PQC時代に向けて

IETF113報告会

2022年5月24日

米谷嘉朗 <yoshiro.yoneya@jprs.co.jp>

本日の目的

- IETF/IRTFの暗号・PKI関連WGやICANNのDNS関連WorkshopなどでPQC(Post Quantum Cryptography; 耐量子暗号)の話題が増えてきている
- インターネットのプロトコル標準化に20年以上携わってきた経験から、プロトコルの開発、SW/HW実装、システム/サービス運用へのPQCの影響を考察する
  - より多くの人の関心を得ることで、PQC時代に向けた関係者による取り組みの出発点としたい
  - 今後も折に触れ議論したいので、参加者のみなさんに「自分にもかかわるかもしれない問題」としてPQC視点を持ち帰ってもらいたい

PQCについて

- 量子コンピュータが普及して計算能力が飛躍的に向上すると、現在の暗号アルゴリズムは簡単に解読されるようになる見込み
- PQCは耐量子暗号とも呼ばれており、量子コンピュータでも容易には解読できない(耐性のある)暗号の総称である
  - 量子暗号とは別物
  - NISTによるPQCアルゴリズムの選定が現在進行中
    https://csrc.nist.gov/Projects/post-quantum-cryptography

注意：暗号の専門家ではないのでPQCそのものの解説はしません

なぜいまPQCに関心を寄せるのか

- 量子コンピュータが普及するまでにはまだ相応の時間は見込まれているが、悠長なことは言っていられないので、量子コンピュータの計算能力にも耐性がある暗号アルゴリズムへ移行しておこう
  - NISTのPQCアルゴリズム選定は間もなく終了の見込み
  - 米国政府は2022年5月にPQCへの移行方針を表明
- 過去の経験から暗号アルゴリズムの移行は長い時間がかかること、暗号をつかう様々な製品やサービスに影響することがわかっているので、インターネットのインフラ技術の「移行問題」と認識して取り組もう

PQCがおよぼす影響の考察

- 以下は網羅的ではありません
- 以下は相互に関連しており独立ではありません

1. プロトコルへの影響
2. リソース(資源)への影響
3. オペレーション(運用)への影響

プロトコルへの影響

- PKIのフォーマットの変更
  - 既存暗号からPQCへの移行期には、既存暗号アルゴリズムとPQCの2つを1つの証明書に入れる方式が検討されている
- IPsec
- QUIC
- TLS
  - Web、Mail、…
- DNSSEC
- MLS
- 送信ドメイン認証
  - DKIM、DMARC、BIMI、…
- 認証/認可
  - 証明書を使うもの
- …

リソース(資源)への影響

- 鍵長の増加
- 署名サイズの増加
- 暗号化/復号/署名計算時間の増加
- …

オペレーション(運用)への影響

- 下位互換性の確保方法
  - サーバ証明書
  - クライアント証明書
- ペイロードサイズの増加によるフラグメントの発生
- 計算時間増加の悪用防止
- 暗号アルゴリズムロールオーバーの実施
- 信頼できるPQC製品の選択
- …

PQCに備える(1/3)

- 自分がかかわっていることに対するPQCの影響を把握しよう
  - IETFに参加するプロトコル設計者として
  - IETFに参加するサービス運用者として
  - IETFで開発されたプロトコルを実装するソフトウェア開発者として
  - …

PQCに備える(2/3)

- 過去の経験に学んでスムーズな移行を考えよう
  (これまでにも大規模なプロトコル移行は行ってきた)
  - IPv4 to IPv6
  - HTTP/1 to HTTP/2 to HTTP/3
  - TCP/UDP to QUIC
  - Do53 to DoE
  - …

PQCに備える(3/3)

- ブレークスルーのタイミングを知ろう
  - PQCの標準化・実装の進捗状況を適度な間隔で把握しておこう
  - 実装(製品)が手に入るようになったら遊んでみよう
  - …

議論

1. 「PQCがおよぼす影響の考察」に関して、
   抜け漏れや間違いは何？

2. 「PQCに備える」に関して、
   抜け漏れや間違いは何？