金融機関としての投資戦略検討に資する定量分析モデル検討 ―PQC移行問題を題材に―

村上 誠樹[1,a)]　後藤 厚宏[2,b)]

概要：企業活動を発展させ継続するためには，セキュリティ投資を適切に実施することが必要である．ITシステム運用に必要な維持管理投資・金融 DX 投資および，それらを支えるセキュリティ投資をベースとし，追加として法規制など外的要因によって追加のセキュリティ投資を実施しなければならない場合においての，投資判断を安全性を判断するための指標が必要となる．本稿では，PQC（耐量子計算機暗号）への移行をテーマに，金融機関を対象として，関連投資の優先順位を評価するための定量分析モデルを検討する．

キーワード：応用一般均衡（CGE）モデリング, Post-Quantum Cryptography（PQC）

Quantitative Analysis Models for Investment Strategy Planning in Financial Institutions: A Case Study on PQC Migration

Masaki Murakami[1,a)]　Atsuhiro Goto[2,b)]

Abstract: To ensure the growth and sustainability of corporate activities, appropriate implementation of security investments is essential. Based on the structure of maintenance investments required for IT system operations, financial DX investments, and the supporting security investments, there is a need for indicators to guide investment decisions-particularly when additional security investments are required due to external factors such as legal and regulatory changes. This study focuses on the migration to post-quantum cryptography (PQC), examining financial institutions as the subject of analysis, and explores a quantitative model for evaluating and prioritizing related security investments.

Keywords: Computable General Equilibrium (CGE) modeling, Post-Quantum Cryptography(PQC)

1. はじめに

近年，サイバー攻撃は国家安全保障や社会経済活動に深刻な影響を及ぼすリスク要因として認識されており，重要インフラを担う民間事業者のみならず，政府の積極的な関与が不可欠となっている． 実際，2025 年 5 月に成立したサイバー対処能力強化法および関連整備法 [1] は，国外から発信される通信を媒介する国内事業者との協定に基づき，攻撃の疑いがある通信情報を取得・分析する仕組みを整備し，国家レベルでの対処体制を制度的に裏付けたものである． この新法は，従来の民間の自主努力に依存したサイバーセキュリティ対策に対し，政府施策としての強力な補完的役割を果たすことを意図している．こうした状況の下では，政策介入がもたらす効果や副作用を事前に評価することが一層重要となる． そのためには，サイバーセキュリティ施策の実効性を定量的に予測・検証するためのシミュレーション手法の研究が求められる． これは単なる技術的対策の評価にとどまらず，制度設計や社会的コストを含めた総合的な政策効果分析を可能にするものである．本稿では，その第一歩として，サイバーセキュリティ投資および政策介入の効果を分析するためのモデル構築に取り組ん

[1] 情報セキュリティ大学院大学
Institute of Information Security
[2] 情報セキュリティ大学院大学
Institute of Information Security
[a)] mgs248506@iisec.ac.jp
[b)] goto@iisec.ac.jp

だ． 以下では，その中間的な成果を報告し，今後の研究の方向性について検討を行う．

2. 本研究の位置づけ

政府が民間企業へのサイバーセキュリティ対策に関与を強める法改正によって民間への強制力やインセンティブによって全体がどう変化し，どのような効果があるかという議論を行って，その政策の効果を評価する手法が必要とされている． このような背景において，技術的な実装とは異なる政策評価の一つの手段として取り組み始めたものである．ツールとしては，応用一般均衡モデルを用いてシミュレーションを実施する． 政策評価などに用いられるものであり，実用上は産業連関分析など実データに基づいて政策決定を行うが，今回は仮想的なパラメータを設定し，変数間の関係性の変化を分析することを目的としている． 動的マクロ経済学で用いられる社会会計行列（Social Accounting Matrix, SAM）を適用する手前の「基礎モデル」であると位置づける．

そのため，研究の目的は分析そのものではなく，モデル構築に限界が存在するという前提の上で，応用一般均衡モデルという手法が政策評価にどのように適用できるかを検証する試みである．

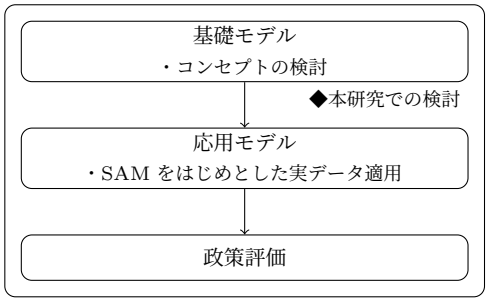

図 1 概念図
Fig. 1 Conceptual diagram

3. 重要インフラのサイバーセキュリティ

まず，サイバーセキュリティ投資の重要性を，実例を示しつつモデルを構築するにあたり題材を選定する必要がある．そこで，本稿では，金融機関における耐量子計算機暗号（PQC）への移行問題とする．操作可能なパラメータとして外力たる業界規制を行える監督省庁となる金融庁が存在するため，政策決定によるポリシー操作が実現足りえることと，金融機関が社会インフラとしての機能を有するためである．本章では，PQC 関連において金融機関を取り巻く背景を説明する．

3.1 用語

本研究の位置づけと対象範囲を定義するにあたり，PQC 移行に関連する用語を記載する．出典は [2] による．

表 1 用語
Table 1 Keywords

用語	説明
耐量子計算機暗号 / PQC (Post Quantum Cryptography)	量子コンピュータが実用化されても（現時点）効率的な攻撃方法が知られていない暗号
CRQC (Cryptographically relevant quantum computer)	量子脆弱性をもつ暗号を現実的な時間とリソースで解読可能な量子コンピュータ
クリプト・インベントリ	暗号利用箇所やアルゴリズムを一覧化した資料
クリプト・アジリティ	別の暗号アルゴリズムへ影響を最小化しながら移行可能とするシステム特性

3.2 社会インフラとしての金融機関とその特性

「金融」は「金銭を融通する」役割を表現したものであり，例えば銀行は「間接的金融」という，他者間がものやサービスを契約する際に，直接相手を探してやり取りすることを仲介する役目を持つ．近年では FinTech サービスの発展もあり，後述するように現代社会において重要インフラとみなされており，預金取扱機関である銀行をはじめ各金融機関は，機能維持のためにセキュアな基盤を運用する手段として暗号技術を幅広く活用している．ここには金融機関やベンダー，監督官庁，そしてユーザ（個人・法人）など，多岐にわたるステークホルダが存在する．そのため，暗号技術の危殆化の際に想定されるリスクは，多層的な観点から検討されなければならない．他方，近年，産業界では量子コンピュータの開発が進展しつつあり，画期的な処理能力の向上によって新規材料開発や創薬などへの貢献が期待されている．一方で，現在広く利用されている暗号技術の安全性低下も指摘されており，量子コンピュータの性能が一定水準を超えれば，一部の暗号は現実的な時間内に解読されるリスクが高いと考えられている．金融機関においては，量子コンピュータが実用的な性能をもつ段階を見越したリスク対策が必要であり，この課題に関しては，金融庁が主催する検討会 [2] でも整理が進められてきた．しかしながら，量子コンピュータ時代における既存暗号の脆弱化リスクが提起されている一方で，PQC への移行にともなう技術的・社会的影響を総合的に分析し，その導入に向けた課題や要件を十分に議論する段階には至っていないのが現状である． 他方，預金取扱機関である銀行はサイバーセキュリティ基本法に基づき，内閣官房内閣サイバーセキュリティセンターが策定する「重要インフラのサイバーセキュリティに係る行動計画」[3] において「金融」分野の重要インフラ事業者に該当する．海外規制動向に関する

情報収集や移行ロードマップの策定など，業界全体が一体となった取り組みが急務となることが想定されるが，現時点では関係者が集まり十分な議論が行われているとはいえない．また，政府としても「Harvest Now, Decrypt Later（HNDL）攻撃」への対策を検討し始めており，安全保障の観点でも重要な課題として認識されつつある．

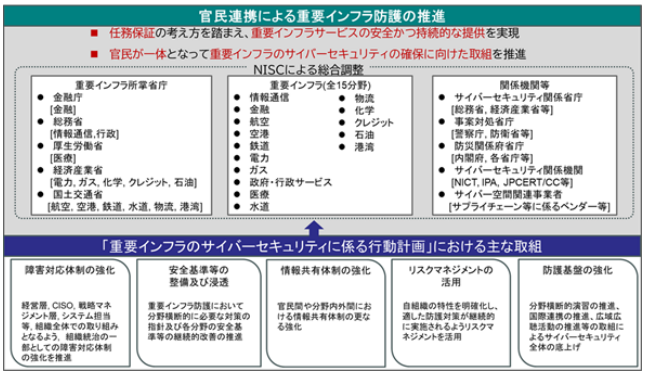

図 2　重要インフラ 15 分野（[3] を参考に著者作成）

Fig. 2　The 15 Sectors of Critical Infrastructure (Source: Created by the authors, based on [3])

以上，量子コンピュータの普及を見据えた金融機関における暗号技術の移行リスクを取り巻く状況から明らかなように，現在社会的・経済的観点を含めて包括的に整理する必要に迫られていることから，題材として選定した．

3.3　対象外とする内容

注意点として，本ケースでは PQC を題材としているもの，暗号技術そのものの技術有用性などには踏み込まず，暗号の置換フェーズの定量的評価にのみ焦点に当てる．

4.　理論的アプローチ

4.1　伝統的なモデル

企業のセキュリティ投資については，2002 年 Gordon らによって提案された情報セキュリティ投資における経済モデルの研究 [4] が有名である．情報セキュリティ投資における最適化問題を経済学的フレームワークで定式化したもので，企業が限られた予算の下で情報資産の保護レベルを決定する際の意思決定プロセスが示唆されるなどが行わ，セキュリティ投資の収穫逓減性などが示された．

4.2　公共インフラの政策シミュレーション

応用一般均衡（GCE）モデリングは，政策介入が経済全体に与える波及効果を定量的に分析することに適する手法であり，公共インフラ政策のシミュレーションにおいて用いられている．例えば，国内航空分野における規制緩和における分析 [5] に活用されるなど，介入効果を定式化し，比較評価するという政策シミュレーション目的で活用される．

4.3　金融システムへの CGE の適用性

金融システムに関する研究としては，例えば [6] が挙げられる．国際貿易やグローバルな経済政策の分析で広く用いられる応用一般均衡（CGE）モデリングである GTAP モデルに，金融の動きを表現するモジュールを追加することで，金融フローに関する政策の影響分析を試みている．

4.4　産業連関表を用いたサイバー被害の定量的予測手法

PQC 移行が遅れた場合やリスク管理に失敗した場合の経済的損失を，定量的に把握する必要がある．これは，PQC 対応を企業として実施する意思決定としては必要な定量的数値となりうると考えられるが，ステークホルダの多さから容易ではない．

そこで，近い考えが行われている内容として，マクロ経済学観点から着目した論文を題材とした小梶 [7] によるサイバー被害の予測研究を紹介する．小梶らは，被害予測や国の対策の精度を高めるために，日本のサイバー攻撃による経済的損失額をマクロ視点で，波及被害 (川上産業，川下産業への影響) も含めて分析することを提案している．具体的には，サイバー攻撃による被害データ（攻撃を受けた産業，失われた労働時間等），マクロ経済データ（生産量，資本ストック，労働力等）を使用し，マクロ経済学モデルに基づき，特定年度の被害額を，国全体における産業毎の直接被害と波及被害について定量的に推計している．さらに特定産業が受けた攻撃の影響（波及被害）が川下に位置する他産業に及ぶか（前方連関），また川上に位置する他産業に及ぶか（後方連関）について定量的に示している．また，前者の直接被害の推計にあたっては，生産・資本・労働から算出する生産関数を用い，波及効果の算出にあたっては，総務省が公表している産業連関表 [8] を中心とした複数の情報源を活用している．

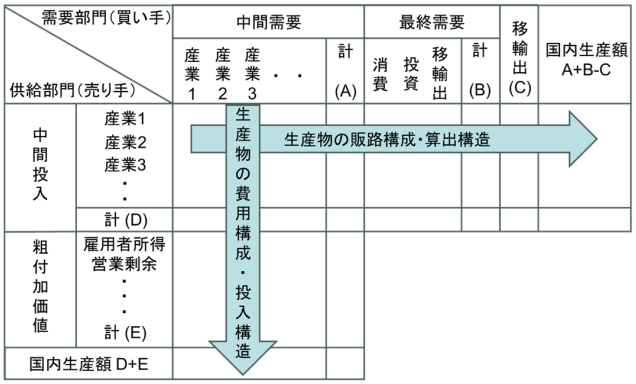

図 3　産業連関表（[7] を参考に著者作成）

Fig. 3　Input-Output Table (Source: Created by the authors, based on [7]).

産業連開表とは，一定の地域（国全体，都道府県など）における一定期間（１年間）の財・サービスの生産状況，

産業相互間の取引状況を行列形式でまとめた統計であり，行列式として産業の連関を計算することで推定を実施している．

応用一般均衡モデリングにおいても，この産業連関表を実データとして定義のうえ分析することで具体的なデータに基づく政策評価を行うことが期待できるが，先述したように，本研究はデータ適用の前段階のモデル構築を検討したものであり，今後の応用研究においての適用が見込まれる．

5. 定量分析モデルの構築

5.1 研究の目的と手法

本研究では，金融機関におけるポスト量子暗号（PQC）への移行をテーマに，応用一般均衡（CGE）モデリングを用いた政策シミュレーションを実施する．一般的に CGE 分析では，産業連関表などの実データに基づく社会会計行列（SAM）を用いるが，本研究では仮想的なパラメータを設定し，金融庁による政策介入の強度と PQC 普及率の関係を分析する．

5.2 シミュレーションの前提条件

本モデルでは，以下のシナリオと前提条件を設定する．

5.2.1 シナリオ：PQC 移行の遅延

金融機関全体で PQC への移行が必須とされる状況を想定する．この際，金融庁の指導・監督（メガバンクのみ，あるいはメガバンクと中規模銀行の両方を対象とする）によって，移行の達成状況に差が生じるシナリオを分析する．

5.2.2 モデル設定

- **対象機関**: メガバンク 10 行，中規模銀行 100 行，小規模銀行 1000 行．
- **トランザクション**: 銀行間の取引は，同一規模内での関係はメガバンクでは大であるが，中・小規模の場合はことなる規模間の取引はランダムかつ少量とする．
- **リスク**: Q-Day（量子コンピュータによる暗号解読が可能となる日）に近づくにつれて，リスクの割合は単調増加すると仮定する．

5.2.3 分析課題

本モデルで解明を試みる主な課題は以下の通りである．

- **金融庁の施策強度**: 金融庁の指導の強さ（対象範囲，指導内容）が，PQC 普及に与える影響．
- **IT 投資のトレードオフ**: PQC 移行のための IT 投資が，DX（デジタルトランスフォーメーション）投資を圧迫し，金融機関の成長を遅らせる可能性．あるいは，PQC 投資を劣後させてでも DX 投資を推進する戦略がもたらす影響．

5.3 CGE 分析におけるモデル記述の基本構成

応用一般均衡モデリングにおいては，以下の構成で要素を設定しソルバーにて求解する．本節では，上記のモデル設定および分析課題に基づき記述する．

- **Indices**: モデルを構成する各要素のインデックス
- **Parameters**: モデル内で調整するパラメータ
- **Decision Variables**: 経済主体行動を表す決定変数
- **Constraints**: 制約や均衡条件などの制約条件
- **Optimization Problem**: 最適化問題

6. モデル構築

6.1 実行環境について

モデル求解には，GAMS(General Algebraic Modeling System)[9] というツールを使用する．特に，モデル拡張や，数値条件の設定の柔軟さを重視し，Python による公式 Wrapper となる GAMSPy[10] を利用する．

6.2 概要

金融機関における量子コンピュータ耐性暗号（Post-Quantum Cryptography, PQC）への移行を最適化する多期間動的計画問題．量子コンピュータの脅威（Q-Day）が迫る中，IT 予算制約下で PQC 投資と DX 投資のバランスを取りながら，システミックリスクを踏まえつつ業界全体の利益を最大化する．

6.3 モデル詳細

6.3.1 インデックス（Indecies）

index	記号	説明
銀行規模	$i, j \in I$	金融機関の規模分類 {mega, medium, small}
時間期間	$t \in T$	四半期単位 $\{t_1, t_2, \ldots, t_{20}\}$
政策種別	$p \in P$	規制政策の強度 {weak, medium, strong}

モデル描画の上での刻み幅になり，これらの組み合わせを以下のパラメータに基づいて設定する．

6.3.2 パラメータ（Parameters）

- **銀行特性パラメータ**

銀行の PQC 対応に要する各種コスト等を設定する．

パラメータ	記号	説明
銀行数	N_i	各タイプの銀行数（単位：社）
IT 予算	B_i	銀行あたり IT 予算（単位：億円/社）
PQC 移行コスト	C_i^{PQC}	完全移行に必要なコスト（単位：億円/社）
保守コスト率	ρ	IT 予算に対する保守費用比率
DX 投資収益率	r_i^{DX}	DX 投資の期待収益率

- **リスクパラメータ**

PQC 対応を実施しない場合のリスク，金融機関ネットワークの伝播影響の相互関係等を設定する．

パラメータ	記号	説明
Q-Day リスク	R_t^Q	時点 t における量子脅威の大きさ
リスク成長率	γ	Q-Day リスクの四半期成長率
ネットワーク強度	ω_{ij}	銀行タイプ間の相互依存度
連鎖リスク率	λ	ネットワーク連鎖によるリスク増幅

- **政策パラメータ**

金融庁からの規制を表現する外力等を設定する．

パラメータ	記号	説明
政策効果	ϵ_p	政策強度による採用促進効果
ペナルティ率	π	未採用に対する規制ペナルティ
割引率	δ	現在価値計算用の四半期割引率

- **税制・利益関連パラメータ**

対応を進めたことによる優遇措置（メリット）として税率軽減を想定，関連する値等を設定する．

パラメータ	記号	説明
法人税率	τ	DX 投資収益に課される標準的な税率
PQC 対応軽減税率	τ^{PQC}	PQC 対応を進めるメガバンクに適用される優遇税率
軽減税率適用閾値	x_{thd}	軽減税率が適用される PQC 採用率の基準値

6.4 決定変数（Variables）

下記がモデルによって表現したい対象であり，ソルバー実行による計算結果の数値が入る．

変数	記号	説明
PQC 採用率	$x_{i,t,p}$	銀行タイプ i の時点 t，政策 p での採用率（範囲 [0,1]）
DX 投資額	$I_{i,t,p}^{DX}$	DX 投資額（億円/行）
PQC 投資額	$I_{i,t,p}^{PQC}$	PQC 投資額（億円/行）
セキュリティレベル	$S_{i,t,p}$	ネットワーク効果を含むセキュリティ指標
サイバー損失	$L_{t,p}^{cyber}$	システム全体のサイバー攻撃損失
DX 投資収益	$R_{i,t,p}^{DX}$	DX 投資から得られる税引前収益
支払税額	$T_{i,t,p}$	DX 投資収益に対する支払税額

6.5 制約条件（Constraints）

6.5.1 予算制約 $(B_i, I_{i,t,p}^{PQC}, I_{i,t,p}^{DX}, \rho)$

各銀行タイプ $i \in I$ ごとに，四半期ごとの IT 予算 B_i があらかじめ設定されている．この予算には PQC 対応に関する投資額 $I_{i,t,p}^{PQC}$，DX 投資額 $I_{i,t,p}^{DX}$，および保守コスト（IT 予算の一定割合 $\rho \cdot B_i$ として計上される）が含まれる．制約として，これらの合計が各期の IT 予算を超えてはならない．したがって，銀行は限られた資源のなかで，どこまで PQC に振り向け，どこまで DX に振り向けるかを戦略的に判断する必要がある．

6.5.2 DX 投資の下限要件 (α, B_i, ρ)

さらに，単に予算の範囲内であればよいわけではなく，DX 投資に関しては必ず一定割合以上を確保しなければならない．これはパラメータ α（最小 DX 投資率）によって定義される．すなわち，IT 予算から保守費用を差し引いた残額のうち，α 倍以上を DX 投資に割り当てることが強制される．この条件は，DX を任意のオプションではなく必須の政策的要件としてモデルに組み込む意図を持つ．

6.5.3 PQC 投資と採用率 $(x_{i,t,p}, I_{i,t,p}^{PQC}, C_i^{PQC}, \epsilon_p)$

PQC の採用率 $x_{i,t,p}$ は，その期にどれだけ PQC 投資を行ったかによって変化する．各銀行タイプごとに設定された単位コスト C_i^{PQC} に応じて，採用率が段階的に上昇する仕組みになっている．また，規制政策の強度を示すパラメータ ϵ_p を導入しており，政策が強ければ同じ投資額でも採用率の増加が加速する．逆に弱い政策環境下では，同じ投資額を投入しても採用率の伸びは小さい．このように，投資行動と政策環境の相互作用を通じて PQC 導入の進展を記述する．

6.5.4 採用率の単調性 $(x_{i,t,p})$

採用率は不可逆的なプロセスとして扱う．すなわち，ある期で導入した PQC 技術が次期以降に撤回されることは想定しない．形式的には，$x_{i,t,p}$ は時間 t に対して単調増加列となる．この制約は，PQC がセキュリティ基盤の更新を前提とする技術であり，いったん導入すれば恒常的に維持されること表現するためである．

6.5.5 初期条件 (x_0, x_0^{mega})

初期時点における PQC 採用率については，銀行タイプごとに異なる値を与える．一般銀行（中小銀行や地域銀行）については共通の初期値 x_0 を設定し，一方でメガバンクについては，先行的な投資余力を有するという実態を反映し，より高い採用率 x_0^{mega} からスタートする．この設定により，導入速度や政策効果の比較を現実的に表現する．

6.5.6 収益と税制 $(R_{i,t,p}^{DX}, T_{i,t,p}, \tau, \tau^{PQC}, x^{thd})$

各銀行が行った DX 投資 $I_{i,t,p}^{DX}$ からは，パラメータ r_i^{DX} に比例した収益が得られると仮定する．これに対して法人税率 τ が適用され，税額 $T_{i,t,p}$ が算出される．ただし，メガバンクが PQC 採用率 $x_{i,t,p}$ を閾値 x^{thd} 以上に引き上げた場合には，優遇税率 τ^{PQC} が適用され，軽減税額が計算される．これにより「早期に PQC 対応を進めた銀行には税制上のメリットを与える」という政策インセンティブをモデル化する．

6.5.7 サイバー損失 $(L_{t,p}^{cyber}, R_t^Q, \omega_{ij}, \lambda)$

PQC 未対応部分が残っている場合には，その割合に応じてサイバー攻撃による損失 $L_{t,p}^{cyber}$ が発生する．この損失は，時点 t の量子脅威の大きさ R_t^Q や，銀行間のネットワーク強度 ω_{ij}，連鎖リスク率 λ などのパラメータを通じて拡大しうる．つまり，単独の銀行が対応を怠った場合で

も，ネットワークを介して他の銀行にも悪影響が及び，システム全体の損失として現れる構造とする．

6.6 目的関数 (Objective Function)

経済主体の行動が単なる費用削減だけでなく，収益機会の最大化によっても動機付けられることを反映するため，目的にはシステム全体の正味利益の最大化を設定する．

6.6.1 総利益 (Total Profit)

全ての銀行の DX 投資から得られる税引後収益の合計．

$$\text{Total Profit}_t^p = \sum_{i \in I} N_i \cdot (R_{i,t,p}^{DX} - T_{i,t,p}) \qquad (1)$$

6.6.2 総損失 (Total Loss)

PQC 投資コスト，サイバー損失，および規制ペナルティの合計．

$$\text{Total Loss}_t^p = \underbrace{\left(\sum_{i \in I} N_i \cdot I_{i,t,p}^{\text{PQC}} \right)}_{\text{PQC 投資コスト}} + \underbrace{L_{t,p}^{\text{cyber}}}_{\text{サイバー損失}} + \text{規制ペナルティ} \qquad (2)$$

6.6.3 正味利益 (Net Profit)

各期のシステム全体の正味利益 NetProfit_t^p を，総利益から総損失を差し引いたものとして定義する．

$$\text{NetProfit}_t^p = \text{Total Profit}_t^p - \text{Total Loss}_t^p \qquad (3)$$

6.6.4 正味価値の最大化

これらを用いて，システム全体の正味利益の現在価値を最大化する目的関数を設定する．具体的には，t 期後の価値を現在価値に割り引く NPV の考え方に基づき，割引率 δ による現在価値を求めつつ，全期間の NetProfit を合計し，その値が最大化する条件を計算する．

$$\max Z_{\text{profit}} = \sum_{t \in T} \sum_{p \in P} \frac{1}{(1+\delta)^{t-1}} \cdot [\text{NetProfit}_t^p] \qquad (4)$$

6.7 構築した均衡モデル設定

導出する式は，I：銀行（3 種），T：時間（四半期 t_1–t_{20} = 5 年），P：政策（3 種）の 3 インデックスについて，非線形計画問題（NLP）を解く（$|I| \times |T| \times |P| = 180$ のスケールで定式化，変数数・制約条件数はいずれも 1000 以上）．

7. 分析結果

Q-day リスクは縦軸は正規化したリスク水準，横軸に時系列を示している．時間の経過とともにリスクは単調増加し，Q-day に近づくほど増加が加速，リスクが後半で急伸する傾向を示す概念として設定している．

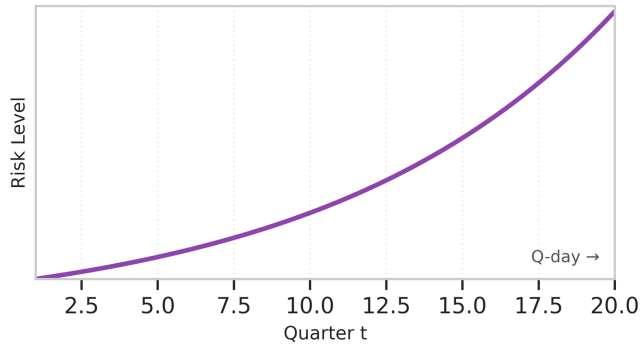

図 4 Q-Day リスクのイメージ
Fig. 4 Image of the risk by Q-day

7.1 基礎事例

以下の図は，通常条件において，PQC 対応進行状況と，それによる量子リスクの減少を示した 1 ケースである．

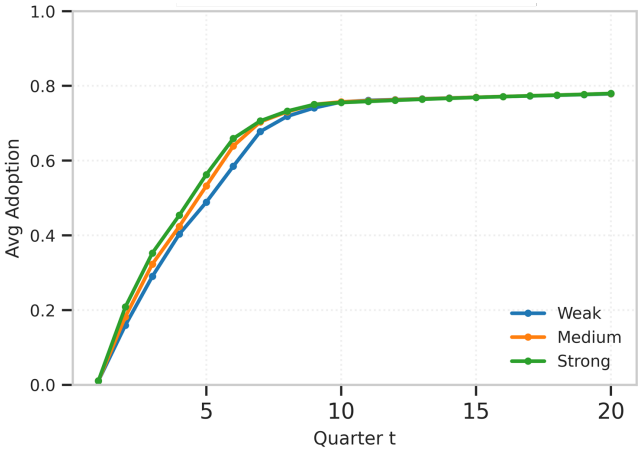

図 5 PQC 対応状況（通常ケース）
Fig. 5 PQC Migration Status: Baseline Scenario

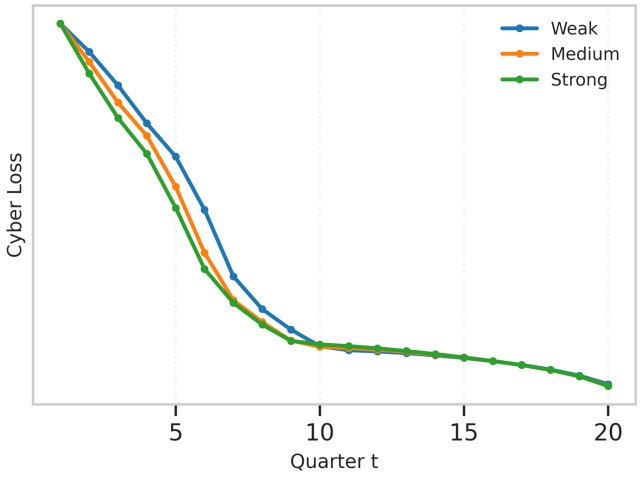

図 6 サイバー損失（通常ケース）
Fig. 6 Cyber Loss: Baseline Scenario

ここからは，直感的な想像のとおり，政策の強制によって普及が進行しやすいという状態が確認される．

7.2 モデル条件による数値変動

7.2.1 保守コスト増のケース

次いで，同パラメータ設定のもと，保守コスト率を約 10 %増やしたケースを示す．

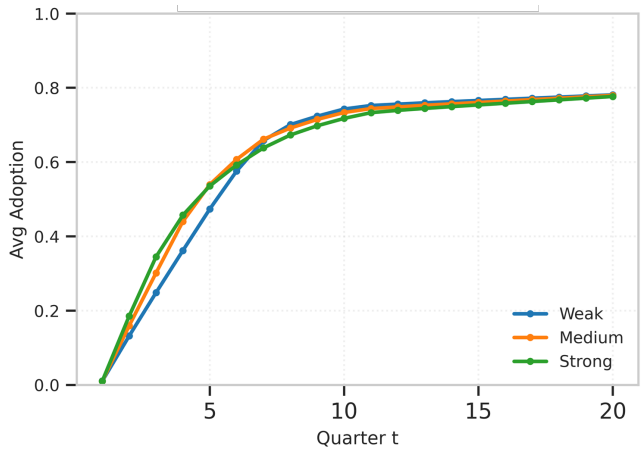

図 7 PQC 対応状況（保守コスト大のケース）

Fig. 7 PQC Migration Status: High Maintenance Cost Scenario

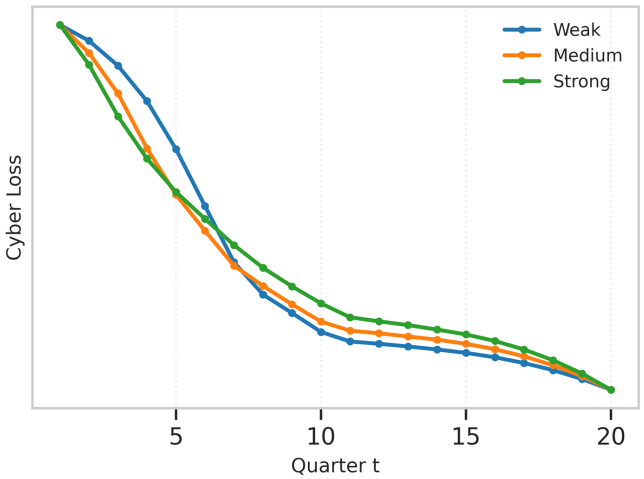

図 8 サイバー損失（保守コスト大のケース）

Fig. 8 Cyber Loss: High Maintenance Cost Scenario

この場合，継続的に保守コストが大きく，かつ DX 投資の一定以上の実施等の条件から，最終的に政策を強制しない Waek での事例が進行するケースである．

7.2.2 DX 投資推進のケース

続いて，更に一事例，DX 投資の最低比率を約 10 %程度増やしたケースである．なお本シナリオは，DX 投資により**最終利益が倍程度**である．

PQC 対応を推進しないことへのペナルティが存在するものの，DX 投資を推進することによるメリットが大きくあることから，政策として Strong である方が PQC 移行が進みずらいという現象になるケースである．

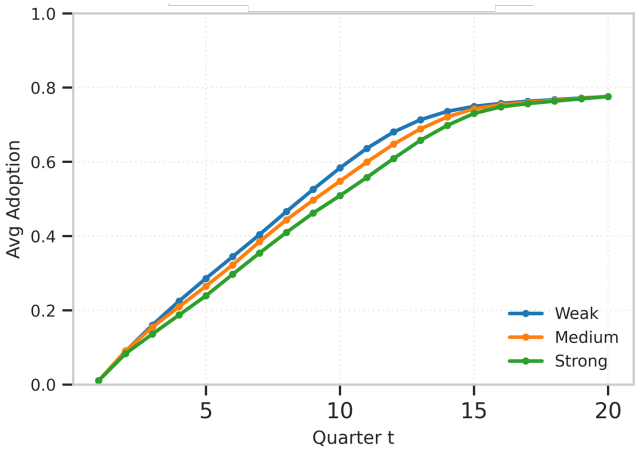

図 9 PQC 対応状況（DX 投資を推進するケース）

Fig. 9 PQC Migration Status: Accelerated DX Investment Scenario

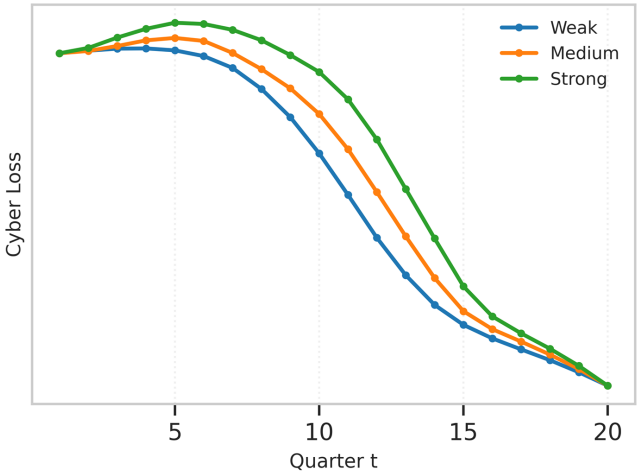

図 10 サイバー損失（DX 投資を推進するケース）

Fig. 10 Cyber Loss: High Maintenance Cost Scenario

8. 考察

本研究では，サイバー投資の妥当性を定量的に評価することを目的としたモデルの構築を試みた．PQC 移行を前倒しするインセンティブとして税制優遇を導入し，採用度合いに応じて実効税率が逓減する設計とし，罰則は導入率の低さに応じて時間とともに作用する加算コストとして実装した（政策強度とは独立に設定している）．

そのうえで，介入要素としての「政策」を PQC 投資コスト逓減に資するインセンティブとして強・中・弱の三水準を設定し，これらの強度差が投資と採用の進行に及ぼす影響を数理最適化により求めるモデルを構築した．

検証の結果，一般には強い政策ほど普及が早まり，曲線は交わりにくい直感的な結果となるが，予算制約や DX の最低投資，ネットワーク効果等の複合要因により，変動する場面も確認された．これは，罰則が存在しても，DX 投資収益性が相対的に勝る条件下では，政策による強制より

も投資合理性が採用を牽引し得ることを示唆すると考えられる．

このように，合理的な意思決定を前提とする全体最適化により，シナリオに沿った分析結果を導くことができるという点で，本研究を続行する意義があると考えている．

9. 結論と今後の課題

サイバーセキュリティ投資における意思決定のモデルを検討するため，応用一般均衡モデリングを用いての分析を試みた． 動的マクロ経済学分野において本ツールが一般的な適用手法であるため，その基礎モデルとして用いることが妥当であるという考えの元実施し，傾向を分析することが出来たと考えている．

マクロ経済学観点からの研究として，パラメータは精緻化した数値を設定化しつつも，モデルをシンプルに表現することとのバランスは重要であり，引き続き改善を実施し応用モデルへの発展を試みたい．

一方，本手法には技術的な制約がある． 具体的には，系全体を宣言的に条件定義し，結果的に表現されうる均衡を計算する事になることに起因するものであり，本稿で実施したように，時系列を表現する際にはその全体での最適化を計算することが限界になること，目的関数には全体の最大化（または最小化等）を設定することである．そのため，個別のインスタンス（銀行個社）の行動には着目することが困難である．

そこで，今後の分析においては，特定の時系列における意図を表現できる Agent-based modeling（ABM）（例として [11] などで解説例あり）を用いて表現するように拡張し，研究を続けることを計画している．

参考文献

[1] 内閣サイバーセキュリティセンター (NISC)：重要インフラのサイバーセキュリティの確保に関する主な資料, https://www.nisc.go.jp/policy/group/infra/siryou/. 最終アクセス日: 2025 年 8 月 20 日.

[2] 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 報告書, (2024).

[3] 内閣サイバーセキュリティセンター (NISC)：重要インフラのサイバーセキュリティに係る行動計画の概要 (2022).

[4] Gordon, L. A. and Loeb, M. P.: The economics of information security investment, *ACM Transactions on Information and System Security (TISSEC)*, Vol. 5, pp. 438–457 (2002).

[5] 国土交通省国土交通政策研究所：国土交通政策研究第 13 号 政策効果の分析システムに関する研究 －国内航空分野における規制緩和及び航空ネットワーク拡充に関する分析－, (2002).

[6] Dixon, P., Giesecke, J., Nassios, J. and Rimmer, M.: Finance in a global CGE model: the effects of financial decoupling between the U.S. and China, *Journal of Global Economic Analysis*, Vol. 6, No. 2, pp. 1–30 (2021).

[7] 小梶 顯義：マクロ経済学モデルに基づくサイバー攻撃に起因する直接被害と波及被害に関する分析と考察，博士論文，情報セキュリティ大学院大学 (2023).

[8] 総務省：産業連関表，https://www.soumu.go.jp/toukei_toukatsu/data/io/.

[9] GAMS Development Corporation: GAMS - General Algebraic Modeling System, https://www.gams.com.

[10] GAMS Development Corporation: GAMSPy, https://gamspy.readthedocs.io/en/latest/.

[11] 荻林成章：ABM による知の蓄積方法論の提案と簿記会計を内包した 経済シミュレーションプログラムの紹介―ABM による複雑系システムにおける社会現象メカニズムの解明―，https://ogi-lab.com/wp-content/uploads/MIMS_ABM_230901.pdf (2023).