量子時代の足音
--暗号2030年問題とDNSの持続可能性

GMOサイバーセキュリティ byイエラエ株式会社
菅野　哲

2025年6月27日

この人、誰？

- 名前
  - 菅野 哲（かんの さとる）
- 所属
  - GMOサイバーセキュリティ byイエラエ株式会社 (～ 2025年6月30日)
    - 上席執行役員
  - GMOコネクト株式会社(2025年7月1日～)
    - 執行役員
  - 公正取引委員会
    - デジタルアナリストとして活動（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、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事業サポートがメイン
    - CRYPTREC 暗号鍵管理ガイダンスWG 委員

Agenda

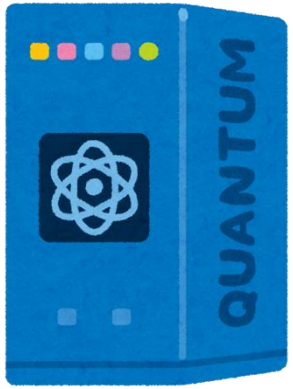
- 量子計算機を振り返る
- 暗号の2030年問題
- DNSの持続可能性への影響
- まとめ

暗号から見た

量子計算機を振り返る

暗号技術への脅威となる量子計算機

- 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

- CRQCの発現による現行暗号への影響は？
  - 共通鍵暗号（例：AES、ChaCha20等）　・・・小
  - 公開鍵暗号（例：RSA、ECDSA等）　・・・**大**

この違いは…
気になる

CRQCが与える現行暗号への影響度

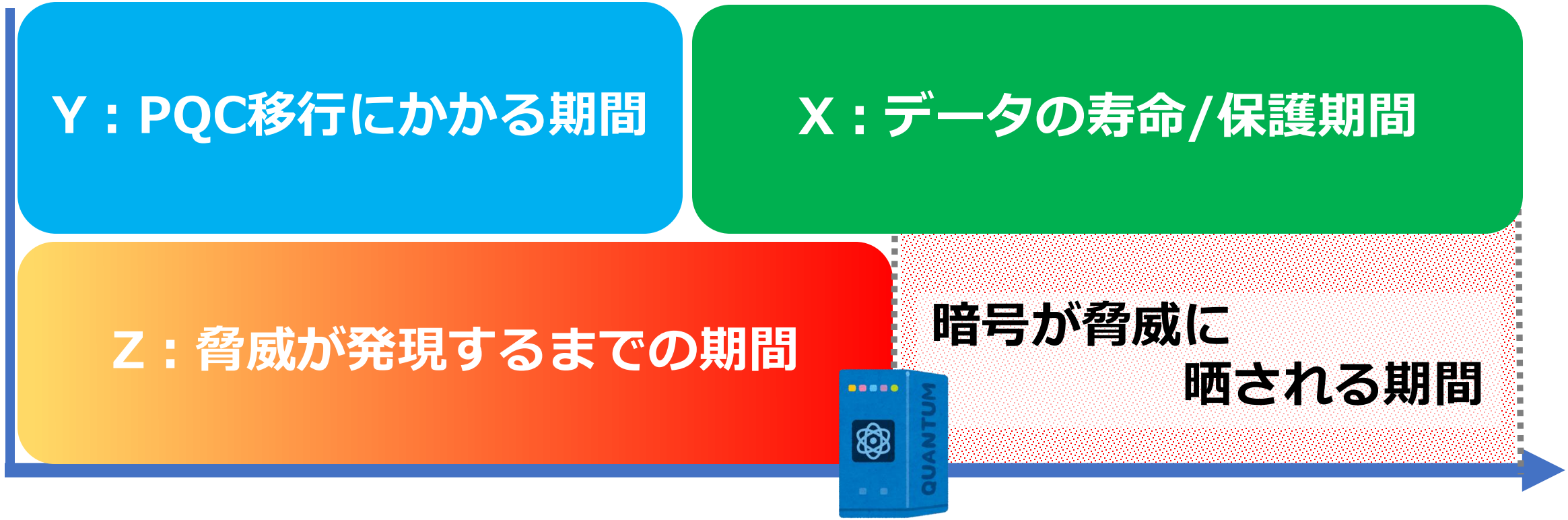
No	暗号の種類	現行暗号例	脅威となる量子アルゴリズム	効率的に解ける問題	暗号への脅威	望ましい対策
1	共通鍵暗号	AES	Grover's Alg	データ探索問題	限定的	鍵長の伸長/暗号利用モードの変更
2			Simon's Alg	周期探索問題	限定的	
3	公開鍵暗号	RSA	Shor's Alg	素因数分解	非常に大きい	PQCへの移行
4		DSA/ECDSA	Shor's Alg	離散対数問題		
5		PQC	（現状）未発見	ー	現在なし	ー

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

脅威となる量子アルゴリズムが未発見な「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

- 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 quick[illegible] 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？

暗号の2030年問題

「暗号の2030年問題」とは？

「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

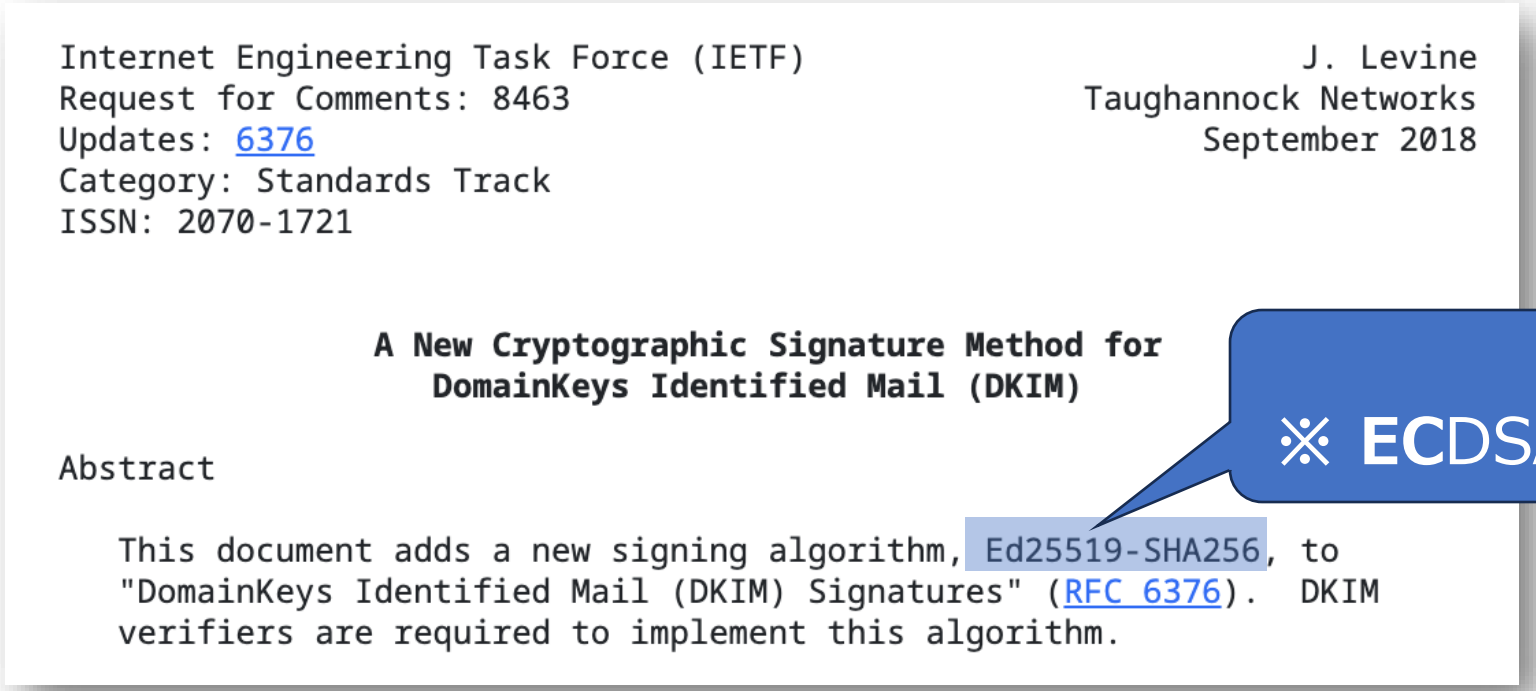
CRQCによる現行暗号への
リスクが許容できない

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



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.

この制約が厳しい…

EdDSA
※ **EC**DSAでないことに注意

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

現行暗号からPQC移行への始まり

- 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

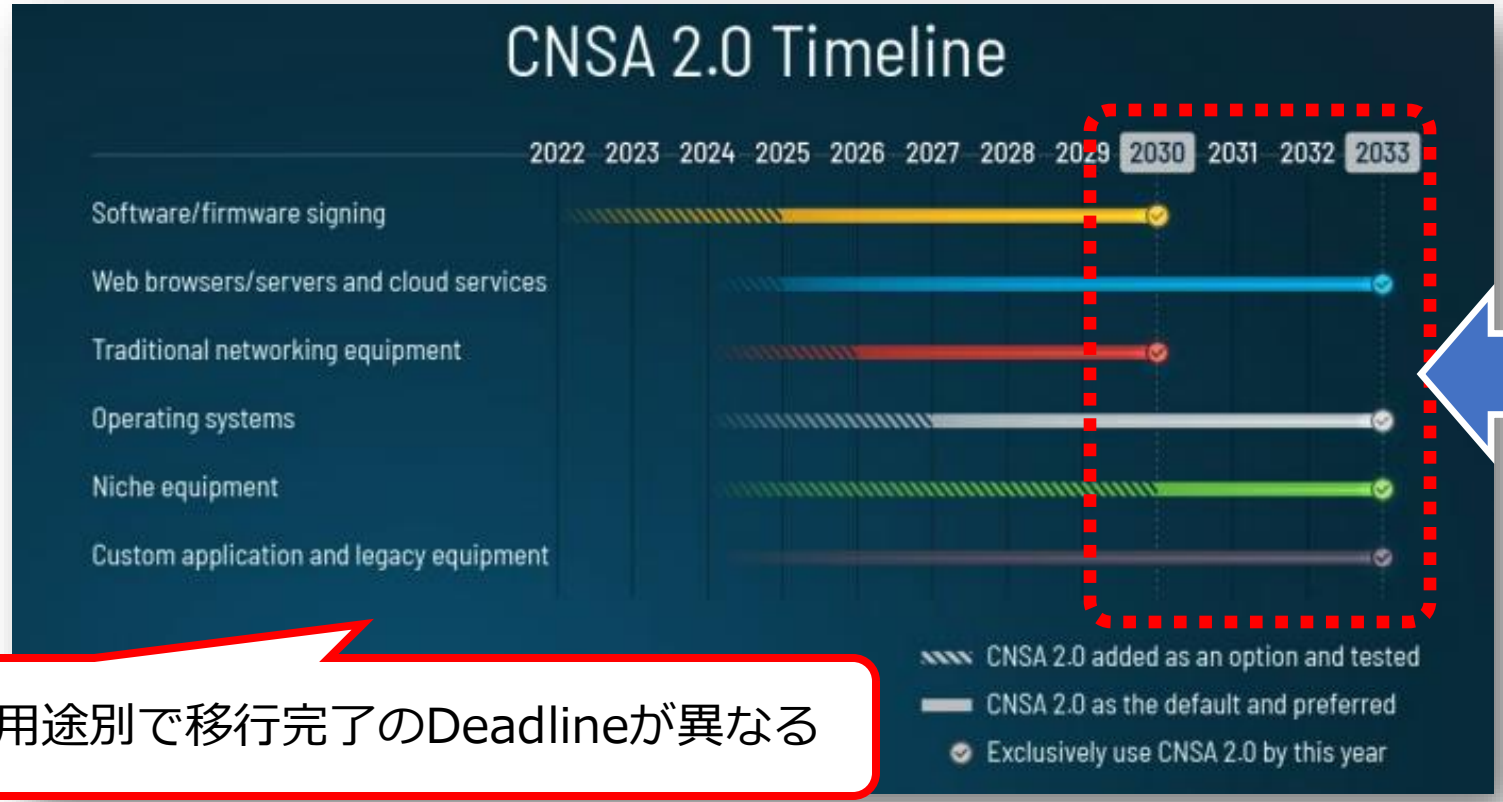
NATIONAL SECURITY MEMORANDUM/NSM-10

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

- 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



用途別で移行完了のDeadlineが異なる

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

NSA「Announcing the Commercial National Security Algorithm Suite 2.0」より
https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

直近のアメリカ政府の動向

- 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 ※現在策定中
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)

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	***CRYSTALS-KYBER***	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	***CRYSTALS-DILITHIUM***	Module-LWE問題 Lattices	1,312	2,528	2,420
	FALCON	SIS問題 Lattices	897	7,533	666
	SPHINCS+	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)

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	***CRYSTALS-KYBER***	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	***CRYSTALS-DILITHIUM***	Module-LWE問題	Lattices	2,592	4,864	4,595
	FALCON	SIS問題	Lattices	1,793	13,953	1,280
	SPHINCS+	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】

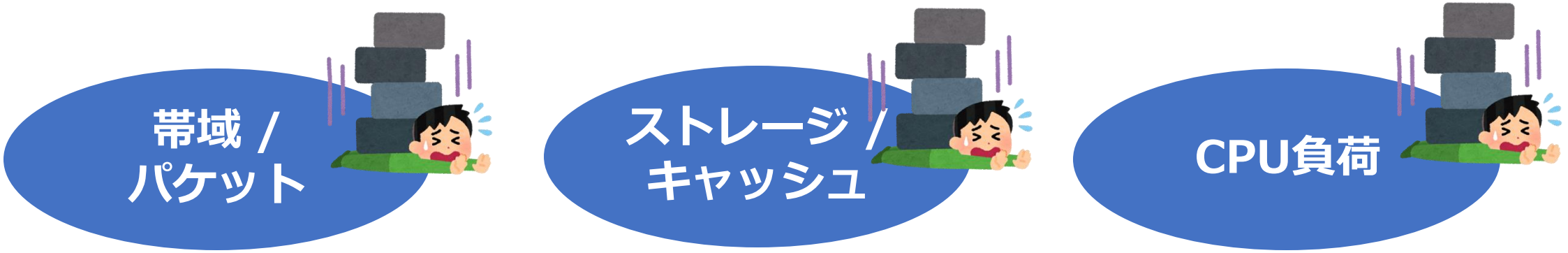
処理も

PQCは基本的に色々とデカい

DNSの持続可能性への影響

なぜ「DNSの持続可能性」に注目したのか？

- DNSから見ると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、インフラ資源が「精神と時の部屋」に入った状態



DNSから見るとPQC移行は暗号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

どのくらいの影響があるのか？をふんわり可視化

- 公開情報からそれぞれの観点で比較することで、影響が見えてくる

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

まだまだあるぞ？ 持続可能性を脅かすポイント

- 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...

DNSのPQC対応に向けた取り組み（現状）

- PQC対応に関する正式なRFCはまだ策定されていない
  - 標準化に向けた実験と知見共有が活発化している
- PQC対応に向けたフィールドテスト
  - 欧米のDNS運用組織（SIDN LabsやdeSECなど）や実装プロジェクト（ISCのBIND 9、PowerDNSなど）が協力
  - PQC署名（FALCON-512やDilithium-2、SPHINCS+128s、XMSS）を実際にDNSへ実装・テストを実施
- これらの知見はどこで活用されるの？
  - IETFやICANNへフィードバック
  - 例：ICANN83（2025年6月）
    - PQC FOR DNSSEC -The Good, the Bad and the Ugly
      https://www.isc.org/docs/osury_pqc_dnssec_presentation0625.pdf

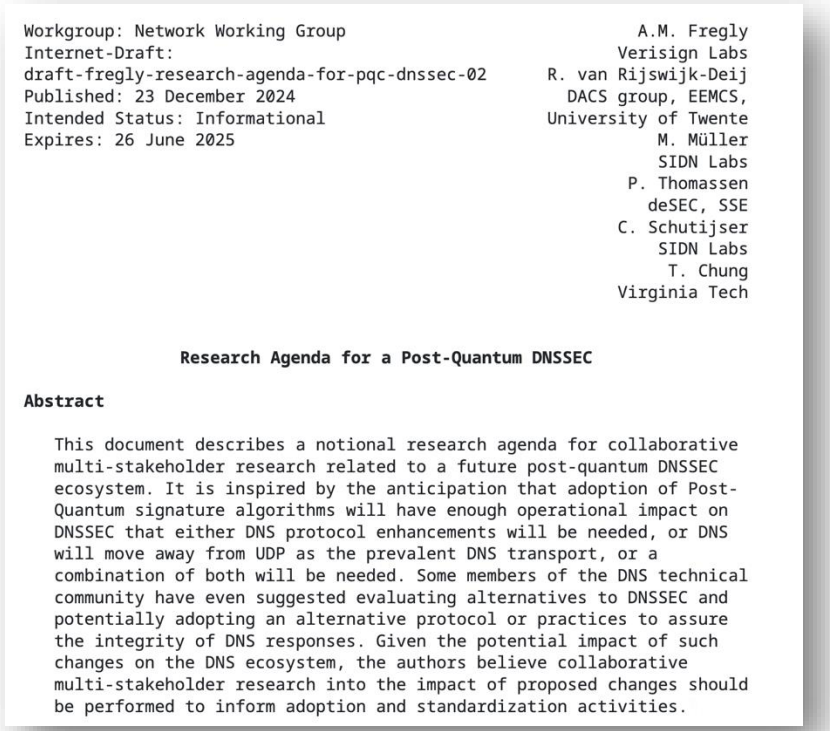
IETFでのPQCを知りたい…

- **I**nternet **E**ngineering **T**ask **F**orce
  - **インターネットに関する技術**の国際標準を策定する組織
  - 生産物としてRFC （Request for Comments）を発行

- PQC対応について把握するための近道
  - CRYPTO Forum（CFRG）
    - インターネットで将来的に必要な暗号技術を検討するResearch Group
    - https://datatracker.ietf.org/rg/cfrg/about/
  - Post-Quantum Use in Protocols (PQUIP) WG
    - PQC移行を支援する運用および設計ガイダンスを文書化
    - https://datatracker.ietf.org/wg/pquip/about/

IETFでの「DNS x PQC」に関する動向

- Internet Draft “Research Agenda for a Post-Quantum DNSSEC”がある
  - 残念なことに、2025年6月26日にExpiredになってしまったが、きっと更新版が投稿されるはず



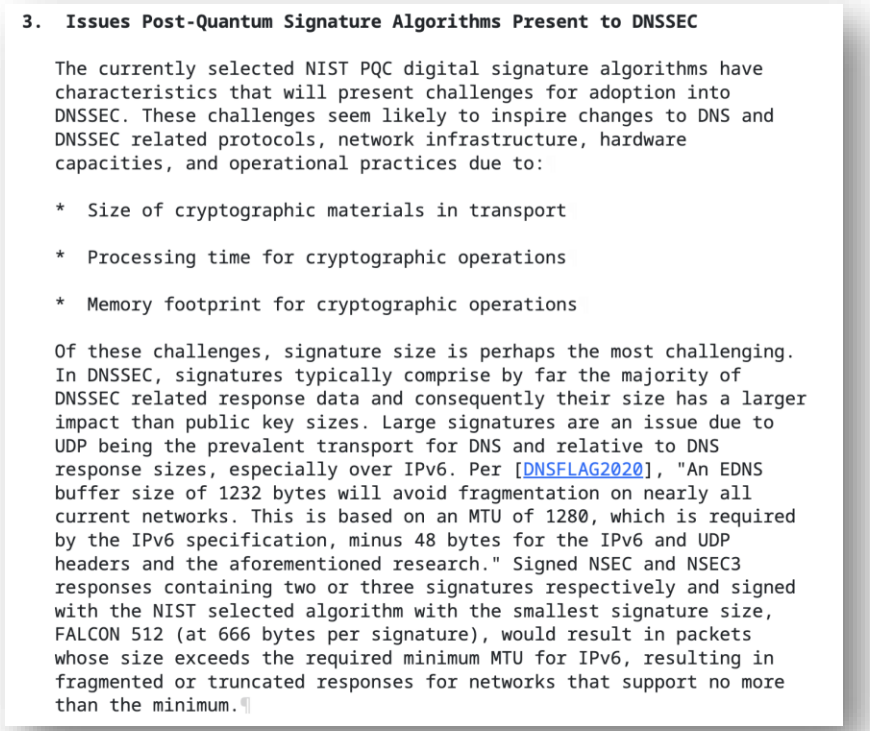
Workgroup: Network Working Group
Internet-Draft:
draft-fregly-research-agenda-for-pqc-dnssec-02
Published: 23 December 2024
Intended Status: Informational
Expires: 26 June 2025

A.M. Fregly
Verisign Labs
R. van Rijswijk-Deij
DACS group, EEMCS,
University of Twente
M. Müller
SIDN Labs
P. Thomassen
deSEC, SSE
C. Schutijser
SIDN Labs
T. Chung
Virginia Tech

Research Agenda for a Post-Quantum DNSSEC

Abstract

This document describes a notional research agenda for collaborative multi-stakeholder research related to a future post-quantum DNSSEC ecosystem. It is inspired by the anticipation that adoption of Post-Quantum signature algorithms will have enough operational impact on DNSSEC that either DNS protocol enhancements will be needed, or DNS will move away from UDP as the prevalent DNS transport, or a combination of both will be needed. Some members of the DNS technical community have even suggested evaluating alternatives to DNSSEC and potentially adopting an alternative protocol or practices to assure the integrity of DNS responses. Given the potential impact of such changes on the DNS ecosystem, the authors believe collaborative multi-stakeholder research into the impact of proposed changes should be performed to inform adoption and standardization activities.



3. Issues Post-Quantum Signature Algorithms Present to DNSSEC

The currently selected NIST PQC digital signature algorithms have characteristics that will present challenges for adoption into DNSSEC. These challenges seem likely to inspire changes to DNS and DNSSEC related protocols, network infrastructure, hardware capacities, and operational practices due to:

* Size of cryptographic materials in transport

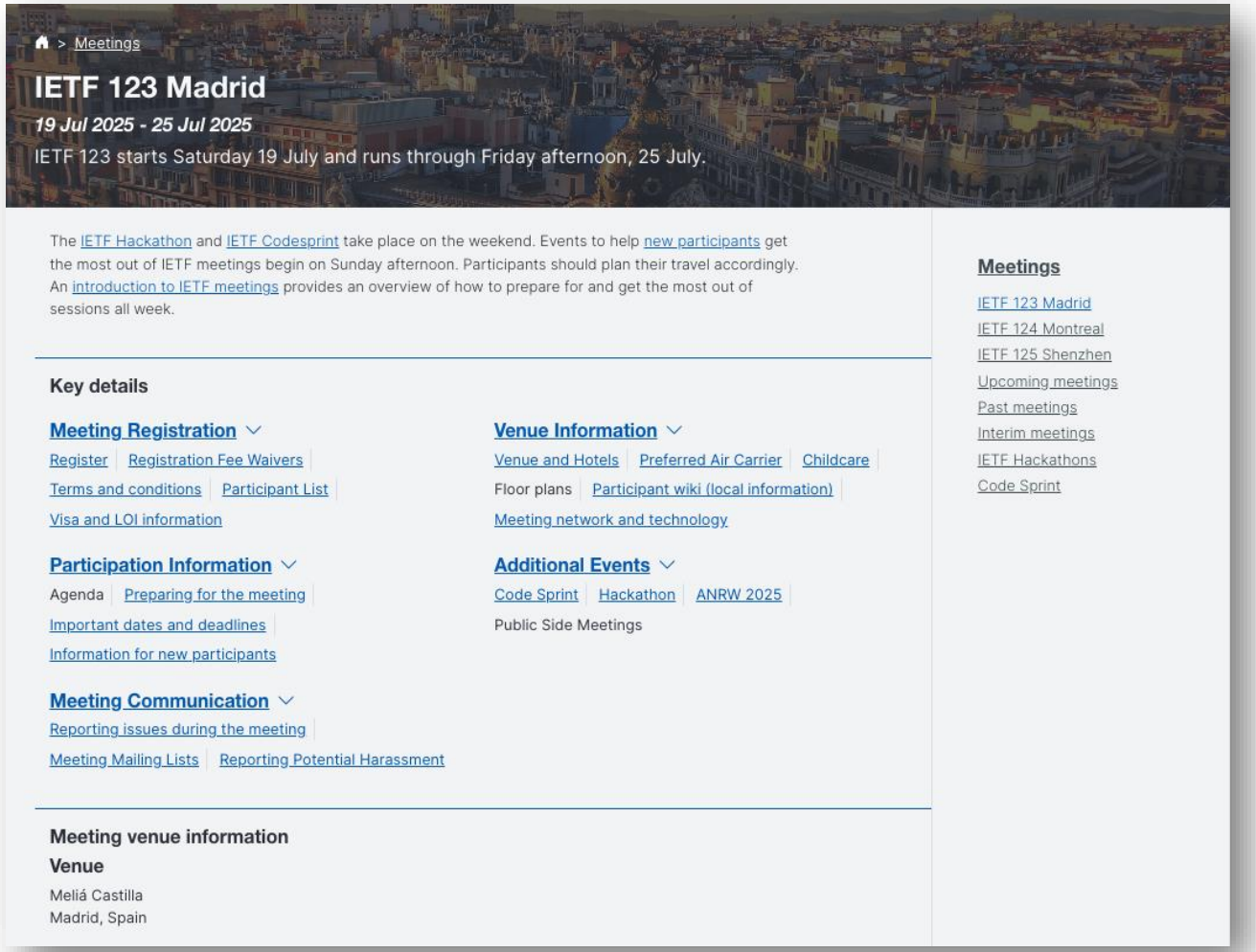
* Processing time for cryptographic operations

* Memory footprint for cryptographic operations

Of these challenges, signature size is perhaps the most challenging. In DNSSEC, signatures typically comprise by far the majority of DNSSEC related response data and consequently their size has a larger impact than public key sizes. Large signatures are an issue due to UDP being the prevalent transport for DNS and relative to DNS response sizes, especially over IPv6. Per [DNSFLAG2020], "An EDNS buffer size of 1232 bytes will avoid fragmentation on nearly all current networks. This is based on an MTU of 1280, which is required by the IPv6 specification, minus 48 bytes for the IPv6 and UDP headers and the aforementioned research." Signed NSEC and NSEC3 responses containing two or three signatures respectively and signed with the NIST selected algorithm with the smallest signature size, FALCON 512 (at 666 bytes per signature), would result in packets whose size exceeds the required minimum MTU for IPv6, resulting in fragmented or truncated responses for networks that support no more than the minimum.¶

https://datatracker.ietf.org/doc/draft-fregly-research-agenda-for-pqc-dnssec/

【共有】IETF 123 7月に開催



https://www.ietf.org/meeting/123/

- 2025年7月19日～25日の期間に開催されます！
- 現状、PQCに関連するセッションも開催予定！
  - PQUIP WG、CFRGも開催
  - IETF Hackathonも実施

まとめ

- 暗号から見た「量子計算機」をご紹介
  - CRQCの発現タイミング次第では「赤信号」か？
- 暗号の2030年問題をご紹介
  - NISTによるPQCコンペを経てアルゴリズムが出揃い始める
  - アメリカ政府のPQCに対する対応は気になる
  - PQCは色々とデカい
- DNSへの持続可能性への影響
  - PQC移行によるDNSインフラのキャパシティ耐性への挑戦

何か気になることなどあれば～

- E-mail
  - kanno@gmo-connect.jp
- SNS
  - X (旧Twitter)
    - https://twitter.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