Internet Week 2024

耐量子計算機暗号は
インターネットにどのような影響をもたらすか

2024年11月20日

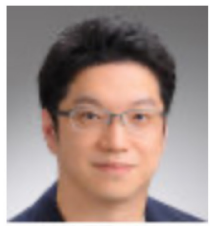
NPO JNSA フェロー　松本　泰

耐量子計算機暗号はインターネットにどのような影響をもたらすか

- 今日のインターネットのセキュリティは、暗号技術により支えられていると言っても過言ではない状況にあります。
- しかしながら、量子コンピュータの登場を見据えると、既存の公開鍵暗号から耐量子計算機暗号（PQC）への暗号移行を検討することが必要になりつつあります。
- インターネットがデジタル社会の基盤として機能していることから、この暗号移行はデジタル社会全体に対して極めて重大な影響を及ぼすものと考えられます。
- 本セッションでは、過去の暗号アルゴリズム移行についての振り返りや、現在のPQCの状況、IETFなどでのPQCに対応する標準化の動向などから、暗号移行がインターネットに対してどのような影響を与えるのか、そしてどのような課題が生じうるのかなどを概説し、今後の暗号移行のあり方を議論します。


松本 泰


伊藤 忠彦


菅野 哲

- **松本 泰(JNSA (日本ネットワークセキュリティ協会) フェロー)**
- **伊藤 忠彦(セコム株式会社 IS研究所 主任研究員)**
- **菅野 哲(GMOサイバーセキュリティ byイエラエ株式会社 常務取締役 CTO of development)**

IETFセキュリティエリアで活躍中
IETF 121 ダブリンにも参加

本日のお品書き？

- 松本　　15分
  - オーバービュー
  - 暗号の2010年問題の振り返りから見たPQC移行
- 伊藤さん　　30分
  - そもそもの量子計算機、PQCなど
  - 耐量子計算機暗号への移行へ向けた課題と社会実装への論点整理
- 菅野さん　　30分
  - 標準化動向　　NIST, IETF などの標準化動向
  - 実装上の課題
- パネルディスカション、Q&A　　45分
  - IETFなどでの標準化の状況と課題
  - インターネット機器などベンダー
  - インターネットの運用
  - 総論として耐量子計算機暗号はインターネットにどのような影響をもたらすか

暗号の2010年問題の振り返りから見たPQC移行

耐量子計算機暗号（PQC）への移行の現在のステータス

- 1994年
  - Shor のアルゴリズム　　公開鍵暗号を解読する量子アルゴリズム
- 2011年
  - 「世界初の商用量子計算機」を謳ったD-Wave Oneの発表
  - →　Shor のアルゴリズムで公開鍵暗号を解読できるようになるのでは？？
  - →　量子計算機が実用化したら（既存の）公開鍵暗号は解読される？？
  - →　現在は、 CRQC(Cryptographically Relevant Quantum Computer.暗号解読可能量子計算機)が実現したら。。
- 2016年
  - NISTにおけるPQC標準化の開始
- 2024年
  - NISTのPQC標準化文書発行（FIPS 203, 204, 205）→ 非常に大きなマイルストーン
  - →PQC自体の標準化からPQCを使ったプロトコル等の標準化へ（IETFでの標準化が極めて重要）
    - →　なので本日は、伊藤さん、菅野さん
- 2024-20??
  - PQC移行への様々な活動→　耐量子計算機暗号はインターネットにどのような影響をもたらすか
- 20??年
  - Q-day　　CRQC(Cryptographically Relevant Quantum Computer)の実現

8年間

H10: 次世代暗号アルゴリズムへの移行 ～暗号の2010年問題にどう対応すべきか～

H10: 次世代暗号アルゴリズムへの移行 ～暗号の2010年問題にどう対応すべきか～

日時	2008年11月27日 9:30 - 12:30
参加料	＜半日セッション券 事前料金 ¥6,000 当日料金 ¥8,000＞

現在、 数十年に一度とも言われる暗号アルゴリズムの移行が全世界的に進行中ですが、 暗号アルゴリズムの移行においては、 インターネットの各レイヤーを支える多くの方の必要にも関わらず、 移行の必要性さえも十分に周知されているとは言えないのが現状です。

本セッションでは、 暗号アルゴリズムの移行が必要とされる技術的背景と、 政府および民間における進捗の現状を解説し、 スムーズな移行に向けて今後日本においてどのよう望まれるかについてディスカッションします。

内容

9:30-9:40 (10分)	1)全体説明 講演者：松本 泰/セコム株式会社 IS研究所  松本 泰
9:40-10:10 (30分)	2)暗号アルゴリズムの安全性のお話 講演者：神田 雅透/ＮＴＴ情報流通プラットフォーム研究所  神田 雅透
10:10-10:50 (40分)	3)政府機関における安全な暗号利用の促進 講演者：繁富 利恵/内閣官房情報セキュリティセンター/産業技術総合研究所情報セキュリティ研究センター  繁富 利恵
11:00-11:20 (20分)	4)次世代暗号アルゴリズムへの移行～暗号の2010年問題にどう対応すべきか～ 講演者：松本 泰/セコム株式会社 IS研究所  松本 泰
11:20-11:40 (20分)	5)SSLサーバの現状調査結果について 講演者：神田 雅透/ＮＴＴ情報流通プラットフォーム研究所  神田 雅透
11:40-12:30 (50分)	6)パネルディスカッション：「次世代暗号への移行に向けて：我々はなにをすべきか？」 モデレーター：松本 泰/セコム株式会社 IS研究所 パネリスト： 神田 雅透/ＮＴＴ情報流通プラットフォーム研究所 繁富 利恵/内閣官房情報セキュリティセンター/産業技術総合研究所情報セキュリティ研究センター 高木 浩光/産業技術総合研究所  松本 泰  神田 雅透  繁富 利恵  高木 浩光

出典： https://www.nic.ad.jp/iw2008/popup/40.html

JNSA

暗号アルゴリズムの移行の議論

セコムIS研究所 Intelligent Systems Laboratory

暗号アルゴリズムの歴史

古典暗号 → 現代暗号 → 評価の確立 → 世代交代

IETF, ISO, ITU Etc…

暗号技術を利用した様々な標準化

標準化へのインパクト

電子署名法、Webサーバ証明書の発行、etc….

暗号技術を利用した様々な実装の展開基盤の確立

実装の展開基盤へのインパクト

暗号は、ITソリューションの「米」じゃなくて「小麦」状態??
ありとあらゆるITソリューションに組み込まれている

出典
https://www.nic.ad.jp/ja/materials/iw/2008/proceedings/H10/IW2008-H10-03.pdf

PQCへの移行

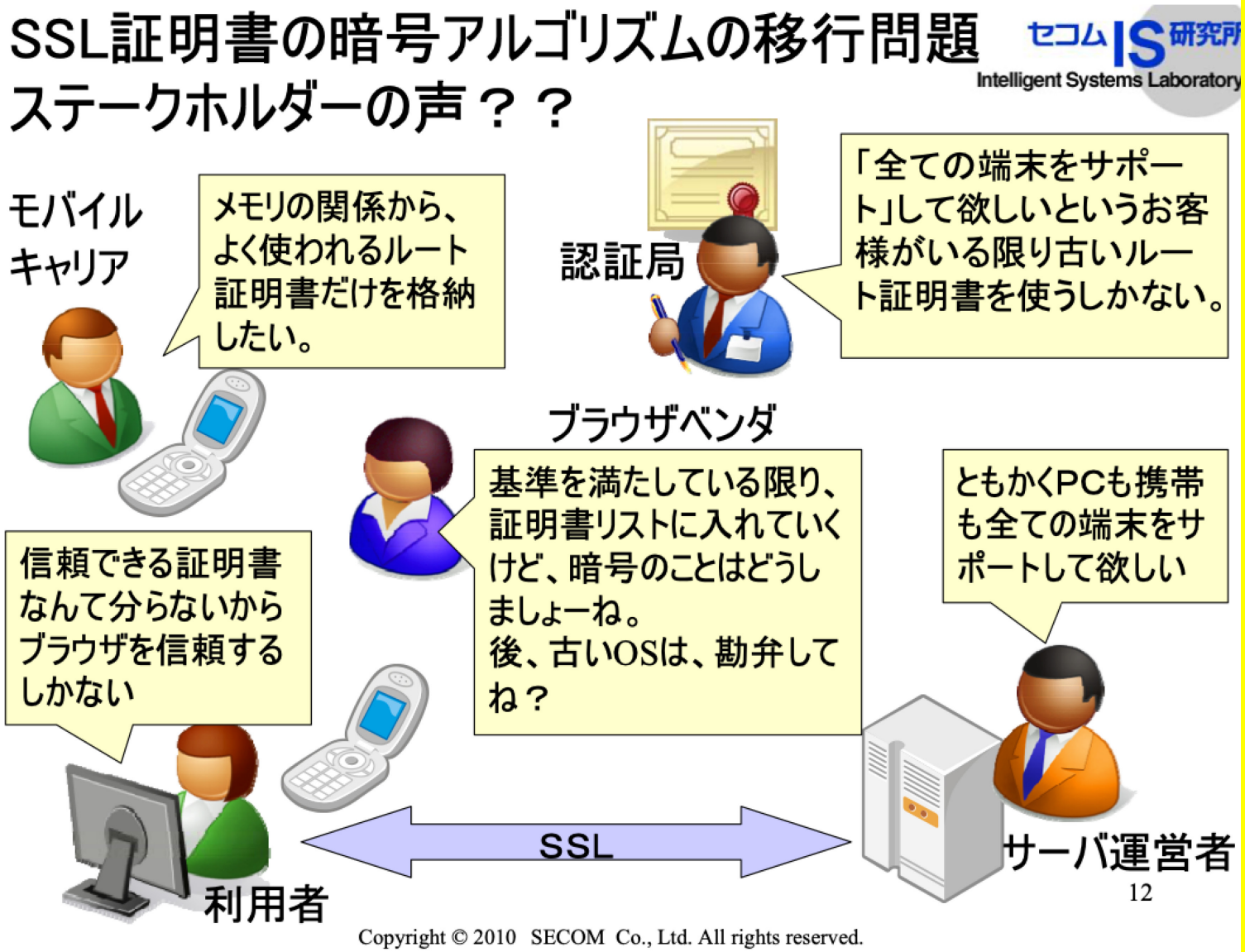
PQCという大幅な世代交代

PQCを利用した様々な標準化

PQCを利用した様々な実装の展開基盤の確立

2008年当時よりも、はるかに深くデジタル社会に組み込まれている公開鍵暗号

暗号の2010年問題における大きな課題



出典：社会基盤としてのPKI / PKIの10年　2010年6月29日
https://www.jnsa.org/seminar/pki-day/2010/data/5_a_matsumoto.pdf

暗号の2010年問題において、WebPKIでは、レガシーな信頼点（RSA1024）が組み込まれた携帯（ガラケー）をサポートするために、移行は、なかなか進まなかった。
マルチステークホルダー環境の移行は、このような状況を作り出すデットロックとなる可能性が強い。

PQC移行おいても同様で、大きな課題となる事例は、多くのステークホルダーが関与しているシステムで使われている場合だと考えられる。（そもそも、公開鍵暗号は、多くのステークホルダー間の信頼関係の構築に大きな役割を果たす。）
インタネットにおける典型例は、WebPKI、DNSSEC、RPKIなど

移行には、何らかの強制力が必要になる場合もある。

日本における耐量子計算機暗号への移行の議論

令和６年７月４日
金融庁

「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」の開催について

１．趣旨

量子コンピュータが実用化されると、現在広く利用されている公開鍵暗号の安全性が損なわれることが指摘されており、耐量子計算機暗号（Post-Quantum Cryptography、PQC）への移行に向けた検討が国内外で始まっています。金融庁では、金融分野における課題や留意事項について、幅広い関係者と議論を行ってきました。

今般、上記の検討の一環として、PQCへの移行を検討する際の推奨事項、課題及び留意事項について関係者と更に検討するため、本検討会を開催します。

出典：
https://www.fsa.go.jp/news/r6/singi/20240704.html

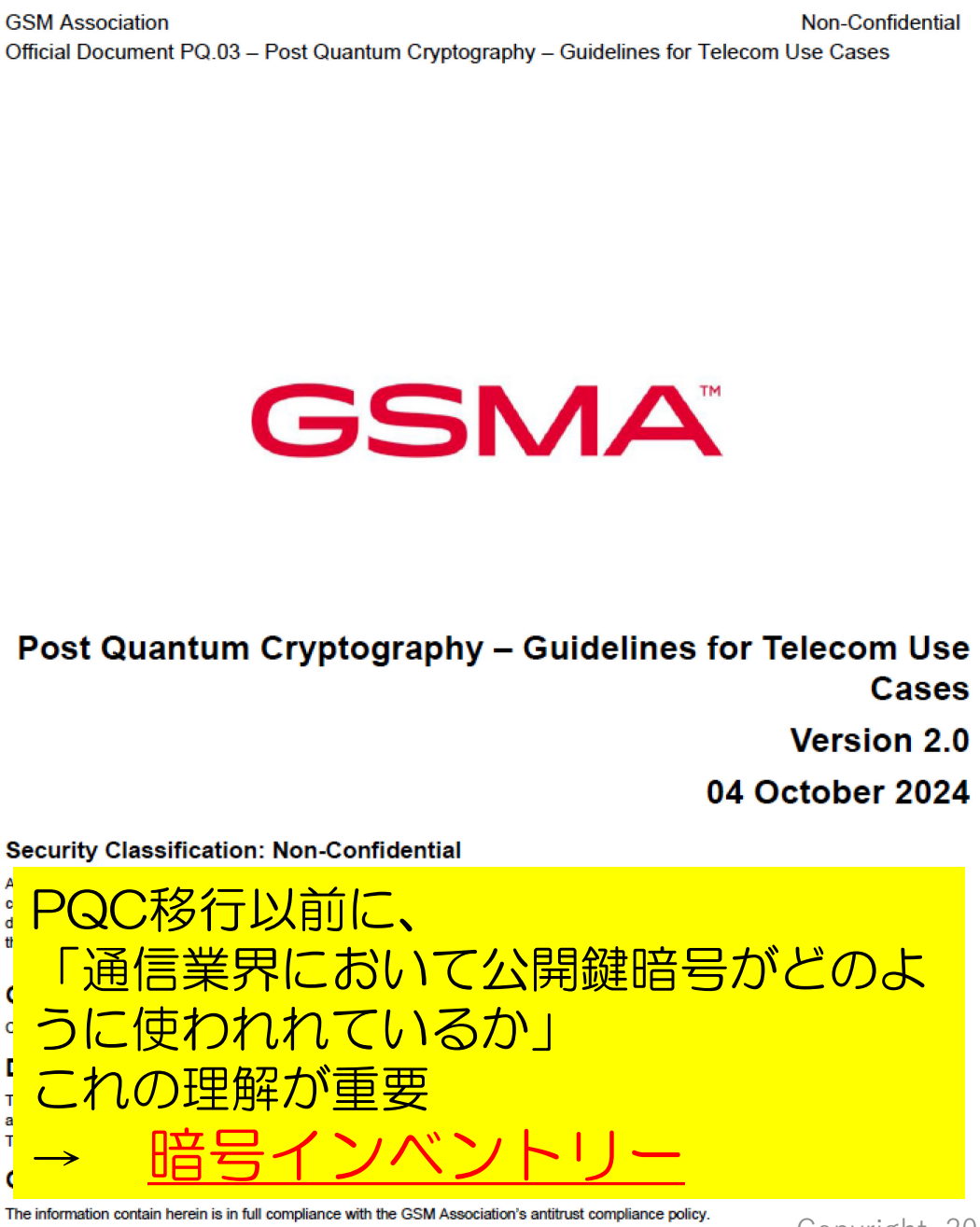
「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」

メンバー等名簿

（敬称略、五十音順）

座長	寺井　理	株式会社みずほフィナンシャルグループ グループ執行役員・情報セキュリティ担当（グループ CISO） 金融 ISAC FinTech セキュリティワーキンググループ座長
メンバー	安藤　彰英	株式会社名古屋銀行　執行役員　業務部長
	岩崎　三郎	株式会社静岡銀行　リスク統括部長
	宇根　正志	日本銀行　金融研究所　参事役
	大城　徹	株式会社しんきん情報システムセンター　上席執行役員
	菅野　洋平	労働金庫連合会　情報システム部　副部長
	白井　大輔	株式会社三井住友フィナンシャルグループ グループ CISO　サイバーセキュリティ統括部長
	高瀬　徹	農林中央金庫　IT 統括部部長（システムリスク管理担当）
	松本　泰	特定非営利活動法人日本ネットワークセキュリティ協会 フェロー
	峰　匡親	株式会社三菱 UFJ フィナンシャル・グループ グループ CISO　サイバーセキュリティ推進部　部長
	村山　朋彦	信組情報サービス株式会社　常勤取締役
オブザーバー	一般社団法人金融 ISAC、CRYPTREC 事務局、公益財団法人金融情報システムセンター、日本銀行　金融機構局、内閣サイバーセキュリティセンター	
事務局	金融庁	

通信業界におけるユースケース毎の考察の事例



ネットワーク事業者のユースケース	特定されたアクション	顧客に影響を与えるユースケース	特定されたアクション
基地局とセキュリティ・ゲートウェイ間のインターフェイスの保護	Yes	仮想プライベート・ネットワーク・サービス	Yes
仮想化されたネットワーク機能	Yes	SD-WANサービス	Yes
クラウド・インフラ	TBD	IoTスマートメーター	Yes
SIM（物理的）	TBD	IoT自動車	Yes
eSIMプロビジョニング（リモート）	Yes	合法的インターセプト	TBD
デバイスとファームウェアのアップグレード	Yes	顧客データのプライバシー	Yes
加入者公開識別子の隠蔽	Yes		
4Gおよび5Gにおける認証とトランスポート・セキュリティ	Yes		

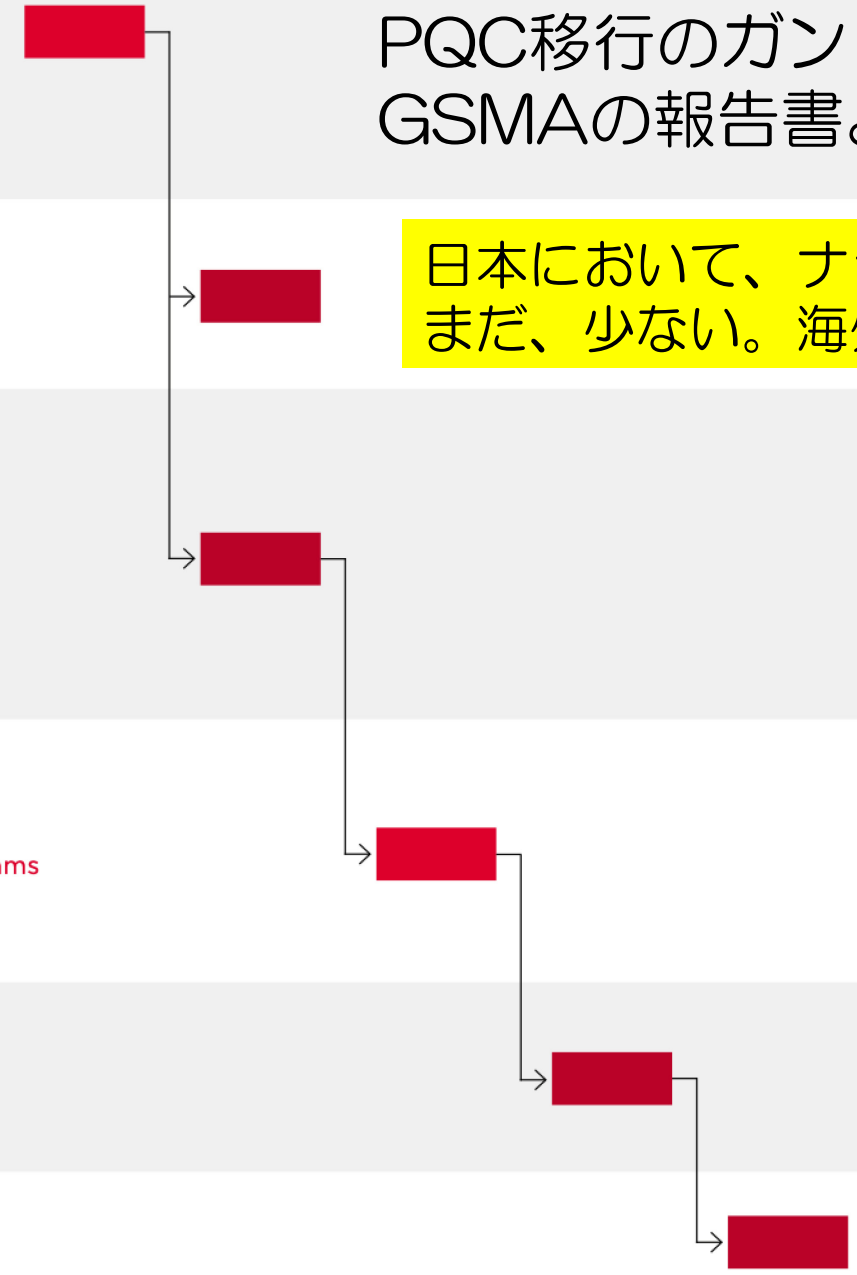
PQC移行以前に、
「通信業界において公開鍵暗号がどのように使われれているか」
これの理解が重要
→　暗号インベントリー

GSMA のPQTN （Post-Quantum Telco Network ）タスクフォースは、2年前から活動を行っている。

出典： https://www.gsma.com/newsroom/gsma_resources/pq-03-post-quantum-cryptography-guidelines-for-telecom-use-cases/

VPNにおける PQC移行のガントチャート GSMAの報告書より

Standards	PQC Standards	— NIST PQC Standards — IETF IPSec/TLS Standards — PKI-related Standards — Key exchange/hybrid Standards — MACsec/MKA
National Guidelines	PQC guidance	— Migration recommendations — PQC regulations
Vendors	Update products for PQC	— Update IPSec VPNs — Update TLS — Update crypto libraries (digital signature algorithms) — Update PKI — Update MACsec/MKA
Operators	Deploy PQC products	— Deploy updated IPSec/TLS — Deploy updated signature algorithms — Deploy updated MACsec/MKA — Deploy updated PKI
PoC	Integration and End-to-End	— Integration testing — End-to-end testing
Migration	Migrate	— Migrate to PQC



日本において、ナショナルガイドライン作成の動きは、まだ、少ない。海外では多くの国が、策定を始めている。

出典
https://www.gsma.com/newsroom/gsma_resources/pq-03-post-quantum-cryptography-guidelines-for-telecom-use-cases/

まとめ

- NISTによるPQC標準化は、非常に大きなマイルストーンであり、PQC対応のフェーズが変わった
  - PQCのアルゴリズムの標準化から、標準化されたPQCを利用したプロトコルなどの標準化のフェーズへ
  - この標準化されたPQCを利用したプロトコルなどの標準化では、IETFが大きな役割を果たしている。
- PQC移行の何が課題となるのか？
  - 一つには、暗号の2010年問題の振り返りが参考になる
    - 実際に、移行に何年かかったのか？
  - しかし、PQC移行は、はるかに複雑
    - PQCという大幅に世代交代した暗号アルゴリズム
    - 2010年問題当時よりも、はるかに深くデジタル社会に組み込まれている公開鍵暗号
    - 更に加速する公開鍵暗号の利用（ゼロトラストなど）
- 耐量子計算機暗号はインターネットにどのような影響をもたらすか
  - 大きな影響をもたらすことは間違いない。
  - しかし、どのように影響をもたらすのか？？　→　パネルディスカッションへ

パネルディスカション

耐量子計算機暗号は
インターネットにどのような影響をもたらすか

パネルディスカション
耐量子計算機暗号はインターネットにどのような影響をもたらすか
TLS、IPsec、DNSsec、X.509などを題材に

- （１）　IETFなどでの標準化の状況と課題
- （２）　インターネット機器などへの実装の課題
- （３）　インターネットの運用

- 総論として耐量子計算機暗号はインターネットにどのような影響をもたらすか

VPNにおけるPQC移行のガントチャート　GSMAの報告書より

Standards	PQC Standards	— NIST PQC Standards — IETF IPSec/TLS Standards — PKI-related Standards — Key exchange/hybrid Standards — MACsec/MKA
National Guidelines	PQC guidance	— Migration recommendations — PQC regulations
Vendors	Update products for PQC	— Update IPSec VPNs — Update TLS — Update crypto libraries (digital signature algorithms) — Update PKI — Update MACsec/MKA
Operators	Deploy PQC products	— Deploy updated IPSec/TLS — Deploy updated signature algorithms — Deploy updated MACsec/MKA — Deploy updated PKI
PoC	Integration and End-to-End	— Integration testing — End-to-end testing
Migration	Migrate	— Migrate to PQC

（１）　IETFなどでの標準化の状況と課題

（２）　インターネット機器など

（３）インターネットの運用

出典
https://www.gsma.com/newsroom/gsma_resources/pq-03-post-quantum-cryptography-guidelines-for-telecom-use-cases/

MISC

DNSsecに関するパネルディスカションの事例

Submission for the 3rd NIST PQC Standardization Conference
Panel- PQC Considerations for DNSSEC

Submission Contacts

Primary Submitter: Andrew Fregly, Verisign, afregly@verisign.com

- Moderator: Haya Shulman, Fraunhofer Project Center for Cybersecurity at the Hebrew University of Jerusalem, has confirmed her participation

Panelists – All proposed panelists have confirmed their participation:

- Jim Goodman, Crypto4a Technologies Inc.
- Russ Housley, Vigil Security LLC
- Burt Kaliski, Verisign
- Victoria Risk, Internet Systems Consortium
- Douglas Stebila, University of Waterloo
- Roland van Rijswijk-Deij, University of Twente and NLnet Labs

https://csrc.nist.gov/CSRC/media/Events/third-pqc-standardization-conference/documents/accepted-papers/panel-pqc-considerations-dnssec-pqc2021.pdf

2021年6月7日に開催された第3回NIST PQC標準化会議
https://csrc.nist.gov/Events/2021/third-pqc-standardization-conference

におけるDNSsecに関するパネルディスカション

このパネルの目的は、DNSおよびDNSSEC関連の標準を定義し実装する関係者と協調しながら、PQCデジタル署名アルゴリズムの選択に関するDNSSEC関連の検討事項をさらに掘り下げることです。
対象となる関係者には、標準化機関、研究者、DNSサービスプロバイダー、DNSおよび暗号技術プロバイダーが含まれます。