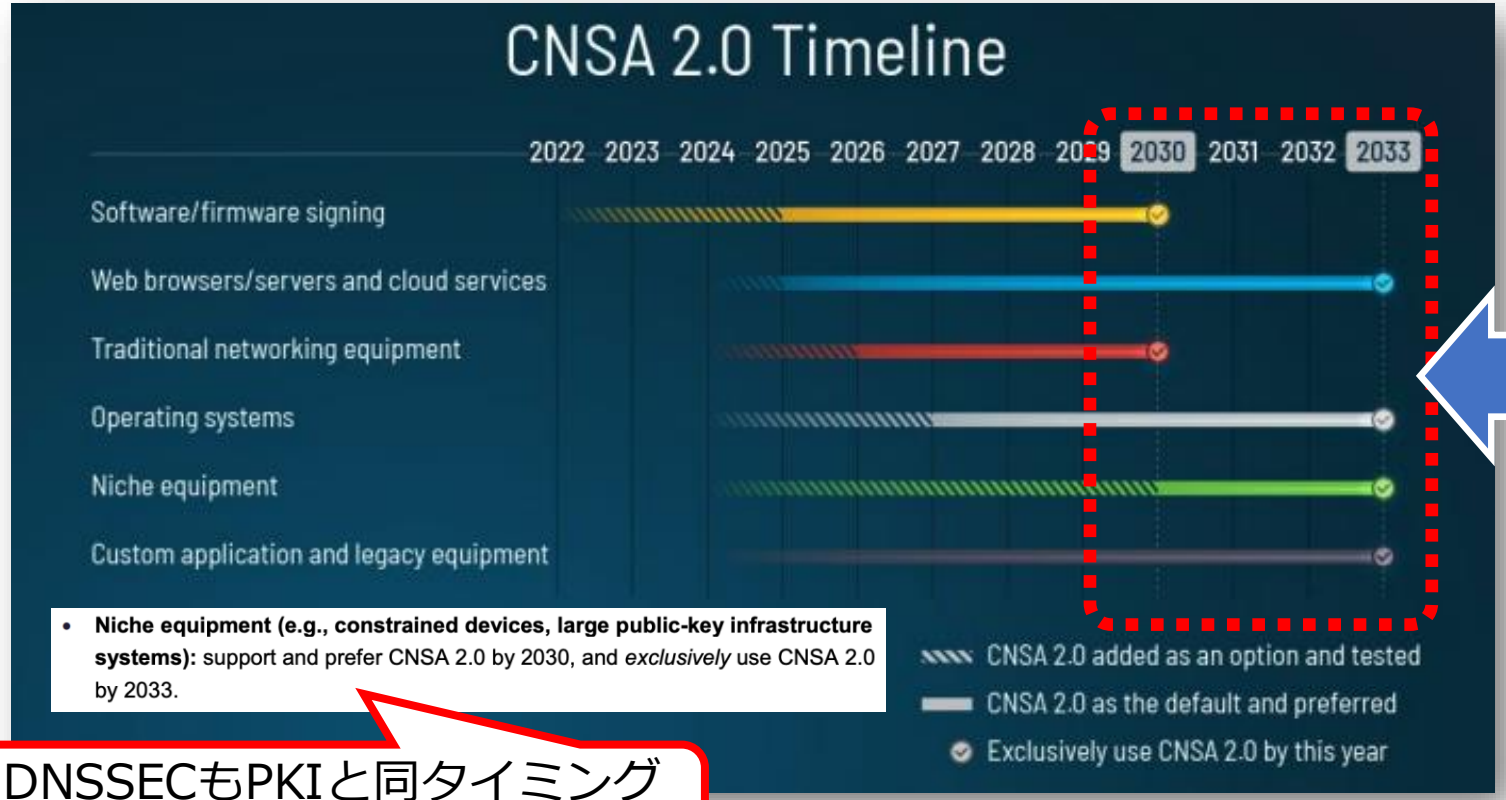
Sec. 3. Mitigating the Risks to Encryption. (a) Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a CRQC. To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035. Currently, the Director of the National Institute of Standards and Technology (NIST) and the Director of the National Security Agency (NSA), in their capacity as the National Manager for National Security Systems (National Manager), are each developing technical standards for quantum-resistant cryptography for their respective jurisdictions. The first sets of these standards are expected to be released publicly by 2024.

https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

PQC暗号移行の1つの事例：CNSA 2.0

GMOコネクト株式会社

- 2022年9月 NSA が国家安全保障に関する機密情報を守るための暗号（CNSA）を Ver 2.0に更新 ⇨ CNSA 2.0は耐量子性なアルゴリズムで構成



CNSA: Commercial National Security Algorithm

2030～2033年まで
CNSAに完全移行！

＜品揃え＞
・公開鍵暗号
　ML-DSA （CRYSTALS-Dilithium）
　ML-KEM （CRYSTALS-Kyber）
・共通鍵暗号
　AES-256, SHA-384/512
・ソフトウェア等更新
　XMSS, LMS

DNSSECもPKIと同タイミング
と考えるのが良さげ

NSA「Announcing the Commercial National Security Algorithm Suite 2.0」より

https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

直近のアメリカ政府の動向

GMOコネクト株式会社

- アメリカ大統領が交代によりPQC移行にも影響あり
  - 2025年6月6日にEO 14144に対する修正令（Amendment）が公開

PRESIDENT DONALD J. TRUMP

The WHITE HOUSE

PRESIDENTIAL ACTIONS

SUSTAINING SELECT EFFORTS TO STRENGTHEN THE NATION'S CYBERSECURITY AND AMENDING EXECUTIVE ORDER 13694 AND EXECUTIVE ORDER 14144

Executive Orders | June 6, 2025

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*), the National Emergencies Act (50 U.S.C. 1601 *et seq.*), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code, it is hereby ordered:

Section 1. Amendments to Executive Order 14144. Executive Order 14144 of January 16, 2025 (Strengthening and Promoting Innovation in the Nation's Cybersecurity), is hereby amended by:

(a) striking subsections 2(a)-(b) and redesignating subsections 2(c), 2(d), and 2(e) as subsections 2(a), 2(b), and 2(c), respectively;

(b) striking the first sentence of subsection 2(e);

項番	トピック	Biden政権の規定	Trump政権の修正	変更の詳細
1	PQC製品カテゴリリスト	CISAは、PQC対応製品が広く利用可能な製品カテゴリのリストを180日以内に発行し、定期的に更新する (EO 14144 Sec. 4(f)(i))	同じ規定を維持 (December 1, 2025までに発行) (修正令 Sec. 2(d) 4(f)(i))	変更なし この要件は継続
2	連邦調達要件	製品カテゴリがリストに掲載されてから90日以内に、各機関は該当カテゴリの製品調達時にPQC対応を要求する (EO 14144 Sec. 4(f)(ii))	完全削除 (修正令で削除)	重大な変更 積極的な調達要件を撤廃
3	既存システムへのPQC実装	ネットワークセキュリティ製品・サービスでPQC対応が提供され次第、PQCまたはハイブリッド鍵確立を可能な限り迅速に実装する (EO 14144 Sec. 4(f)(iii))	完全削除 (修正令で削除)	重大な変更 即座の実装要件を撤廃
4	国際協力・推進	国務省とNISTが主要国の政府・産業界に対し、NIST標準化のPQCアルゴリズムへの移行を促すよう90日以内に特定・関与する (EO 14144 Sec. 4(f)(iv))	完全削除 (修正令で削除)	重大な変更 国際的なPQC推進活動を停止
5	TLS 1.3対応要件	NSS（国防省）と非NSS（OMB）が、2030年1月2日までにTLS 1.3以降への対応要件を各々発行する (EO 14144 Sec. 4(f)(v))	同じ規定を維持 (修正令 Sec. 2(d) 4(f)(ii))	変更なし TLS要件は継続
6	PQC基本認識	量子コンピュータの脅威とCRQC（暗号解読関連量子コンピュータ）の定義、NSM-10への言及 (EO 14144 Sec. 4(f)冒頭)	同じ記述を維持 (修正令 Sec. 2(d) 4(f)冒頭)	変更なし 基本的な脅威認識は共有

https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/

NISTが発行したPQCに関する標準仕様

- 2024年8月13日 NISTからFIPS 203/204/205 の最終版が遂に公開された

旧名称	新名称	標準仕様名
CRYSTALS-Kyber	ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)	FIPS 203
CRYSTALS-Dilithium	ML-DSA (Module-Lattice-Based Digital Signature Algorithm)	FIPS 204
SPHINCS+	SLH-DSA (Stateless Hash-Based Digital Signature Algorithm)	FIPS 205
FALCON	FN-DSA (FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm)	FIPS 206 ※現在、公開待ち
HQC	？？？	FIPS 20X ※ 2027年予定

・FIPS 203 ML-KEM (Kyber): https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf
・FIPS 204 ML-DSA (Dilithium): https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf
・FIPS 205 SLH-DSA (SPHINCS+): https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.205.pdf

PQCアルゴリズムとデータサイズ比較 (128bit安全相当)

GMOコネクト株式会社

カテゴリー	アルゴリズム名	利用する問題		データサイズ（byte）		
				公開鍵	秘密鍵	暗号文/署名
公開鍵暗号/KEM	***ML-KEM***	Module-LWE問題	Lattices	800	1,632	760
	BIKE	QC-MDPC符号のSDP	Code	1,540	280	1,572
	Classic McEliece	Gappa符号のSDP	Code	261,120	6,492	128
	HQC	Quasi-Cycle符号のSDP	Code	2,249	40	1,572
デジタル署名	***ML-DSA***	Module-LWE問題	Lattices	1,312	2,528	2,420
	FN-DSA	SIS問題	Lattices	897	7,533	666
	SLH-DSA	ハッシュ関数の衝突探索問題	Hash	32	64	7,856

※ 128bit安全相当を実現した際のデータサイズ
※ 太字・斜体はコンペの勝者

詳細は、PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates
https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

PQCアルゴリズムとデータサイズ比較 (256bit安全相当)

GMOコネクト株式会社

カテゴリー	アルゴリズム名	利用する問題		データサイズ（byte）		
				公開鍵	秘密鍵	暗号文/署名
公開鍵暗号/KEM	***ML-KEM***	Module-LWE問題	Lattices	1,568	3,168	1,568
	BIKE	QC-MDPC符号のSDP	Code	5,122	580	5,154
	Classic McEliece	Gappa符号のSDP	Code	1,357,824	14,120	240
	HQC	Quasi-Cycle符号のSDP	Code	7,245	40	14,469
デジタル署名	***ML-DSA***	Module-LWE問題	Lattices	2,592	4,864	4,595
	FN-DSA	SIS問題	Lattices	1,793	13,953	1,280
	SLH-DSA	ハッシュ関数の衝突探索問題	Hash	64	128	49,856

※ 256bit安全相当を実現した際のデータサイズ
※ 太字・斜体はコンペの勝者

詳細は、PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates
https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

【結論】

NISTによってPQC選定済み
データサイズの巨大化が止まらない

DNSを取り巻く現状と標準化動向

PQCへの移行によるDNS / DNSSECでの懸念点は？

GMOコネクト株式会社

近年、IETFやOARC45などでPQC移行により発生することの懸念点は以下のようなものが挙げられている。

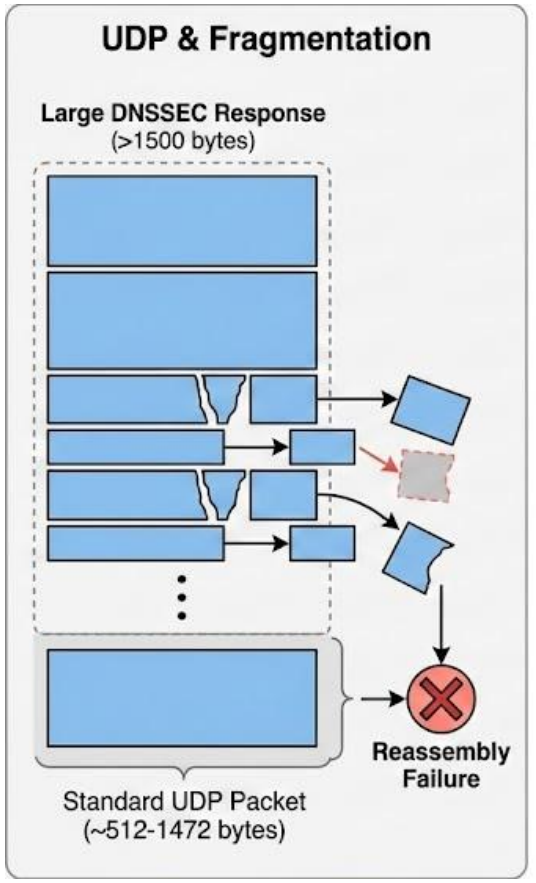
- **Fragmentation**
  - UDPの限界とIPフラグメンテーション問題
- **Key Rollover at Root/TLD**
  - 鍵ロールオーバーの困難化
- **Verification exhaustion**
  - 署名検証によるDoS攻撃耐性の低下

次のスライド以降で詳しく掘り下げて理解を深めます

Fragmentation: UDPの限界とIPフラグメンテーション問題

GMOコネクト株式会社

- 課題:
  - ML-DSAの署名サイズはUDPの推奨ペイロードサイズ（1232 bytes）を超過してしまう
- 影響:
  - IPフラグメンテーションが発生すると、ファイアウォールでドロップされやすくなり（DNS Flag Day 2020の逆行）、名前解決の信頼性が低下する
- 結果:
  - TCPへのフォールバックが頻発し、DNSサーバのリソース枯渇やレイテンシ増大を招く



<参考：128bit安全相当>

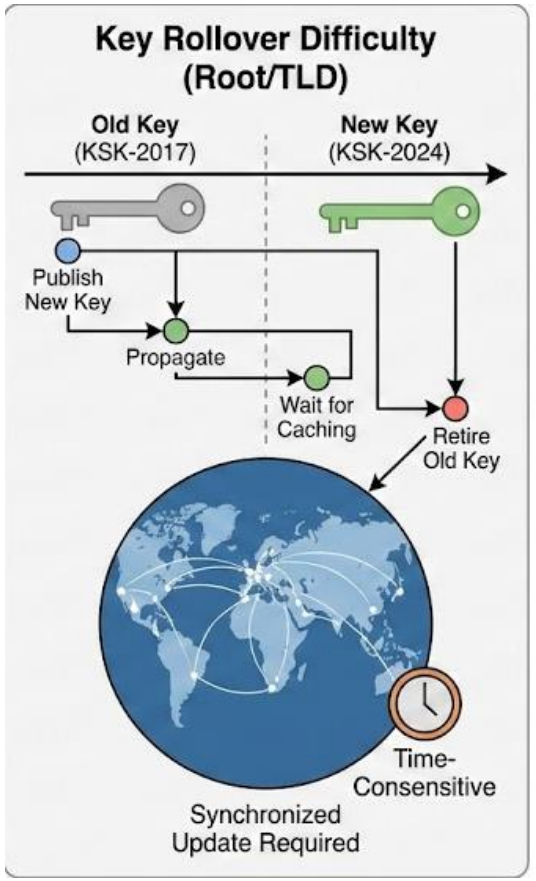
カテゴリー	アルゴリズム名	利用する問題		データサイズ（byte）		
				公開鍵	秘密鍵	暗号文/署名
公開鍵暗号/KEM	ML-KEM	Module-LWE問題	Lattices	800	1,632	760
	BIKE	QC-MDPC符号のSDP	Code	1,540	280	1,572
	Classic McEliece	Gappa符号のSDP	Code	261,120	6,492	128
	HQC	Quasi-Cyclic符号のSDP	Code	2,249	40	1,573
デジタル署名	ML-DSA	Module-LWE問題	Lattices	1,312	2,528	2,420
	FN-DSA	SIS問題	Lattices	897	7,553	666
	SLH-DSA	ハッシュ関数の衝突探索問題	Hash	32	64	7,856

【参考情報：DNS Flag Day 2020】
IPフラグメンテーションに起因する通信遅延やセキュリティリスクを防ぐための取り組みです。
EDNSバッファサイズの推奨値を1232bytesに設定し、それを超える応答はTCPへフォールバックさせ、より堅牢で確実なDNS通信を目指している。
https://www.dnsflagday.net/2020/index.html

Key Rollover at Root/TLD: 鍵ロールオーバーの困難化

GMOコネクト株式会社

- 課題:
  - ZSK（Zone Signing Key）ならまだしも、KSK（Key Signing Key）をPQC化する場合、親ゾーン（TLDやRoot）のDSレコードも巨大化する…
- 影響:
  - 親ゾーンへの登録パケットサイズ制限に抵触したり、親ゾーンのファイルサイズが肥大化する懸念がある
- 解決に向けた動向:
  - これを解決するために議論されている DELEG レコード(※)やDSレコードの署名を省略する提案などあり
  - DELEGレコードは、親ゾーン（TLD）には「PQC対応の鍵情報そのもの」ではなく、「PQC対応のネームサーバへのヒント（SVCB形式）」を置くだけで良くなるため、親ゾーンの肥大化問題を根本解決できる可能性あり

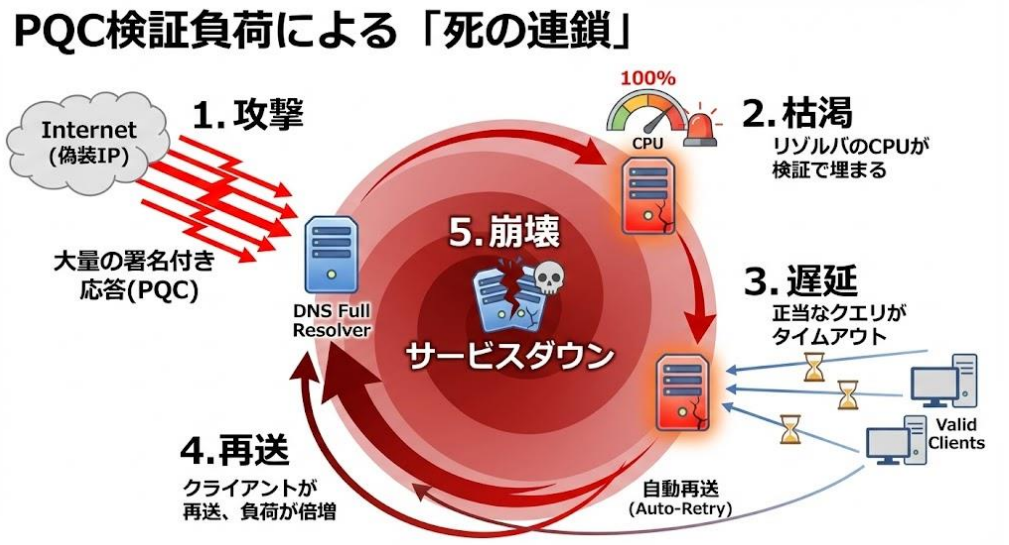


【参考情報：DELEG レコード】
IETF DNS Delegation (DELEG) WGにて” Extensible Delegation for DNS”というInternet-Draftで検討。
DNSの委任情報を現代化する新技術です。従来のNSレコードとは異なり、SVCB形式で通信プロトコルDoT/DoQ）や鍵情報を指定する

Verification exhaustion: 署名検証によるDoS攻撃耐性の低下

GMOコネクト株式会社

- 課題:
  - PQC署名（ML-DSAやSLH-DSA）の検証コストはECDSAの8〜15倍に及ぶ！
- 影響:
  - リゾルバ（キャッシュDNS）側のCPU負荷が跳ね上がるため、悪意を持って大量の署名検証をさせる攻撃（CPU exhaustion DoS）に対して脆弱になる
- 結果:
  - 正当なクエリの巻き添え（Noisy Neighbors Effect）、再送の嵐による事態悪化、運用コストとエネルギー消費の急増を引き起こす



リソースの視点からどの程度の影響があるのか？

GMOコネクト株式会社

- 公開情報をベースにリソースの観点の比較で影響が浮き彫りに！

リソース	ECDSA	ML-DSA（Dilithium-2）	FN-DSA（FALCON-512）	SLH-DSA（SPHINCS+-128s）	Ref
帯域/パケット	64 byte (x1)	2,420 byte (x38)	666 byte (x10)	7,856 byte (x123)	★1
ストレージ/キャッシュ	x1	x38	x10	x67	★2
CPU負荷	x1	x8～12	x4～6	x15	★3

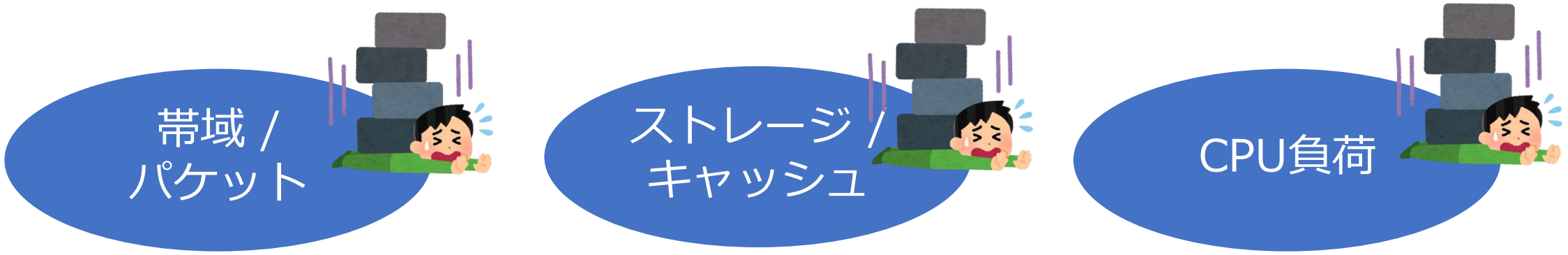
※ 128bit安全相当

- 帯域/パケット（★1）
  - https://openquantumsafe.org/liboqs/algorithms/sig/dilithium.html
  - https://openquantumsafe.org/liboqs/algorithms/sig/falcon.html
  - https://openquantumsafe.org/liboqs/algorithms/sig/sphincs.html
- ストレージ/キャッシュ（★2）
  - https://blog.verisign.com/security/post-quantum-dnssec-preparation/
- CPU負荷（★3）
  - https://blog.powerdns.com/2024/07/15/more-pqc-in-powerdns-a-dnssec-field-study
  - https://www.ndss-symposium.org/wp-content/uploads/2020/02/24203.pdf

PQC移行によるDNSへの懸念事項をまとめる

GMOコネクト株式会社

- PQC移行は「DNSインフラのキャパシティ耐性」への挑戦
  - ざっくりいうと、インフラ資源に対する負荷試験のような状態？！



PQC移行は「暗号を変更するだけ」の話だけではなく
DNSの在り方を問いかけるような重みあり

【参考情報】PQC移行による懸念・影響

GMOコネクト株式会社

- リフレクションDDoS攻撃の攻撃力アップ
  - PQCによりサイズ膨張 => 帯域増幅率の跳ね上がる
  - EDNS0・TCP フォールバック を徹底すれば帯域アンプリフィケーション自体は抑え込めるが、セッション枯渇型 DoS の可能性も？
- Resource Record Signature (RRSIG) サイズの爆発
  - UDP 1232 byte制限にヒット → ML-DSAを含む負荷応答は 必ず断片化または TC=1
- ゾーン肥大化と転送コスト
  - com ゾーン 現行署名と比較して SLH-DSA →67 倍、ML-DSAでも 37 倍に膨張（Verisign試算）
  - TLD や ccTLD のバックアップ/ミラー設備が容量不足に陥る懸念？
- 署名検証コストとエネルギー消費量増加
  - ML-DSA 検証は ECDSA の8倍、SLH-DSAで15倍（PowerDNS 実験より）
  - ルートサーバクラスで年間 追加消費電力 ≈ 15 MWh と推計（ECDSA→ ML-DSA 切替時）

などなど...

現状を打破するための
活動はないの？

どのようなところで課題解決に向けた議論がされているのか？

GMOコネクト株式会社

- 現在、人類は顕在化してきた懸念や問題に対して、実験やHackathonを通してナレッジを蓄積している

- 直近でDNSSECにおけるPQC移行についての調査報告等が活発ないくつかの活動について議論を共有します

NIST： PQC標準化の第2波 / On-Ramp プロジェクト

GMOコネクト株式会社

- 目的: PQCの**多様性確保**（Latticeベース中心の選定からの脱却）と**特定用途**（短い署名など）への最適化を狙っている
- 背景: FIPS 204 (ML-DSA) や FIPS 206 (FN-DSA) は格子暗号ベース。もし格子ベース暗号に致命的な脆弱性が見つかった場合の「**保険**」が必要という着想
- DNSにとっての注目ポイント ⇨ 署名サイズの削減
  - 現在のPQC署名（ML-DSA等）は、DNSパケット(UDP)にはまだ大きいという課題がある
  - On-Rampでは検証速度を犠牲にしてでも「**署名サイズが極めて小さい**」アルゴリズムを検討
- 今後の見通し (2025年11月時点)
  - 現在、候補アルゴリズムの選定・評価プロセスが進行中で、標準化完了は数年先（2027-2028年以降？）の見込み
- 結論: **「銀の弾丸」になる可能性はある**が、現時点の移行計画（2030年問題対応）の前提にはできないので要注意！

【参考情報：On-Rampでのアルゴリズム例】https://csrc.nist.gov/projects/pqc-dig-sig
- 多変数多項式暗号 (Multivariate): 例：UOV (Unbalanced Oil and Vinegar)
  - 署名は小さいが、公開鍵が非常に大きい（DNSには不向き？）
- 同種写像暗号 (Isogeny-based): 例：SQISign
  - 署名サイズがRSA並みに小さいのが最大の特徴。DNSSECにとって理想的だが、署名・検証の計算コストが高い

DNS OARC45（1/2）

GMOコネクト株式会社

- 2025年10月7-8日に開催され、”Post-Quantum Diversity for DNSSEC: Routine Performance, Resilient Fallback”という発表あり
- 注目する点として、**Routine Performance(＝普段使い)とResilient Fallback(＝保険)向けの2種類のPQC併用戦略**です！

- 併用戦略のキモチ
  - Routine Performance
    - メリット：署名サイズが小、処理が高速、アルゴリズム移行が容易
    - デメリット：新しい暗号学的仮定なので安全性評価の歴史が浅い。脆弱な可能性も！？
  - Resilient Fallback
    - メリット：ハッシュ関数など長年の信頼がある、量子計算機耐性あり
    - デメリット：署名サイズが巨大、UDPパケットには無理
      - 解決方法として、複数のDNSレコードに1つの署名を共有できるMTL (Merkle Tree Ladder) モードによって実用的な署名サイズ（1.6KB）に！

https://indico.dns-oarc.net/event/55/contributions/1181/attachments/1136/2377/Post-Quantum%20Diversity%20for%20DNSSEC%20OARC%2045.pdf

DNS OARC45 （2/2）

GMOコネクト株式会社

- Routine PerformanceとResilient Fallback併用戦略での運用イメージ

【PQC移行時に脆弱性発見】

2026年: PQC-X標準化
└→ Routine: PQC-X
Fallback: SLH-DSA-MTL (待機)

2028年: PQC-Xに理論的脆弱性発見！
└→ 即座にFallbackへ切り替え
Routine: 停止
Main Use: SLH-DSA-MTL（昇格）
※ 新たなRoutine候補を選定

2030年: 新しいアルゴリズム(PQC-Y)標準化
└→ Routine: PQC-Y
Fallback: SLH-DSA-MTL (再び待機)

【DNS運用者の選択肢】

【Rootゾーン】
保守運用が重要
→ Resilient Fallback (SLH-DSA-MTL) を選択
→ 鍵の事前公開期間が長いので安全性重視

【TLDゾーン】
署名数が多い(数百万レコード) 、高可用性の要求
→ Routine Performance (MAYO/HAWK) を選択
→ MTLモードの署名償却効果も大きい

【その他ゾーン(Second-Level以下)】
各組織のポリシーに応じて選択
→ 両方をサポート、状況に応じて使い分け

https://indico.dns-oarc.net/event/55/contributions/1181/attachments/1136/2377/Post-Quantum%20Diversity%20for%20DNSSEC%20OARC%2045.pdf

IETF 124

GMOコネクト株式会社

- 2025年11月1～7日に開催され、
  - 11月1～2日にIETF Hackathonで” PQC DNSSEC MTL Mode Update”
  - 11月7日にDNSOP WGで”**Post-Quantum DNSSEC**”などの発表が行われた。

【DNSOP WG】
- PQC DNSSEC戦略の提示
  - 2種類のアルゴリズム戦略(Routine Performance + Resilient Fallback)
  - draft-sheth-pqc-dnssec-strategyの紹介
- コミュニティの進捗報告
  - IETF 122, 123でのハッカソン成果
  - オープンソース実装の進展(BIND, NSD, Unbound, CoreDNS)
- 標準化の所在に関する重要な議論
  - 「Where does this work belong?」という問題提起
  - 議論サマリー:
    - DNSOP: DNSSECコンポーネントを扱うが、Merkle tree構造には不向きかも
    - CFRG: MTLモードの作業を引き受けることに興味を示さなかった
    - PLANTS (新設中): Merkle tree構造を含む作業を扱う予定だが、証明書以外にも対応すべきか?

https://datatracker.ietf.org/meeting/124/materials/slides-124-hackathon-sessd-ietf-124-hackathon-pqc-dnssec-mtl-mode-update-00

https://datatracker.ietf.org/meeting/124/materials/slides-124-dnsop-sessb-post-quantum-dnssec-00

DNSにおけるPQC実装状況が気になる…

GMOコネクト株式会社

- DNS運用者の実務者としては、最先端の議論がどのようなところで行われているのか把握できたけど、実際に動作する実装はどんな状況なのか？と気になるところ…

主要なソフトウェア実装状況

GMOコネクト株式会社

- 主要な実装におけるPQC対応状況のサマリーは以下のとおり。詳細については、リリースノート等をご確認ください。

実装	PQC署名対応状況	MTL対応	ステータス
BIND 9（ISC）	実験: ブランチ/オプションで一部対応	検討・PoC段階	実験（安定版へのマージ待ち）
NSD / Unbound（NLnet Labs）	実験: 複数PQC署名を評価中	PoCあり（評価用）	実験・検証中
Knot DNS（CZ.NIC）	限定的/実験対応中	未対応	実験（一部テスト版）
PowerDNS（Auth/Rec）	実験・評価中心	未対応	検証・ベンチマーク段階
CoreDNS	実験プラグイン等で評価	PoCあり（評価用）	実験的（本番利用は非推奨）

※ 2025年11月現在

実装状況（主要なDNSソフトウェア）

GMOコネクト株式会社

- IETF124 Hackathonの” PQC DNSSEC MTL Mode Update”より抜粋

Name server implementations

Reference Open-Source	Link	Algorithms
MTL reference library	https://github.com/verisign/MTL	MTL mode with SLH-DSA and ML-DSA
MTL LDNS library	https://github.com/verisign/mtl-mode-ldns	RSA, ECDSA, ML-DSA(1), FL-DSA(1), SLH-DSA(1), Mayo I/II(1), SQI Sign(1), Hawk(1), SNOVA(1) , SLH-DSA w/MTL mode(1), ML-DSA w/MTL mode(1)
NSD [authoritative name server]	https://github.com/NLnetLabs/nsd/pull/397	RSA(2), ECDSA(2), ML-DSA(2), FL-DSA(2), SLH-DSA(2), Mayo I/II(2), SQI Sign(2), Hawk(2), SNOVA(2) , SLH-DSA w/MTL mode(2)(3) , ML-DSA w/MTL mode(2)(3)
Unbound [recursive resolver]	https://github.com/verisign/mtl-mode-unbound	RSA(2), ECDSA(2), ML-DSA(2), FL-DSA(2), SLH-DSA(2), Mayo I/II(2), SQI Sign(2), Hawk(2), SNOVA(2) , SLH-DSA w/MTL mode(2)(3)), ML-DSA w/MTL mode(2)(3)
BIND [authoritative and recursive resolver]	TBD	RSA, ECDSA, FL-DSA(1), Mayo (1), SQI Sign(1), Hawk(1), ANTRAG-512, SLH-DSA w/MTL mode(1)
Core DNS [authoritative]	https://github.com/fjblanco/mtl_coredns_plugin	RSA, ECDSA, ML-DSA(1), FL-DSA(1), SLH-DSA(1), Mayo I/II(1), SNOVA(1) , SLH-DSA w/MTL mode(1)

Reference Source	Link	Algorithms
Core DNS [authoritative]	https://github.com/fjblanco/mtl_coredns_plugin	RSA, ECDSA, ML-DSA(1), FL-DSA(1), SLH-DSA(1), Mayo I/II(1), SNOVA(1) , SLH-DSA w/MTL mode(1)

1 - Enabled at compile time, depends on additional cryptographic libraries
2 - When signed with LDNS.
3 - Includes POC for MTL mode EDNS option.

4

以下に分類されるアルゴリズムが実装されている
- 現行暗号
- NIST PQC
- NIST On-Ramp
- MTL mode

https://datatracker.ietf.org/meeting/124/materials/slides-124-hackathon-sessd-ietf-124-hackathon-pqc-dnssec-mtl-mode-update-00

まとめ

まとめ

本講演では、次のことについてご紹介しました。

- 暗号の2030年問題
  - 128bit安全への移行 & PQC移行の2つの側面があるけど、どちらもデータサイズが障壁に！
- 「量子計算機」やNISTにより選定されたPQCアルゴリズム
  - PQC移行のタイムリミット
- DNS/DNSSECにおけるPQC移行で顕在化する懸念や課題
  - PQCは色々とデカい
  - DNSへの影響
- 顕在化した懸念や課題に向けた前向きな活動
  - NIST On-Rampプロジェクト、OARC、IETFなどによるPQC移行の促進
  - Hackathonなどによる相互運用性確認やPQCアルゴリズム実装による課題の抽出

最後にDNS運用に携わる皆さまへ

GMOコネクト株式会社

- 今すぐPQC署名を有効にする必要はないかもしれませんが、基本である「**DNSソフトウェアを最新**」に保ち、**TCP/EDNS0のパケットサイズ設定（1232bytes）が適切**か、自社のファイアウォールが**フラグメントパケットをドロップしていない**か、今のうちに足回りの点検を開始していただけたらと考えます。

今日からできる具体的な「Next Step」になります！

聴講していただいた皆さまに1bitでも
お役に立てたのであれば嬉しいです

PQC移行に向けた情報収集でお役立ち参考URL（1/2）

GMOコネクト株式会社

- NIST Post-Quantum Cryptography
  - FIPSの最終版公開、追加ラウンドの標準化、実装ガイダンスが公開
  - https://csrc.nist.gov/projects/post-quantum-cryptography
- IETF DNSOP WG
  - DNSSEC関連のドラフト更新、運用上の課題議論され、知見を標準化
  - https://datatracker.ietf.org/wg/dnsop/documents/
- IETF PQUIP WG
  - PQC移行に向けたガイドや運用手順、実装者向け文書などを標準化
  - https://datatracker.ietf.org/wg/pquip/documents/
- DNS-OARC (DNS Operations, Analysis, and Research Center)
  - ワークショップ発表資料、PQC実測データ、運用者コミュニティの議論に関する情報豊富
  - https://www.dns-oarc.net/

PQC移行に向けた情報収集でお役立ち参考URL（2/2）

GMOコネクト株式会社

- Verisign Labs - PQC DNSSEC Research
  - MTLモードの技術論文、ルートゾーン実験結果、署名サイズ最適化研究に関する情報あり
  - https://www.verisign.com/en_US/company-information/verisign-labs/index.xhtml
- ICANN SSAC (Security and Stability Advisory Committee)
  - PQC移行に関するアドバイザリ文書、リスク評価レポートに関する情報あり
  - https://www.icann.org/groups/ssac
- NLnet Labs - DNSSEC & PQC Implementation
  - NSD/Unboundの実装進捗、実験的機能のリリースノート、技術ブログの情報あり
  - https://www.nlnetlabs.nl/projects/

何か気になることなどあれば～

GMOコネクト株式会社

- E-mail
  - kanno@gmo-connect.jp
- SNS
  - X (旧Twitter)
    - https://x.com/satorukanno
  - Facebook
    - https://www.facebook.com/satoru.kanno

お気軽にご連絡ください！

すべての人にインターネット