金融機関の投資戦略検討に資する動的定量分析モデル
― PQC移行問題を題材に ―

A Dynamic Quantitative Model for Financial Institution Investment Strategy
― The Case of PQC Migration ―

村上 誠樹 暗号・認証分科会 情報セキュリティ大学院大学

Abstract: Financial institutions must make forward-looking security investment decisions under uncertainty, particularly regarding post-quantum cryptography (PQC) migration. As cryptographic standards evolve and systemic risks interact with macroeconomic conditions such as interest rates and policy measures, determining the appropriate level and timing of investment becomes a complex optimization problem. This study develops a dynamic quantitative model that adapts a computable general equilibrium (CGE) framework to individual financial institutions. By parameterizing scenario conditions—including baseline profits, policy environments, and the interest rate-earnings relationship—the model formulates security investment and risk reduction as an optimization problem. Scenario-based and sensitivity analyses provide an analytical tool to support strategic investment allocation under future risk uncertainty.

1.研究背景

- 量子コンピュータ時代の到来における、耐量子計算機暗号PQC（Post-Quantum Cryptography ）への移行が金融機関で必要となっており、安全保障からも必要高
- 各機関からガイドラインが提示されているものの、根拠を伴う説明付けに資する投資判断の基準は不足

- 企業におけるERM（Enterprise Risk Management）は過去・現在のみの視点で、将来の視点は限定的
- リスクベースアプローチを実施する企業としてPQC移行の投資対応における規模・優先度付けの経営判断が困難

2.目的

- **「将来のセキュリティ投資」に資する、PQC移行に限定しない汎用的シミュレーションモデルを構築**
- 本研究では「金融機関のPQC移行」を具体的題材とし、必要となるモデルおよび分析手法を設計・実装

- PQC移行を含むセキュリティ投資を金融機関における「投資配分・リスク低減」の最適化問題として定式化することで、

金融分野の将来リスクを定量的に評価し、企業はセキュリティ投資をどの水準まで配分すべきか

を判断するための分析枠組みを提示する

3. 本研究の実施事項

日本国内で大手金融機関が、監督省庁のもとPQC移行に向け進行している現状を表現
重要インフラである金融機関が、PQCに移行しないことのリスクや・不安定な状況を定量的に表現するモデルを提案

1対象領域	2脅威	3ツール
金融機関	PQCリスク	数理最適化
システミックリスクを抱える重要インフラ	量子コンピュータ実現による暗号解読リスク	マクロ経済学手法をもとに定量評価

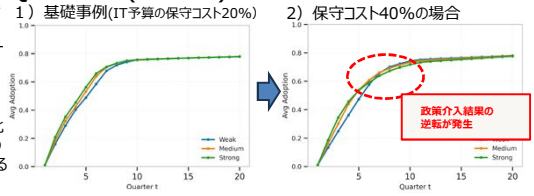
4.成果：モデルの基礎構造

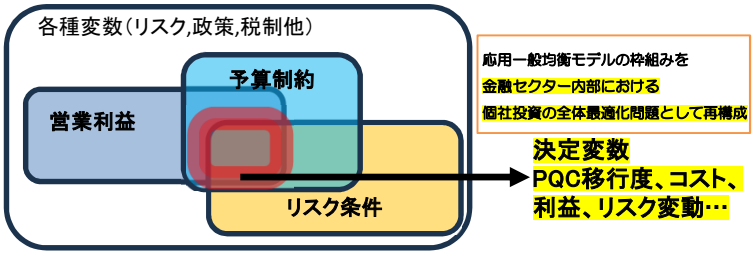
政策介入の経済的波及効果の分析に用いられるマクロ経済学の手法
「応用一般均衡モデリング」Computable General Equilibrium Modeling
をもとにセキュリティ投資、利益等を包括表現するモデルを構築
（コンピュータセキュリティシンポジウム2025にて発表済）

事例：金融機関のPQC移行率(平均値)のシミュレーション推移

・金融機関全体において、金融庁の指導・監督によって各行のPQC移行の達成状況に差が生じるシナリオ(強・中・弱は政策介入)

・個々の金融機関が保守投資、DX投資を実施する中、それらの比率を変える事でPQC移行のためのIT投資の推移の変動を表現できるかをシミュレート





5.進行中：シナリオベースアプローチ構築

営業利益	−	セキュリティ投資	−	リスク損失
攻めのDX投資利益＋営業活動		IT投資の予算内でのセキュリティ投資		対処しなかった際の損失を設定

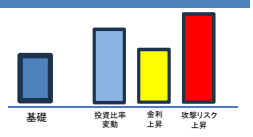
＝ 最大化対象（純利益）

- 金融機関の個社活動による基礎利益
- 政策介入の有無や経営上の優先度
- 金利と利益の関係

などをシナリオ条件として設定の上、納得できる根拠をパラメータ化した数理最適化問題として解く

6.感度分析

前提条件を変動させることで総損失（リスク＋コスト）への影響度への感度分析を実施することでの妥当性検証



7.今後の活動

経済学、社会学分野学会の論文投稿に向け準備中