NICT提出資料

PQCの実装・活用状況調査

2026年3月30日

国立研究開発法人情報通信研究機構
小川一人、青野良範

耐量子計算機暗号(PQC：Post Quantum Cryptography)

- 高性能な量子コンピュータの実現
  - 理論上
    - ✓周期的な構造を発見することが得意
  - Shorのアルゴリズムの開発（1994年）
    - 量子コンピュータにより素因数分解を現実的な時間で求解するアルゴリズム
    - ✓この開発により、

      量子コンピュータ >> 現在のコンピュータ

      が示された。
  - Shorのアルゴリズムを利用して、素因数分解問題だけでなく離散対数問題を効率的に求解することが可能

耐量子計算機暗号(PQC：Post Quantum Cryptography)

- 高性能な量子コンピュータの実現により完全に危殆化する暗号方式
  ＝　素因数分解問題や離散対数問題の求解困難性を
  安全性の根拠とする暗号方式

CRYPTREC 電子政府推奨暗号リスト

技術分類		暗号技術	
公開鍵暗号	署名	DSA(注18)	離散対数
		ECDSA	離散対数
		EdDSA	離散対数
		RSA-PSS(注1)	素因数分解
		RSASSA-PKCS1-v1_5(注1)	素因数分解
	守秘	RSA-OAEP(注1)	素因数分解
	鍵共有	DH	離散対数
		ECDH	離散対数
共通鍵暗号	64ビットブロック暗号(注2)	該当なし	
	128ビットブロック暗号	AES	
		Camellia	
	ストリーム暗号	KCipher-2	
ハッシュ関数		SHA-256	
		SHA-384	
		SHA-512	
		SHA-512/256	
		SHA3-256	
		SHA3-384	
		SHA3-512	
		SHAKE128(注12)	
		SHAKE256(注12)	
（次ページに続く）			

危殆化する方式

リスト内のすべての公開鍵暗号

技術分類		暗号技術
公開鍵暗号	署名	DSA(注18)
		ECDSA
		EdDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)
（次ページに続く）		

耐量子計算機暗号(PQC：Post Quantum Cryptography)

- 高性能な量子コンピュータの実現より前にPQCを作る必要性
  - 最低でも“耐量子計算機性持つ公開鍵暗号”は必要

CRYPTREC 電子政府推奨暗号リスト

技術分類		暗号技術	
公開鍵暗号	署名	DSA(注18)	離散対数
		ECDSA	離散対数
		EdDSA	離散対数
		RSA-PSS(注1)	素因数分解
		RSASSA-PKCS1-v1_5(注1)	素因数分解
	守秘	RSA-OAEP(注1)	素因数分解
	鍵共有	DH	離散対数
		ECDH	離散対数
共通鍵暗号	64ビットブロック暗号(注2)	該当なし	
	128ビットブロック暗号	AES	
		Camellia	
	ストリーム暗号	KCipher-2	
ハッシュ関数		SHA-256	
		SHA-384	
		SHA-512	
		SHA-512/256	
		SHA3-256	
		SHA3-384	
		SHA3-512	
		SHAKE128(注12)	
		SHAKE256(注12)	
（次ページに続く）			

危殆化する方式

リスト内のすべての公開鍵暗号

技術分類		暗号技術
公開鍵暗号	署名	DSA(注18)
		ECDSA
		EdDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	該当なし
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)
（次ページに続く）		

耐量子計算機暗号(PQC：Post Quantum Cryptography)

- 共通鍵暗号の量子コンピュータ耐性について
  - Groverのアルゴリズム、Simonのアルゴリズム、BHTアルゴリズムを用いた攻撃が現在有効と考えられている。
    - これらのアルゴリズムおよび他のアルゴリズムに対する安全性解析は継続中

- 現時点での評価
  - 共通鍵暗号：現在の安全性レベルを保持するためには、鍵長を2倍にすればよい
  - ハッシュ関数：出力長384ビット以上を用いることが無難

量子コンピュータに暗号解析の脅威

- リアルタイム解読
  - 量子コンピュータの開発状況を考える限り、暗号をリアルタイムで解読するまでには、まだまだ時間を要する。

- ハーベスト攻撃　←　要注意
  - 現行の暗号方式で暗号化されたデータを保管し、量子コンピュータが完成された際に、復号を行う攻撃
    - 長期間の機密を維持する必要があるデータに対する攻撃

PQCの開発・標準化状況

- 米国、中国、韓国などで、公募選定が行われている。
  - ➢ 他の国では、ほとんどの国で米国の標準に追従する傾向がある。

- 米国の状況
  3種類のPQC（ML-KEM、ML-DSA、SLH-DSA）が標準化済
  以後、数個のアルゴリズムが標準化予定（下表参照）

標準化名	用途	呼称	提案技術	開発者
FIPS 203	鍵共有（KEM）	ML-KEM	CRYSTALS-Kyber	IBM、Google、Cloudflare、Leuven大学
FIPS 204	署名	ML-DSA	CRYSTALS-Dilithium	IBM、ENS Lyon、Ruhr大学
FIPS 205	署名	SLH-DSA	SPHINCS+	Cisco、Google、Eindhoven大学、他
（FIPS-206）	署名	（FN-DSA）	FALCON	IBM、PQShield、Rennes大学他
（FIPS-207）	鍵共有（KEM）	（HQC-KEM）	HQC	INRIA、Bordeaux大学他
	署名			

PQC実装に関する標準化状況

IETF：

- 既存プロトコルにPQCを組み込むためのWGを設置
  - TLS関連で多数のドラフトが存在
    - ✓TLS1.3では、PQCが導入された
  - SSH、IPsecにおけるハイブリッド鍵交換方式のドラフト等が審査中

主要プロダクトにおけるPQC実装状況

プロダクト名	種別	PQC対応状況	備考
Microsoft Edge	ブラウザ	対応済み	2023年11月リリース以降はデフォルトで有効
Google Chrome	ブラウザ	対応済み	2024年4月リリース以降はデフォルトで有効
Mozilla Firefox	ブラウザ	対応済み	2024年10月リリース以降はデフォルトで有効
Apple Safari	ブラウザ	対応済み	2025年9月リリース以降はデフォルトで有効
OpenSSL	ライブラリ	対応済み	
RHEL10	OS	対応済み	標準パッケージで提供あり
Ubuntu	OS	試験的実装済み	標準パッケージで提供なし 25.10 に導入する方向で検討
FreeBSD	OS	試験的実装済み	標準パッケージで提供なし ver15で標準的にサポートする方向で検討
Windows	OS	試験的実装済み	標準パッケージで提供なし 2025年5月以降Widows11＋Build27852で試験的実装
Windows Server	OS	対応済み	2025年11月リリース以降はデフォルトで有効

NICT内部
ライブネットから見るPQC利用率の現状

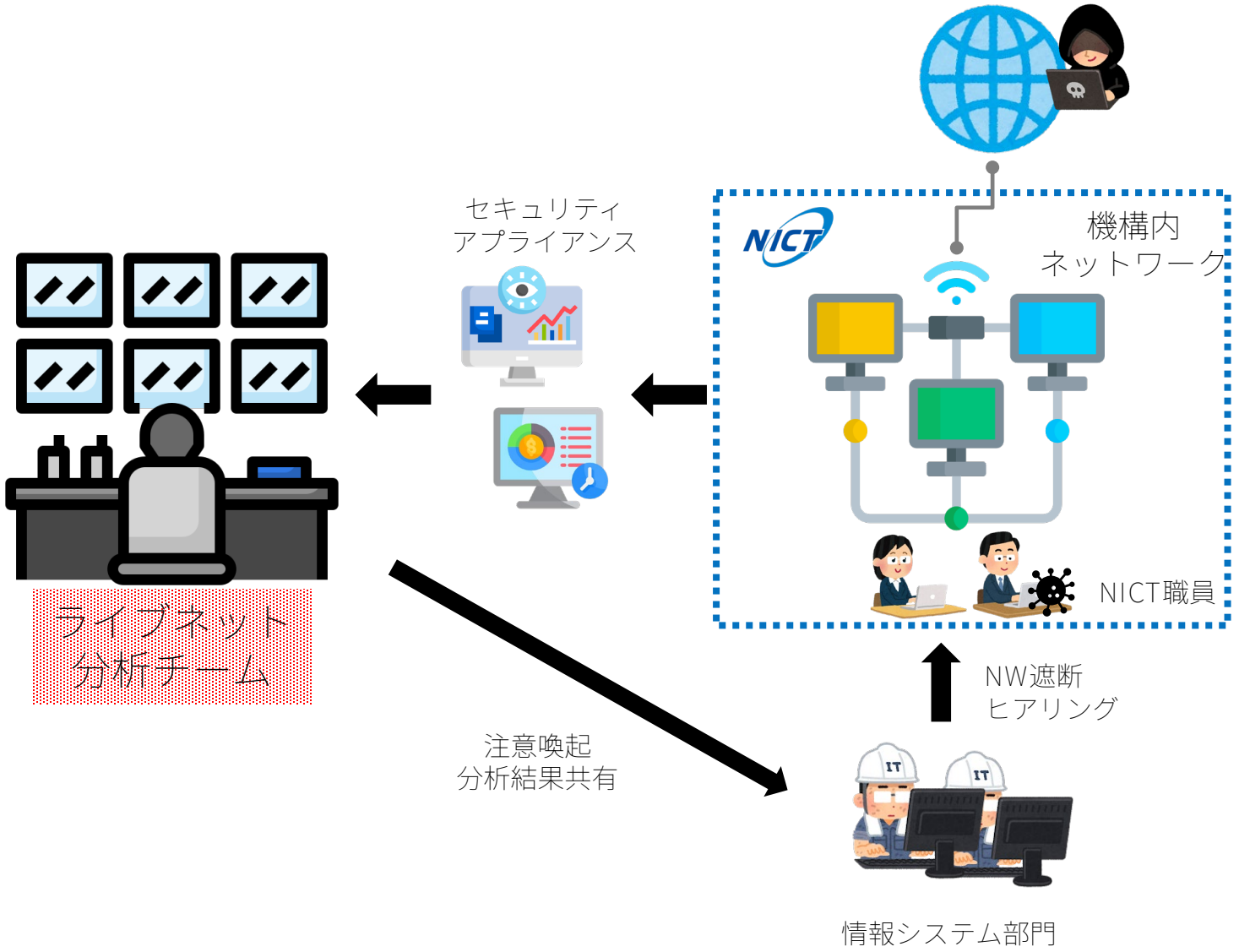
調査者
NICT　サイバーセキュリティ研究所
神宮真人　主任研究技術員

NICT National Institute of Information and Communications Technology

調査結果概要

- NICT内のトラフィック（ライブネットトラフィック）を対象にPQC利用率を調査
- PQC利用率は約12%　--- PQCの鍵交換をした割合
- PQC提案率は約43%　--- PQCの鍵交換を提案した割合
- PQC対応ドメインの傾向
  - Googleが圧倒的に多い
  - 広告・マーケティング業界、クラウド・CDN業界
  - 金融、政府
- PQC対応がクライアント側で先行し、サーバ側の対応が追いついていない
  - ただしQUIC (HTTP/3)に関してはサーバ側の対応が先行している

参考：ライブネット分析



分析対象

- NICTネットワーク(ライブネット）のトラフィック

オペレーション

- アラートを分析
- 情報システム部門と連携し、インシデント対処

分析

- アラートの統計処理
- 攻撃通信の分析
- SIEMルール整備・自動化
- 脅威情報を活用したスレットハンティング

ライブネットトラフィックでPQC利用状況を調査

- 調査対象
  - 2025年9月8日（月）の全トラフィック
  - 取り込んだファイルサイズ：約20TB
- PQC検知ツールを開発
  - https://github.com/nict-csl/PQC-Detector.git
  - プログラム言語：python3
  - パケット分析ライブラリ：pyshark
  - TLS Supported Group Mapping：WireSharkのライブラリをベースにNICTで作成
- 処理内容
  - tcpdumpでライブネットトラフィックを取得
  - ファイルからTLS ClientHelloとServerHelloパケットを抽出（TLS1.3, QUIC含む）
  - ClientHelloからSupportedGroupsとServerNameを含むCSVを出力
  - ServerHelloからKeyShareGroupとCipherSuiteを含むCSVを出力
  - CSVを集計してPQC提案率とPQC利用率を算出

PQC利用率集計結果

- PQC提案率：42.5% (2,991,932 / 7,044,025)ーーーPCからサーバへの提案
- PQC選択率：11.8% (810,056 / 6,877,907)ーーーサーバがPQC提案を選択
- 提案率と選択率で約3.6倍の差が存在
- クライアントが先行し、サーバが追いついていない状況

プロトコルについて

- TLS1.3、QUICのみ、PQCに対応している

業界別

- Google系は対応するドメイン数が非常に多い。
- 政府機関は対応するドメイン数が少ない。

ClientHello集計結果

- ClientHello総パケット数：7,044,025
- PQC提案数：2,991,932 (42.5%)
- TLSのPQC提案割合が約45%に対して、QUICは約8%と低い水準（ServerHelloと逆転）
  つまり、サーバ：QUICが先行、クライアント：TLSが先行
- 要素技術名：X25519MLKEM768が99.7%とほぼすべてとなっている。
- POP3, SMTPS等の通信においてもPQC提案が見られた

プロトコル別集計結果

Protocol	All	PQC	PQC Rate
TLS	6,611,799	2,955,765	44.7%
QUIC	423,226	36,167	8.4%
合計	7,044,025	2,991,932	42.5%

宛先Port別集計結果

宛先Port	PQC提案数
443	2,991,529
5228	271
8443	83
61613	33
992	9
44443	6
14443	1
合計	2,991,932

NamedGroup別集計結果

NamedGroups	PQC
X25519MLKEM768	2,983,340 (99.7%)
X25519Kyber768Draft00	8,592 (0.3%)

ServerHello集計結果

- ServerHello総パケット数：6,877,907
- PQC選択数：810,056
- TLS1.3のPQC割合が約15%に対して、QUICは約57％と高い水準で対応
- 要素技術：X25519MLKEM768が99.7%とほぼすべてとなっている。

プロトコルバージョン別集計結果

Protocol	All	PQC選択	PQC Rate
TLSv1.3	5,247,432	779,605	14.9%
TLSv1.2	1,571,317	0	-
QUIC	53,441	30,451	57.0%
TLSv1.0	5,402	0	-
TLS1.3 draft	315	0	-
合計	6,877,907	810,056	11.8%

送信元Port別集計結果

送信元Port	PQC
443	809,782
5228	272
993	2
合計	810,056

NamedGroup別集計結果

NamedGroups	PQC
X25519MLKEM768	807,766 (99.7%)
X25519Kyber768Draft00	2,290 (0.3%)

PQC対応ドメイン分析結果

- PQC対応ドメイン数：16,494
- PQC対応サーバ数：21,641　（同一ドメインで別ポートは別サーバとしてカウント）
- PQC対応の傾向
  - Google系のドメインは多い
  - 金融、政府のドメインは少ない

※注　調査データはNICT職員の業務通信に限定

表：主要テック企業別割合

企業	例	ドメイン数
Google系	Google Apps、YouTube、検索	5,119
Microsoft系	Office365, Teams, SharePoint	193
Amazon系	AWS S3, CloudFront	157
Apple系	iCloud	109

表：業界別割合

業界	例	ドメイン数
広告・マーケティング系	Google広告、DoubleClick	9,895
クラウド・CDN系	AWS, CloudFront	3,274
メディア・コンテンツ系	ニュース、メディア	2,725
コミュニケーション系	Slack, Teams, Zoom	792
政府・教育系	政府機関	596
金融系	銀行、金融	412

NICT以外による調査

- CloudFlare, “The state of the post-quantum Internet”, Mar. 2024. , https://blog.cloudflare.com/pq-2025/
  - 2024年3月時点でCloudflareのネットワーク上の約3.7%がPQC-KEM（ハイブリッド構成）を使用
  - Client 50%、Server 39%のPQC実装率
  - PQCによる鍵共有では4%の時間増がある

- Post-Quantum Cryptography (PQC) Network Instrument: Measuring PQC Adoption Rates and Identifying Migration Pathways. / Sowa, Jakub; Hoang, Bach; Yeluru, Advaith et al., 2024. p. 1835-1846 (Proceedings - IEEE Quantum Week 2024, QCE 2024; Vol. 1).
  - 調査対象：ホスト／プロトコル（SSH, TLSなど）を大規模測定
  - SSHのPQ鍵交換採用率0.029%
  - 採用は2023-2024年で増加傾向

- F5, ”The State of Post-Quantum Cryptography (PQC) on the Web”, Jun. 2025. , https://www.f5.com/labs/articles/the-state-of-pqc-on-the-web
  - 調査対象：世界の上位100万ウェブサイトおよび主要ブラウザ
  - 上位100万サイト中、約8.6%がPQCハイブリッドKEMをサポート
  - 銀行サイトではPQCサポート率わずか3%と、最も低いセクターの一つ
  - ChromeはPQC対応版利用率93%
  - Firefoxはトラフィックⅰ少数ながらPQC対応版利用率85%

PQCの実装商品調査

事例

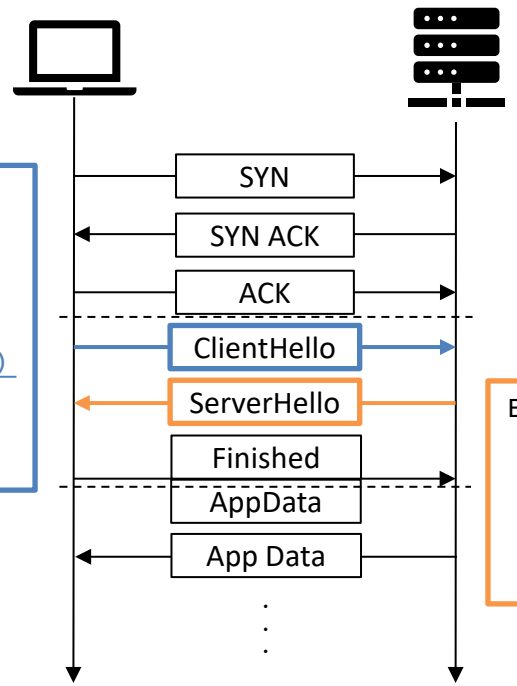
- 凸版印刷（現　凸版デジタル）とNICT：CRYSTALS-Dilithiumを導入したカードを開発
  - https://www.nict.go.jp/press/2022/10/24-1.html
- 東芝情報システム：PQCライブラリ　Quantum Safe Crypto Library
  - https://www.tjsys.co.jp/embedded/encryption/index_j.htm
- Zoom Video Communications: ZoomにPQCを導入
- Apple:iMessageにPQCを導入
- HP：ビジネス向けPCにファームウェアでPQC導入
- OQS(Open Quantum Safe)などで、共同でオープンソースライブラリを作成する動きもある

参考：TLSでPQCが使われているか判定する方法

- TLS handshakeのClientHelloとServerHelloパケットで判定可能
  - ClientHello : TLS1.3 + Supported Groups ExtensionにPQC Hybrid KEMが指定されているか
  - ServerHello: TLS1.3 + Key Share ExtensionにPQC Hybrid KEMが指定されているか
  - TLS1.3未満はPQC非対応
  - QUIC (HTTP/3)の場合はInitial or Handshakeパケットに含まれるTLS1.3ヘッダで同様に判定
- ClientHelloでPQCが指定された場合 ：PQCを提案した（クライアントが潜在的に対応）
- ServerHelloでPQCが指定された場合：PQCを選択した（両者がPQC対応）

クライアントが従来の鍵交換方式と
PQC Hybrid KEM(X25519MLKEM768)を4つ**提案**

```
Extension: supported_groups (len=10)
    Type: supported_groups (10)
    Length: 10
    Supported Groups List Length: 8
    Supported Groups (4 groups)
        Supported Group: X25519MLKEM768 (0x11ec)
        Supported Group: x25519 (0x001d)
        Supported Group: secp256r1 (0x0017)
        Supported Group: secp384r1 (0x0018)
```



"draft-ietf-tls-hybrid-design-16", 2025,
https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/16/

サーバがPQC Hybrid KEM(X25519MLKEM768)を**選択**

```
Extension: key_share (len=1124)
    Type: key_share (51)
    Length: 1124
    Key Share extension
        Key Share Entry: Group: X25519MLKEM768 (0x11ec)
            Key Exchange Length: 1120
```