Internet Week 2023
C8 PKIのこのごろ

ライトニングトーク
PQC関連

11/21/2023

大久保　智史
DigiCert, Inc.

WHOAMI

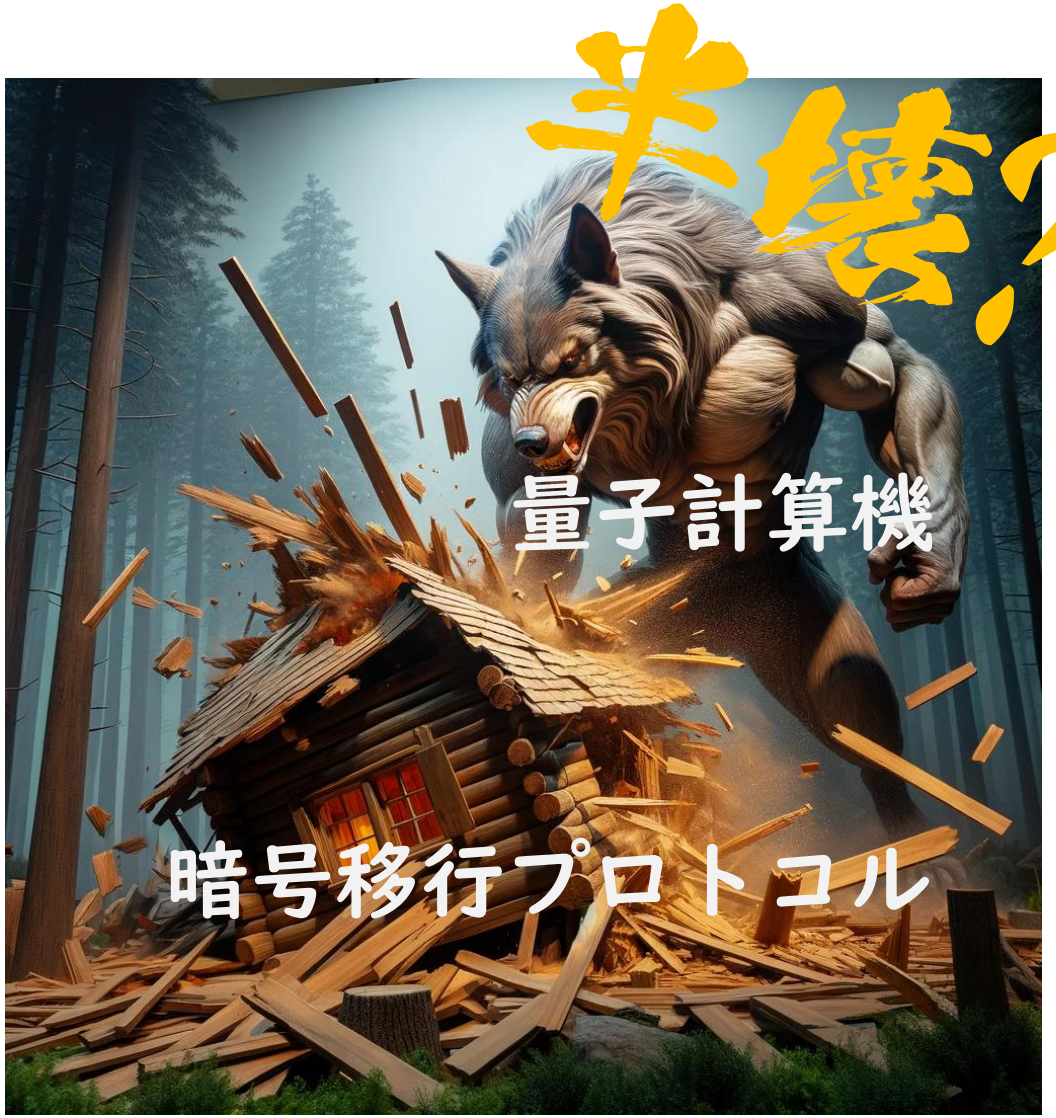
- 名前
  - 大久保　智史（おおくぼ　ともふみ）
- 所属
  - DigiCert, Inc.
  - Director, Data Analytics/Compliance
- 何者か
  - 国内外で珍しいオフライン暗号鍵管理の数少ない専門家
  - ルートDNSSECの暗号鍵管理の設計を行った
  - 現在IETFでPQCの移行周りの標準化活動を行っている

量子コンピュータ等の脅威（イメージ）

注）菅野さんのお話にあったように暗号は怖くありません

従来の暗号アルゴリズムの運命（イメージ）

PQC移行プロトコル（イメージ）



PQC完全移行完了（イメージ）

木の家は果たして無駄であったのか？

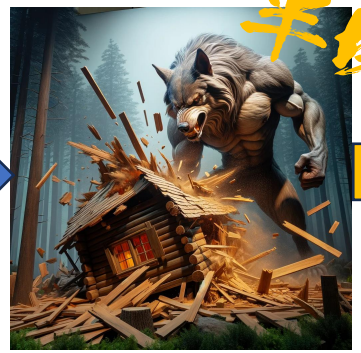
- 暗号アルゴリズムの移行には…
  - 技術、プロトコルの策定（年単位）
  - サーバ、クライアントソフトの実装（年単位）
  - プロダクション環境への導入（年単位）
- 移行コストを下げる（新旧アルゴリズムが使える）
- 社会的インパクトを和らげる
- PKIは想像以上に種々様々なところで複雑に使われている
  - 暗号使途の複雑さは加速の一途を辿る
  - インターネット上に留まらず、実生活に影響を及ぼす
- 新アルゴリズムへの移行が完了すると移行プロトコルは一旦役目を終える（むしろ、終えなければならない）
- 移行プロトコルの仕組みは別の移行イベントがあった時に再利用できる（鍵長やパラメータ、アルゴリズム）

タイムラインで見てみる最悪のシナリオ

菜 従来の暗号アルゴリズム

木 PQC移行プロトコル

引越完了！



石 PQC暗号アルゴリズム

引越完了！

IETFで登場しているPQC移行プロトコル

- Composite型(Getting adopted at IETF LAMPS WG! 🎉)
  - Composite Signatures For Use In Internet PKI
  - Mike Ounsworth , John Gray , Massimiliano Pala and Jan Klaußner
    - https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/
- Chameleon型(Now available in Bouncy Castle ! 🎉)
  - Corey Bonnell , John Gray , D. Hook , Tomofumi Okubo and Mike Ounsworth
  - A Mechanism for Encoding Differences in Paired Certificates
    - https://datatracker.ietf.org/doc/draft-bonnell-lamps-chameleon-certs/
- Discovery型(NEW!)
  - A Mechanism for X.509 Certificate Discovery
  - Tomofumi Okubo , Corey Bonnell and John Gray
    - https://datatracker.ietf.org/doc/draft-lamps-okubo-certdiscovery/

ご清聴ありがとうございました！

- ご質問、ご意見はこちらまでお気軽に！
  - tomofumi.okubo@digicert.com
- PQC移行プロトコルの推進をする同志、ユースケース求む！
  - ＩＥＴＦはリモートで参加で、しかも無料で参加できます。実際、大半の作業や議論はリモートが前提です。ご興味のある方はぜひお問い合わせください。