JANOG58, Matsuyama, Japan

ネットワークエンジニアが読むべき PQC移行に関するガイドラインの紹介

Internet Initiative Japan

須賀祐治

2026-07-17

Ongoing Innovation

Disclaimer

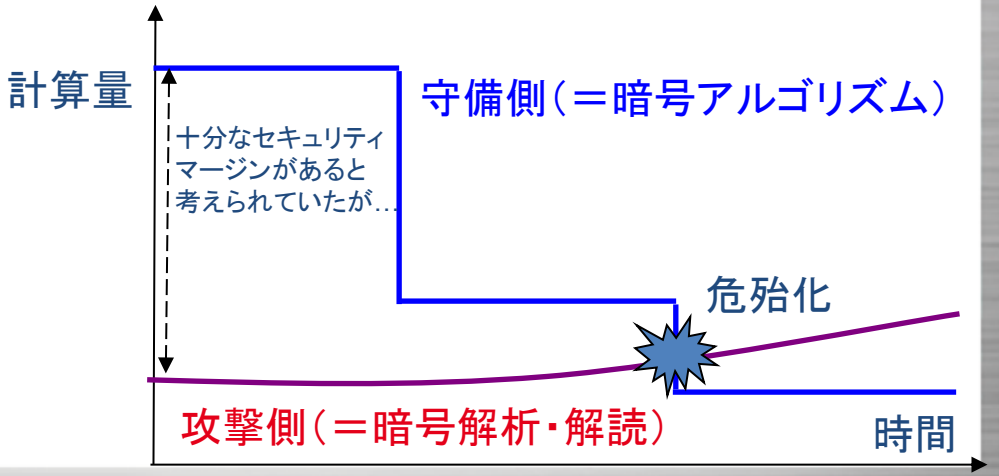
- **The views expressed in this talk are those of the author and do not necessarily reflect**

参考情報

- 暗号技術検討会2025年度報告書
  CRYPTREC RP-1000-2025
  - https://www.cryptrec.go.jp/report/cryptrec-rp-1000-2025.pdf
- 電子政府における調達のために参照すべき暗号のリスト
  CRYPTREC LS-0001-2022R2
  - https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022r2.pdf
- CRYPTRECとは
  - https://www.cryptrec.go.jp/about.html
- CRYPTREC暗号リスト
  - https://www.cryptrec.go.jp/list.html
- 暗号技術ガイドライン一覧
  - https://www.cryptrec.go.jp/tech_guidelines.html

暗号技術の必然：暗号危殆化

- **時間とともに緩やかに進行＝ 経年劣化**
  - 計算機能力の向上：CPU/GPU性能の向上
  - 計算機モデルの変化：量子計算機の実現
- **急に進展することがあり得る**
  - 暗号解析手法の進歩
    - nビット安全性のnが急激に低下



CRYPTRECとは何か

- 日本の暗号技術評価プロジェクト
  - Cryptography Research and Evaluation Committees
  - [暗号技術検討会報告書，2.2節，p.4]
- 電子政府推奨暗号等の安全性を評価・監視
- 暗号技術の普及促進も目的
- 2003年に電子政府推奨暗号リストを策定
  - [暗号技術検討会報告書，2.1節，p.4]

耐量子計算機暗号（PQC）

PQC: Post-Quantum Cryptography

≠ 量子暗号

- **古典コンピュータでの暗号処理を想定**
  - 耐[量子コンピュータ]暗号
  - 素因数分解（RSA）や離散対数問題（ECDSA）が近いうちに解かれるかも・・・
- **米国NISTでのコンペティション，FIPS化**

  KEM/DEM（CRYSTALS-KYBER）
  デジタル署名（CRYSTALS-Dilithium, FALCON, SPHINCS+）
- **暗号Agilityが大切（滑らかな移行）**

ごく最近のネタ1: ANSSI

- フランスはPQC「非対応」のセキュリティ製品認証を2027年から停止へ

ごく最近のネタ2: G7

G7: A look back at the plenary meeting of the working group on cybersecurity

Publié le Monday 8 June 2026

As part of France's G7 presidency, ANSSI hosted the plenary meeting of the **G7 Working Group on Cybersecurity** in Paris on 27 May 2026. The national cybersecurity agencies of the member states reaffirmed their commitment to continuing and strengthening coordination between them in the face of rapidly evolving cyber threats and emerging technologies, in order to uphold an open, stable and secure cyberspace.

They also welcomed the publication of two deliverables :

- **Minimum Elements – SBOM for AI**, negotiated by the Italian ACN and the German BSI under the Canadian (2025) and French (2026) presidencies. This document provides public and private sector stakeholders with concrete guidelines on what can reasonably be expected from a Software Bill of Materials (SBOM) for AI, as well as ways to enhance transparency and cybersecurity throughout the AI supply chain.
- **Statement on PQC Migration** negotiated by Canada under its presidency, this document represents the first deliverable published by the group on post-quantum cryptography (PQC). It offers practical guidance to technical leaders in medium and large enterprises to prepare for the transition to PQC.

The work of the G7 Working Group on Cybersecurity will continue until the end of the French presidency.

G7 Cybersecurity Working Group Statement on preparing for a post-quantum cryptography migration

This document is jointly published by:

- Canada's Communications Security Establishment (CSE)
- Germany's Federal Office for Information Security (BSI)
- Italy's National Cybersecurity Agency (ACN)
- France's National Cybersecurity Agency (ANSSI)
- The US Cybersecurity and Infrastructure Security Agency (CISA)
- UK's National Cyber Security Centre (NCSC)
- Japan's National Cybersecurity Office (NCO)

in collaboration with the EU Commission.

Preparing for Quantum Technologies: Key Considerations for Financial Sector Participants

Report prepared by the G7 Central Bank Quantum Technologies Working Group co-chaired by the Banque de France and the Bank of Canada

May 2026

この資料の位置づけ（Foreword）

- Preparing for Quantum Technologies: Key Considerations for Financial Sector Participants
- G7 Central Bank Quantum Technologies Working Group
- 共同議長: Banque de France and Bank of Canada
- May 2026

今後も P*C 対応は終わらない

P*C		概要
PAC	Post-AI Cryptography	AI／自動探索・自動証明・最適化で鍵候補のランキングや差分・統計攻撃を恒常加速する.
PBC	Post-Bio Cryptography	粘菌・細胞集合・in-vitro 計算など生物計算で組合せ探索の枝刈り・初期解生成を物理並列で行う.
PQC	Post-Quantum Cryptography	Shor／Grover等により既存公開鍵や低強度対称鍵の安全余裕を削る.
PLC	Post-Learning-assisted Cryptography	機械学習でSCA特徴抽出・鍵推定の順位付け・プロトコル空間探索を自動化する.
PHC	Post-Hardware Cryptography	電磁・消費電力・故障注入・μアーキ欠陥を突いた鍵漏えいを量的に容易化する（Side-Channel攻撃）
PWC	Post-Wetware Cryptography	人間系（認知・運用）を最適化して鍵・秘密を奪取する. 純粋な数理破りではないが実効性は高い.
PPC	Post-Physical Cryptography	実装そのものへの物理攻撃（TEMPEST／環境注入／実機奪取）で理論安全を迂回する.

CRYPTRECとしてのPQCの解説

- PQC（Post-Quantum Cryptography）
  - 日本語では耐量子計算機暗号
  - ※「耐量子暗号」は誤用（委員長との対話において確認）
  - 量子計算機に耐性を持つ暗号技術
- PQCリスト：CRQCへの耐性を有することが確認された暗号技術のリスト
  - CRQC(Cryptographically Relevant Quantum Computer)
    ＝ 現行暗号を解読可能な水準の量子計算機のこと

CRYPTRECの体制

- 事務局はデジタル庁，総務省，経産省
  - 暗号技術検討会が全体を統括
  - 暗号技術評価委員会が安全性・実装性能を評価
  - 暗号技術活用委員会が利用・運用面を検討
- 2026年度はPQCリスト検討TFを設置予定

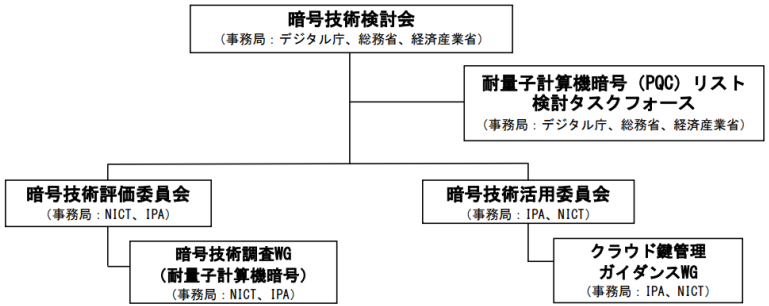


図4-1 CRYPTREC体制図（2026年度）（予定）

CRYPTREC暗号リストの更新

- CRYPTREC暗号リストを2026年3月30日に更新
  - 文書番号はCRYPTREC LS-0001-2022R2
- 表2「耐量子計算機暗号（PQC）リスト」を新設
  - 従来の表を表1「現行暗号リスト」と整理

PQCリスト新設の意図

- 「電子政府推奨暗号リスト」という文言の定着
- 既存関連文書への影響の抑制
- 従来の3リスト構成を長期的に維持しやすい整理
- CRQC耐性を持つ暗号技術の明示
- 利用者が選択可能な暗号を判断しやすくする意図
  - [暗号技術検討会報告書，2.4.2節，p.7]

PQCリスト

- 鍵共有：ML-KEM（ML-KEM-768, -1024）
- 署名は現時点では掲載なし
- 共通鍵暗号・ハッシュ関数も記載
  - AES-192，AES-256
  - SHA-384，SHA-512，SHA3-384，SHA3-512
- 192ビットセキュリティ以上のものだけをチョイス(NIST Categoryも見て欲しい)

2026年度の評価対象

- PQCリスト検討TFを設置予定
  - CRYPTREC暗号リストのPQC対応課題を整理
  - [暗号技術検討会報告書，4章，p.27]
- ML-DSA（FIPS204）
  SLH-DSA（FIPS205）
  の安全性・実装性能を今後評価予定
  - FIPS203だけ前倒しで評価しただけなのでご安心を
  - 必要に応じ年度途中のリスト改定も検討

TLS暗号設定ガイドラインの今後

- スケジュール感：2027年度見直し
  - 2026年度に見直し検討を実施予定
  - [暗号技術検討会報告書，4章，p.27]
- PQCサポートに向けたTLS 1.3への移行が論点
  - これもやらなあかんこと：
    電子証明書の有効期限短縮化等への対応
    暗号強度要件設定基準も見直し予定

Key Takeaways

- CRYPTRECは暗号アルゴリズム選定の公的参照点
- 2026年3月改定でPQCリストを新設
  - ML-KEMが鍵共有として掲載
  - 署名方式は現時点では未掲載だけど評価対象になってる
- TLS暗号設定ガイドラインも見直し検討へ

Appendix：今後の検討課題となりうるもの

- Category 1・2相当暗号の扱い
- Camellia，KCipher-2, SHAKE-256は現在掲載保留
- 現行暗号とPQCを組み合わせたハイブリッド構成の扱い
- FIPS 204／FIPS 205後の評価順序
  - [暗号技術検討会報告書，2.4.3節，p.8]

Appendix：ハイブリッド構成の扱いをどうするか

- ハイブリッド構成をPQCリストに含めると複雑化
  - TLS暗号設定ガイドライン等で扱う案
- 上記は報告書中の意見であり決定事項ではない
  - [暗号技術検討会報告書，3.2.2節，p.24]
- 一方，TLSガイドライン見直し検討は予定として明記してて，私もちゃんとやります
  - [暗号技術検討会報告書，4章，p.27]

Ongoing Innovation

IIJ Internet Initiative Japan

Stay safe and healthy