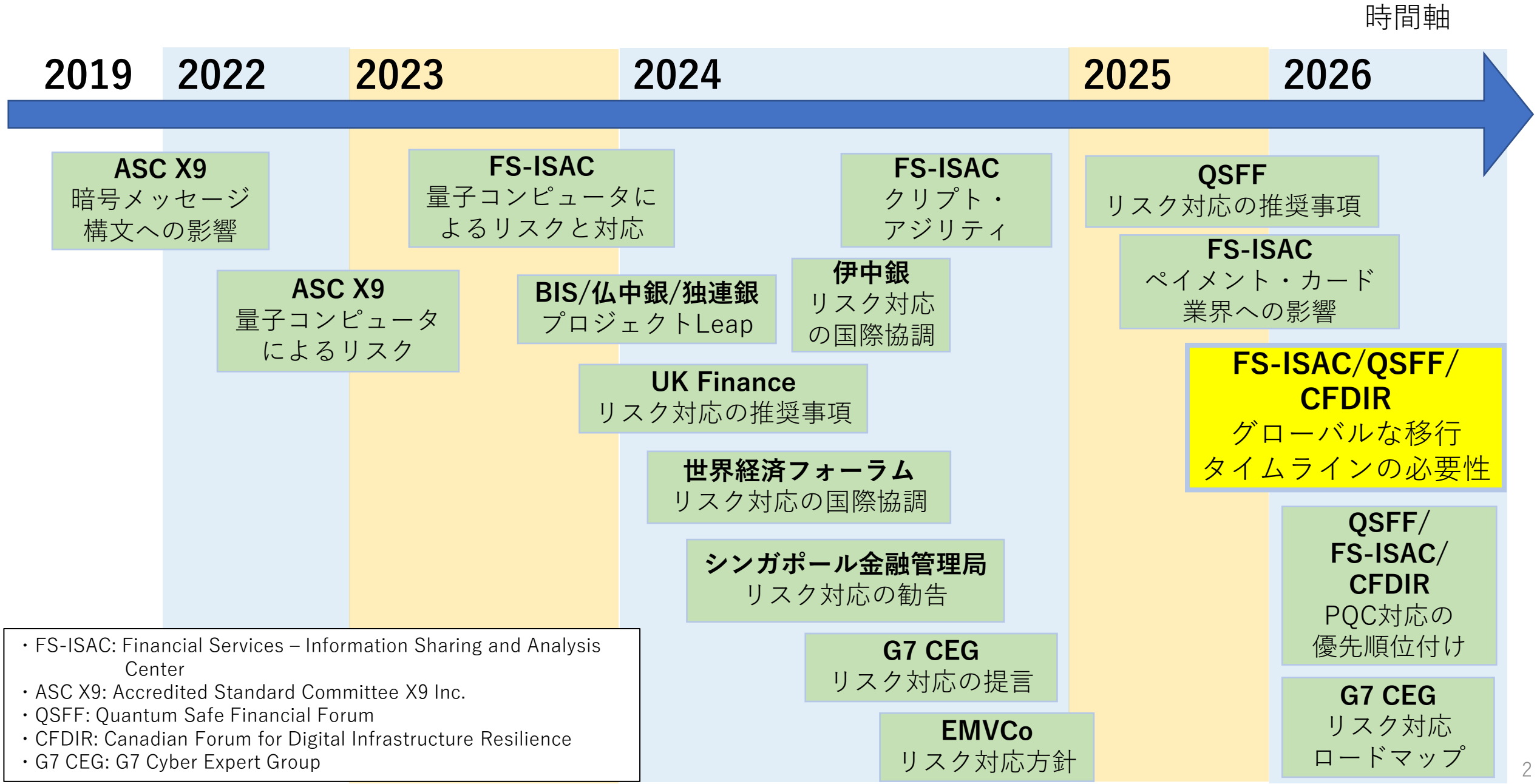
情報セキュリティ・シンポジウム
2026年2月27日

海外の**PQC**移行に関する動向

金融研究所参事役
宇根正志

本発表の内容は、発表者個人に属し、日本銀行の公式見解を示すものではありません。

金融関連の当局・団体による提言・ガイダンス



- FS-ISAC: Financial Services – Information Sharing and Analysis Center
- ASC X9: Accredited Standard Committee X9 Inc.
- QSFF: Quantum Safe Financial Forum
- CFDIR: Canadian Forum for Digital Infrastructure Resilience
- G7 CEG: G7 Cyber Expert Group

提言・ガイダンスの主なポイント

- **業界としての取組み**を重視（UK Finance）
- **グローバルな相互運用性、国際協調**を重視
  （世界経済フォーラムほか）

  ⇒　金融分野で議論・検討が先行している背景の1つ
- **ハイブリッド方式**を推奨（ASC X9ほか）
- **クリプト・アジリティ**を重視（FS ISACほか）
- **長期的な計画と対応**を重視（FS ISACほか）

FS-ISAC/QSFF/CFDIRのポジションペーパー

“The Timeline for Post-Quantum Cryptographic Migration” （2025年9月）

- 提言作成の参加者が所属する金融機関・団体
  - Banco Santander, CIBC, Wells Fargo, European Investment Bank, TD Bank, Dutch Banking Association, National Bank of Canada, Allianz SE, Bank of Montreal, Scotiabank, Bank of Spain, Mizuho Americas
- **PQC対応の難しさ（時間がかかる）**を再認識すべき
  - 金融サービスの複雑な依存関係がハードルに
- **グローバルな移行タイムラインの策定**が重要
- **ステークホルダー**との調整が必須
  - 金融サービスを提供する事業者・団体、ベンダー、標準化機関、当局

・FS-ISAC: Financial Services Information Sharing and Analysis Center
・QSFF: Quantum Safe Financial Forum
・CFDIR: Quantum Readiness Working Group of Canadian Forum for Digital Infrastructure Resilience
・https://www.fsisac.com/the-timeline-for-post-quantum-cryptographic-migration

マスターカード社の研究調査レポート

“Migration to Post-Quantum Cryptography” （2025年10月）

- 著者：
  - マスターカード、シンガポール南洋理工大学、PQStation のスタッフ
- **Quantum Key Distribution：広く展開・使用するには高価**
  - PQCにアド・オンして使用
  - 特に高いセキュリティが必要なケースでの補完的手段
- **ペイメントカードへのPQC実装（署名）**に課題
  - 処理時間・メモリの制約
  - 共通鍵暗号の活用も視野に
- ハイブリッド方式によるTLS（Transport Layer Security）実装（鍵共有）
  - 楕円曲線暗号とML-KEMの組合せ

・Beric, J. et al., “Migration to Post-Quantum Cryptography,” Mastercard R&D white paper, October 2025.
・https://www.mastercard.com/global/en/news-and-trends/Insights/2025/post-quantum-cryptography-white-paper.html