

これまでとこれからのインターネットを支える技術：耐量子暗号と DNS

JPNIC 大谷 亘 <alt@nic.ad.jp>

2025/05/19 国内 IGF 活動活発化チーム 第 4 回勉強会



今日のテーマ

- 耐量子暗号 (PQC)
 - 本スライドにて
- DNS
 - 別スライドにて
 - ICANN RSSAC 作成のマテリアルを日本語化

▶▶▶ 今日の内容でわかること・わからないこと

- なるべく嘘（事実でないこと）はつかないようにしますが, 外れ値や原則から離れた例外を意図的に隠すことがあります
- 今日のキーワードをもとに, 気になったことを調べる用途でご活用いただきたい

わかること

- 各技術が何者なのかなんとなく
- **キーワード**
- 各技術がインターネットにおいてはたす **役割**
- インターネット政策を考える上でやろうとしていることが **「技術的に可能」**か**「不可能」**か

わからないこと

- 各技術の詳細な定義
- 各技術の実装
- 技術の最先端で起こっていること



PQC

耐量子暗号 (PQC: Post-Quantum Cryptography)

- 量子コンピュータの発展による既存暗号(RSA/ECC など)への脅威に耐える暗号方式
- 実装は古典コンピュータ上で動作し, **量子技術自体は使わない**
- 安全性は「既知の量子アルゴリズムで解読できない問題」に基づく（例: 格子問題, ハッシュ関数）
- 複数の方式が考案されている



従来暗号と Shor のアルゴリズム

従来の暗号技術の特徴

- 秘密鍵から暗号文を作るのはかんたん（暗号化等）
- 公開鍵を使って暗号文を平文に戻すのもかんたん（復号等）
- 暗号文から**秘密鍵を見つけるのが難しい**（解読）
- 古典コンピュータでは鍵長が大きいほど解読に多くの演算時間が必要
 - このグラフをいかに急激にできるか？ が暗号強度につながる
 - RSA: 指数グラフ
 - 楕円曲線暗号: 楕円曲線グラフ



従来暗号と Shor のアルゴリズム

Shor のアルゴリズム

- 1994 年に Peter Shor が発表
- 「量子コンピュータを使うと素因数分解を多項式時間で演算できる」
 - 素因数分解: RSA での解読操作
 - 多項式時間: **現実的な時間**
- **現状の量子コンピュータではまだ実用的に解読できない**
 - 「今後量子コンピュータが発展したら...」という不安
- PQC の概念が生まれるきっかけ

上記は非対象鍵暗号のお話だが, 対象鍵暗号についても同様 (Grover のアルゴリズム) の状況



従来暗号とその限界

種類	基盤問題	鍵長例	用途例
RSA	素因数分解	2049-4096 ビット	TLS, DNS, デジタル署名
ECC	離散対数問題	secp256r1 等	TLS, 証明課題
AES	ブロック暗号	128/256 ビット	VPN, ディスク暗号化

- いずれも鍵長を長くすれば強度を高められる
- 鍵長を長くすると通常の暗号化/復号コストも高くなる
- どこまで長くすれば「安全」？



従来暗号とその限界

- 通信の世界（の一部）: 今解読・偽造しないと意味がない
 - 署名有効期間の短縮など
- データ保存の世界: **Harvest Now, Decrypt Later**
 - 鍵長を長くする？
 - 「今」だけでなく「将来」の脅威に耐える必要がある
 - PQC



PQC の標準化

- NIST (米国) の標準 (FIPS) が話題
 - [NIST FIPS](#): 米国政府機関での情報処理標準
 - 国内では [CRYPTREC](#) がガイドライン等
- NIST 標準は PQC 以外のセキュリティ分野でも重要視
 - [NIST SP Series](#) など
- 2016 年から標準化プロセスを開始, 現在も進行中
 - 安全性・性能・実装容易性・耐量子性・多様性

標準化された PQC アルゴリズム

- 鍵共有・暗号化
 - ML-KEM
 - [FIPS 203](#)
 - HQC
 - バックアップ候補として先月選定
- デジタル署名
 - ML-DSA
 - [FIPS 204](#)
 - SLH-DSA
 - [FIPS 205](#)
 - FN-DSA
 - 来年ドラフト標準公開？



各分野における動き

- 金融
 - 認証・鍵交換・暗号化等の基盤として従来暗号を使用
 - 政府・金融機関で PQC への対応計画・実験
- 行政
 - 大量の個人情報・外交機密等のデータを暗号化して保存
 - 米国政府では NIST で標準化が完了次第移行するか？
 - ITU-T, OECD, ISO 等でもガイドライン策定の動き
- 医療
 - 電カルデータなど・インフラ遮断は生死に直結
 - 数十年単位の長期的な安全性が必要



各分野における動き

- 重要インフラ
 - 電力・ガス・水道・交通・通信など
 - 各国事業者で実験が進行
- インターネットインフラ
 - BGP (RPKI), DNS (DNSSEC), Web TLS
 - IETF にて研究・実装共に WG が活動
 - 各基盤で PQC の利用が実験的に開始



アジリティとハイブリッド設計

- PQC 対応の本質は「**従来プロトコルを延命するだけでは耐えられない**」とわかったこと
- 現状の PQC アルゴリズムも **危殆化する前提** を今のうちにしておく
 - あとからプロトコルを差し替えても運用できるように（アジリティ）
 - 複数のプロトコルを使用できるように（ハイブリッド）

技術実装・政策要件の両面で前提とする必要がある



DNS のお話

- 別スライドにて
- ICANN RSSAC (ルートサーバシステム諮問委員会) による解説「RSS Messaging Project」
 - RSSAC Chair である Jeff Osborn 氏より許諾を得て日本語化
 - [RIPE88](#) でのドラフト
 - [ICANN89](#) での版

これまでとこれからのインターネットを支える技術：耐量子暗号と DNS

JPNIC 大谷 亘 <alt@nic.ad.jp>

2025/05/19 国内 IGF 活動活発化チーム 第 4 回勉強会