信頼される安心を、社会へ。
SECOM

PQCと標準化動向

セコム株式会社　IS研究所
伊藤忠彦

2026年2月27日

伊藤　忠彦（セコム株式会社　IS研究所　上級研究員）

信頼される安心を、社会へ。
SECOM

研究分野：暗号の運用技術及びそのガバナンス

- **暗号鍵管理**、ルート認証局の**ポリシー管理**、**暗号移行**、制度設計

主な活動領域：標準化やルール整備

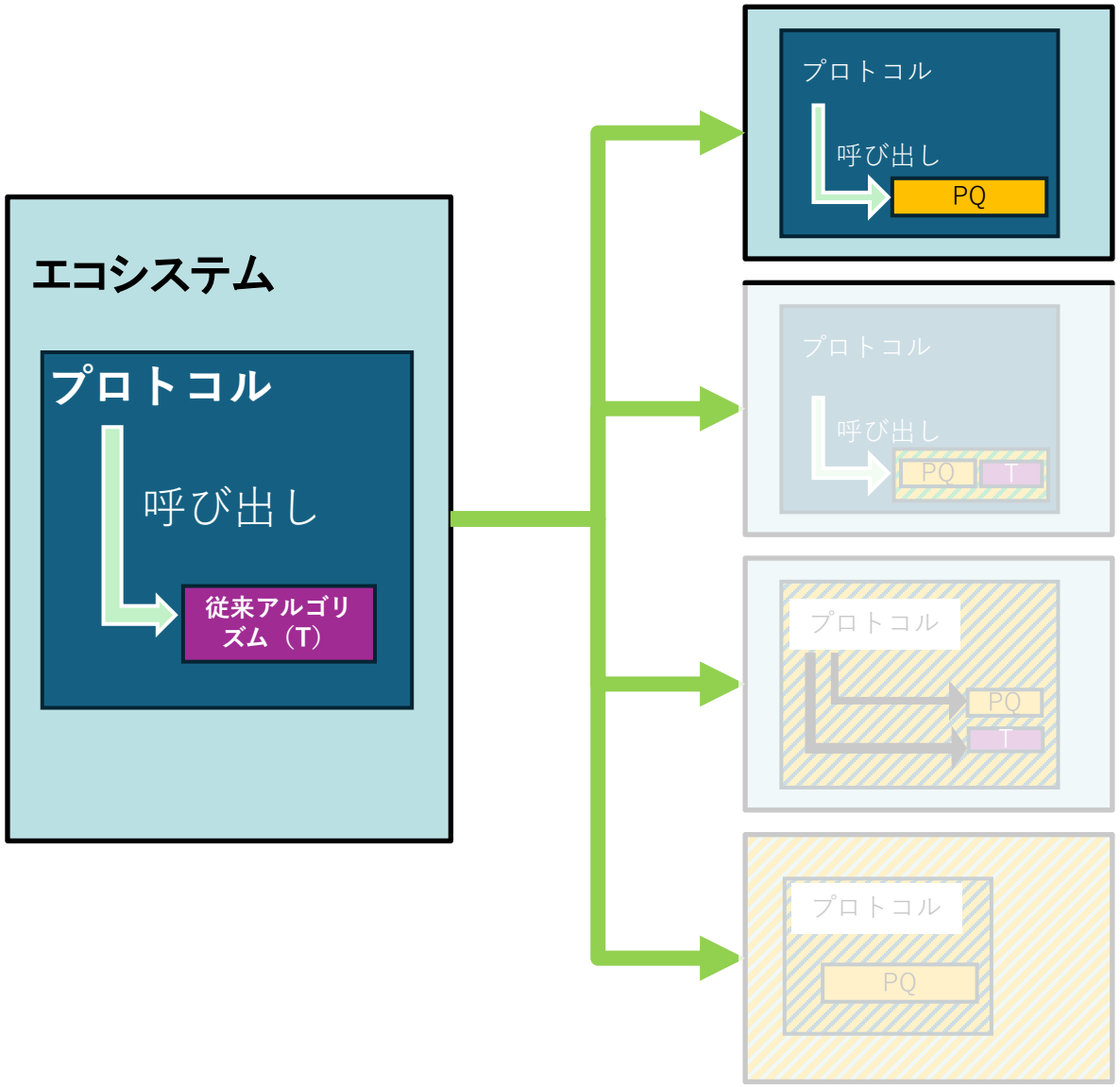
- **IETF**　(鍵管理関連国際標準の提案：RFC 8813, RFC 9295, RFC 9336, RFC 9919など)
- **CA/BForum**　(Web用証明書に関する国際ルール整備)
- **IPA** 非常勤 研究員（国内向けガイドライン作り等）
- **CRYPTREC** 暗号技術評価委員会 耐量子暗号WG
- **CRYPTREC** 暗号技術評価委員会
- **JNSA**（日本ネットワークセキュリティ協会）　PKI・PQC運用技術WG

PQCアルゴリズムの標準化

信頼される安心を、社会へ。
SECOM

アルゴリズム	CMS（pure方式）	X.509証明書（pure方式）
FIPS 203 ML-KEM (2024年8月)	RFC-to-be 9935 (近日公開)	RFC-to-be 9936 (近日公開)
FIPS 204 ML-DSA (2024年8月)	RFC 9882 (2025年10月)	RFC 9881 (2025年10月)
FIPS 205 SLH-DSA (2024年8月)	RFC 9909 (2025年12月)	RFC 9814 (2025年12月)
FIPS 206 FN-DSA (近日公開)	NISTの標準化を待つ見通し サイドチャネル攻撃の懸念が指摘されている	

一言でPQC移行と言っても、複数のアプローチが存在



Pure PQC

従来アルゴリズムをそのままPQCへ
（プロトコルやエコシステムへの変更は最低限）
標準化や実装も比較的早い
近く、利用可能

PQ/T Composite

2つのアルゴリズムから単一のアルゴリズムを構築
プロトコルやエコシステムへの変更は少ない
安全性は高いが、アルゴリズム（斜線）部分の**複雑性は増す**
（Pureに比べ）標準化に時間を要し、利用にはもう少し時間がかかる

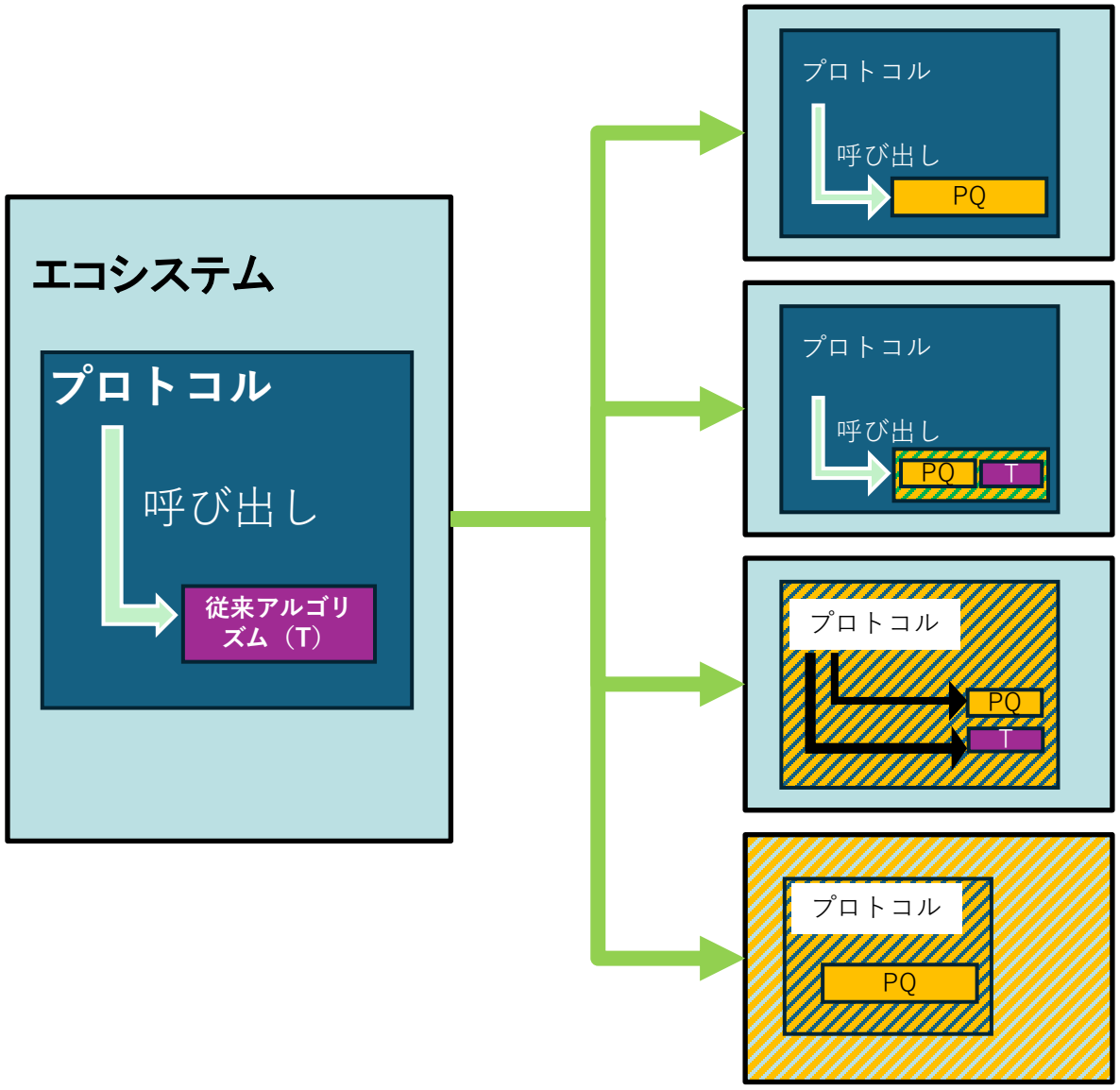
Hybrid “Protocol”等のアプローチ

後方互換性等のために、プロトコルもある程度変更

プロトコルのみならず、エコシステムも変更するアプローチ

時間がかかりがち

一言でPQC移行と言っても、複数のアプローチが存在



Pure PQC

従来アルゴリズムをそのままPQCへ
（プロトコルやエコシステムへの変更は最低限）
標準化や実装も比較的早い
近く、利用可能

PQ/T Composite

2つのアルゴリズムから単一のアルゴリズムを構築
プロトコルやエコシステムへの変更は少ない
安全性は高いが、アルゴリズム（斜線）部分の**複雑性は増す**
（Pureに比べ）標準化に時間を要し、利用にはもう少し時間がかかる

一般的な解決策
（多数のプロトコルで実行可）

Hybrid “Protocol”等のアプローチ

後方互換性等のために、プロトコルもある程度変更
プロトコルごとに検討が必要

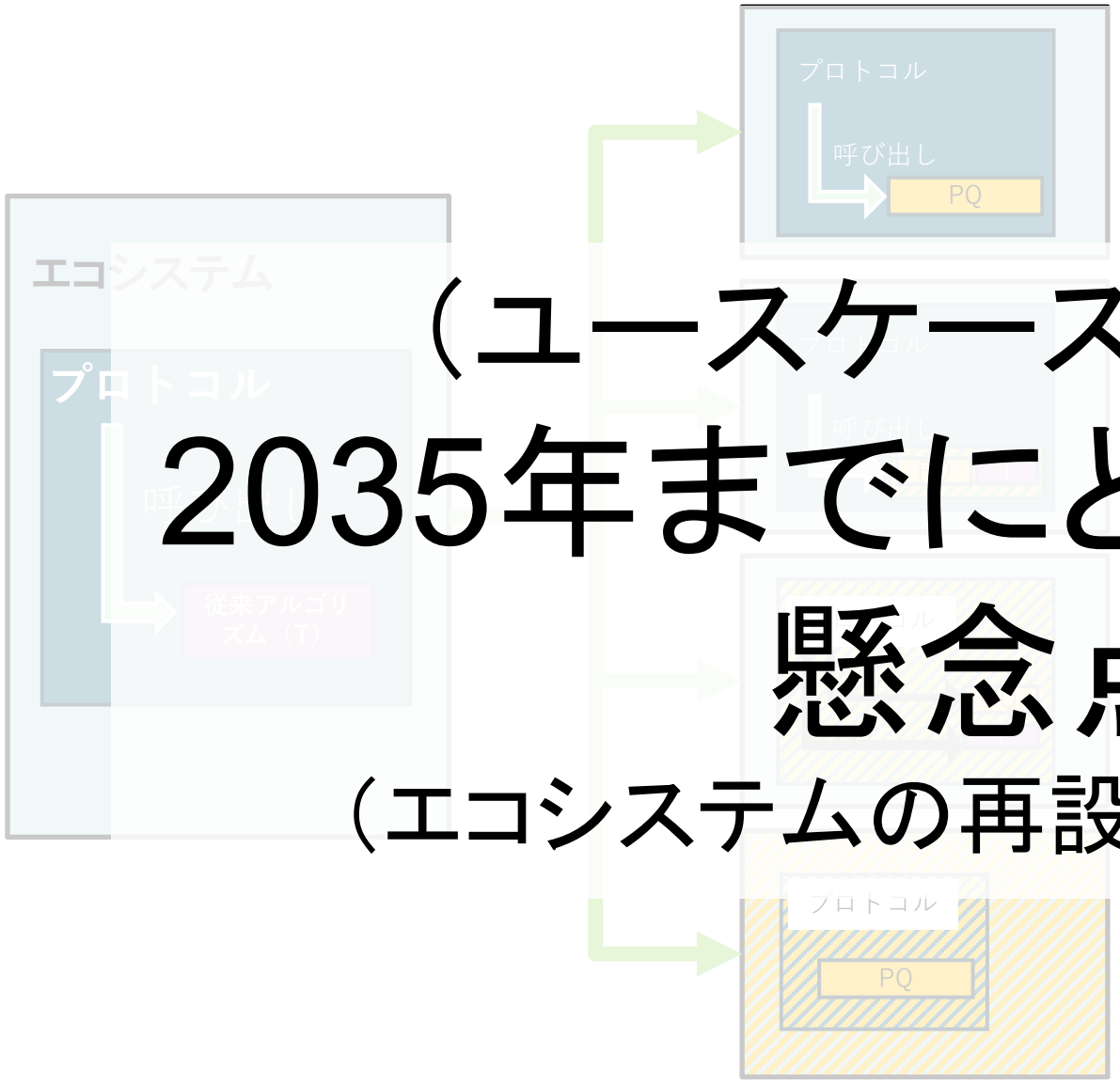
プロトコルのみならず、エコシステムも変更するアプローチ

他のアプローチで解決できない課題/要件がある場合採用
プロトコルごとに検討が必要
プレイヤーが多い / 変化が多いと、合意形成に時間がかかりがち

特定プロトコル向け
解決策

一言でPQCと言っても、複数のアプローチが存在

信頼される安心を、社会へ。
SECOM



Pure PQC

従来アルゴリズムをそのままPQCへ
（プロトコルやエコシステムへの変更は最低限）
標準化や実装も比較的早い
近く、利用可能

一般的な解決策
（多数のプロトコルで実行可）

2つのアルゴリズムから単一のアルゴリズムを構築
プロトコルやエコシステムへの変更は少な
安全性は高
（Pureに比べ変化に時間を要す、利用も時間がかかる

Hybrid “Protocol”等のアプローチ
安全性等のために、プロトコルもある程度変更
プロトコルごとに検討が必要

特定プロトコル向け
解決策

プロトコルのみならず、
エコシステムも変更するアプローチ
他のアプローチで解決できない課題/要件がある場合採用
プロトコルごとに検討が必要
プレイヤーが多い / 変化が多いと、合意形成に時間がかかりがち

（ユースケース依存だろうが）
2035年までにどこまでできる？
懸念点は？
（エコシステムの再設計などできるのか？）

個別対応が必要そうなケース：暗号資産関連

- ブロックチェーンの暗号移行は、暗号移行を難しくする要素の見本市
  - 更新できない署名鍵の存在
  - 最近のブロックチェーンは複雑性が増しており、
    移行難易度がさらに高まっている
  - etc.
- ガバナンスで解決する要素が、他のプロトコルより大きくならざるをえない
  - 新たな課題：
    - 誰が我慢するのか？
    - ステークホルダの対話の場は？
    - 検討するインセンティブは？
- 現状、明確な解決策は見つかっていないが…

論点整理

SCIS 2026 2026 Symposium on
Cryptography and Information Security
Hakodate, Japan, Jan. 26 – 30, 2026
The Institute of Electronics,
Information and Communication Engineers

PQC 移行の超難問: 複雑化するブロックチェーンと交錯する人間のエゴ

The Grand Challenge of PQC Migration: Increasing Blockchain Complexity and Conflicting Human Egos

福田 岐弦 * 松尾 真一郎 † 須賀 祐治 ‡ 伊藤 忠彦 §
Kigen Fukuda Shin'ichiro Matsuo Yuji Suga Tadahiko Ito

あらまし 2008 年のビットコインの発明以来, ブロックチェーンは単なるトランザクション台帳から, 複数レイヤーにまたがる多機能な金融システムへと進化を遂げた. 現在, そのセキュリティは量子コンピュータの登場により脅かされている. 耐量子計算機暗号 (PQC) への移行の必要性は広く議論されているが, ブロックチェーンはその分散性や長期的セキュリティ要件ゆえに, 暗号移行の難易度が極めて高い領域である. 今日, システムの複雑化により単純な暗号移行モデルの適用がもはや困難となっていることに加え, 短期的利益を追求する投資家や採算性を重視するマイナーなど, 人間の経済的合理性や打算が移行の重大な障害となっている. 本稿は, 2025 年 12 月現在におけるブロックチェーンの PQC 移行の困難性と現状について, 包括的な分析を提供する. 具体的には, 移行検討が必要な構成要素とそれらの技術的課題を分析するとともに, 倫理的ジレンマやステークホルダー間のインセンティブの衝突など, 運用面での障害について体系化して整理する. また, 今後アカデミアやブロックチェーンコミュニティが協力し取り組むべき研究の指針について提言する. 本研究は, 進行中のコミュニティの議論や先行研究を集約することで, ブロックチェーンの量子耐性獲得のための検討の基盤を確立することを目指す.

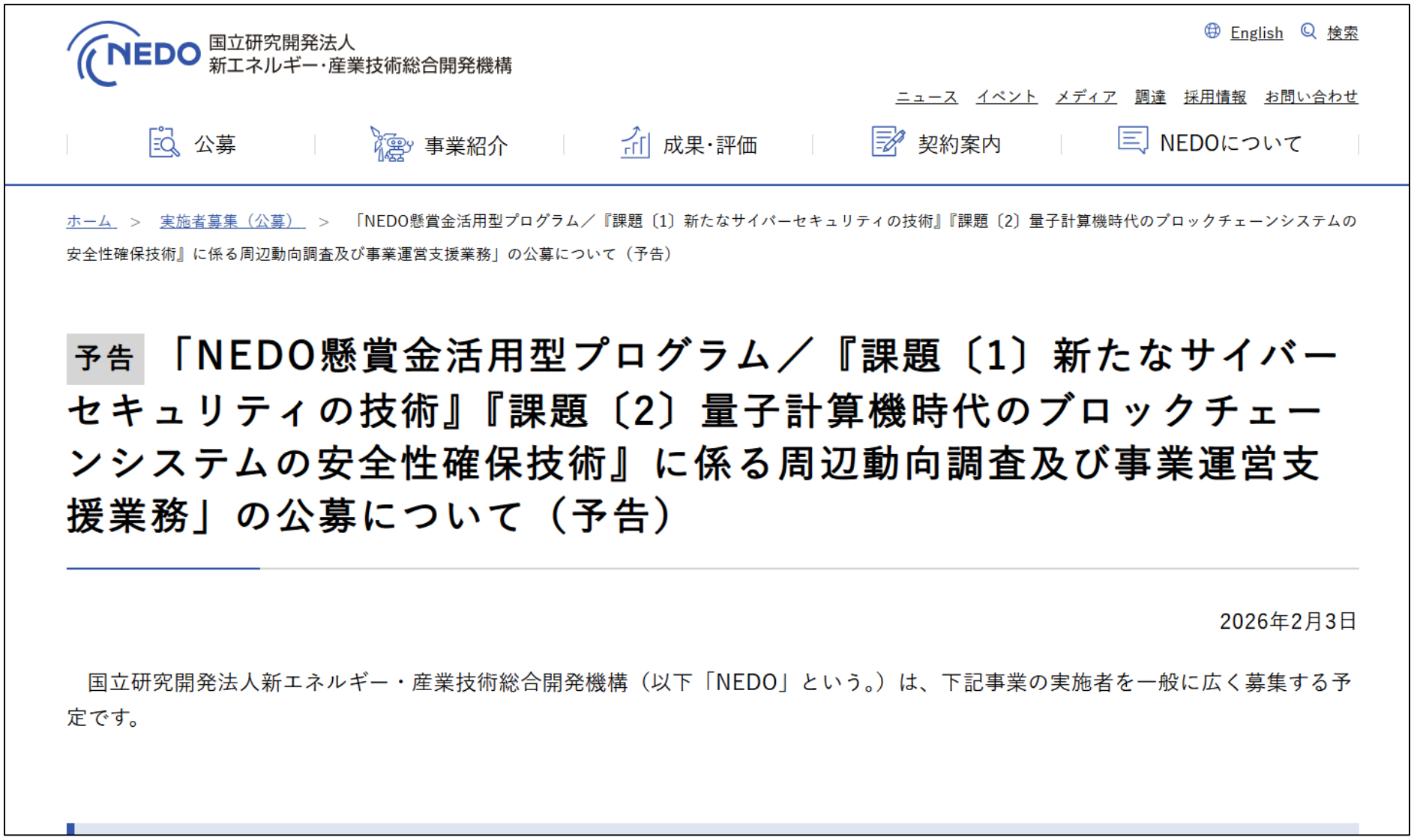
キーワード ブロックチェーン, 耐量子計算機暗号, ガバナンス

https://eprint.iacr.org/2025/1626 （リンクは英文の公開版）

ガバナンスに関する対話

https://bgin-global.org/events/20260301-block14/jp

検討へのインセンティブ



国立研究開発法人
新エネルギー・産業技術総合開発機構

English 検索

ニュース イベント メディア 調達 採用情報 お問い合わせ

公募 事業紹介 成果・評価 契約案内 NEDOについて

ホーム ＞ 実施者募集（公募） ＞ 「NEDO懸賞金活用型プログラム／『課題〔1〕新たなサイバーセキュリティの技術』『課題〔2〕量子計算機時代のブロックチェーンシステムの安全性確保技術』に係る周辺動向調査及び事業運営支援業務」の公募について（予告）

予告 「NEDO懸賞金活用型プログラム／『課題〔1〕新たなサイバーセキュリティの技術』『課題〔2〕量子計算機時代のブロックチェーンシステムの安全性確保技術』に係る周辺動向調査及び事業運営支援業務」の公募について（予告）

2026年2月3日

国立研究開発法人新エネルギー・産業技術総合開発機構（以下「NEDO」という。）は、下記事業の実施者を一般に広く募集する予定です。

https://www.nedo.go.jp/koubo/IT1_100390.html