

# 金融研究

2026年4月 / 第45巻第2号

---

量子耐性を有するシステムの実現に向けて：  
金融分野における取組みと対応の推奨事項 ..... 宇根正志

貿易取引の為替リスクヘッジにおける  
ディープ・ヘッジングの活用 ..... 三輪幸哉

---

日本銀行金融研究所

## 日本銀行 金融研究所

Institute for Monetary and Economic Studies (IMES)

Bank of Japan

### 特別顧問

星 岳雄 東京大学教授

### 国内顧問

大橋和彦 一橋大学・東京科学大学教授

粕谷 誠 東京大学教授

神田秀樹 東京大学名誉教授

塩路悦朗 中央大学教授

福田慎一 東京都立大学特任教授

### 海外顧問

**Markus K. Brunnermeier**

Edwards S. Stanford Professor of Economics, Princeton University

**Athanasios Orphanides**

Professor of the Practice, Global Economics and Management, Massachusetts Institute of Technology

### 所 長

渡辺真吾

本誌に掲載されている論文等の内容や意見は、執筆者個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではありません。

# 金融研究

2026年4月/第45巻第2号

## 目次

- |    |                                             |      |
|----|---------------------------------------------|------|
| 1  | 量子耐性を有するシステムの実現に向けて：<br>金融分野における取組みと対応の推奨事項 | 宇根正志 |
| 25 | 貿易取引の為替リスクヘッジにおける<br>ディーブ・ヘッジングの活用          | 三輪幸哉 |
| 57 | 金融研究所の概要等                                   |      |



# 量子耐性を有する システムの実現に向けて： 金融分野における 取組みと対応の推奨事項

うねまさし  
宇根正志

## 要 旨

金融分野では、量子コンピュータ開発の今後の進展を展望し、量子コンピュータによる暗号アルゴリズムへのリスクにどのように対応していくかに関心が集まっている。大規模かつ実用的な量子コンピュータが実現すると、現在普及している公開鍵暗号のセキュリティが低下し、それによって保護されている情報が解読される可能性がある。こうしたリスクへの対応として、既存の公開鍵暗号を量子コンピュータでも解読困難な耐量子計算機暗号に移行させていくことが求められる。近年、暗号アルゴリズムの移行に関する調査報告や提言が金融関連の団体や当局から相次いで発表されており、いずれも、リスク低減に向けて暗号アルゴリズムの移行に関する検討の早期着手が望ましいとしている。そのうえで、各金融機関のシステムにおける暗号アルゴリズムの使用状況の調査・管理（暗号インベントリの整備）、長期間保護が必要な情報の特定とリスクの評価、対応すべきシステムの優先順位付け、暗号アルゴリズムを円滑に切り替える仕組みの実装（暗号アジリティの向上）を推奨事項として挙げている。また、金融機関が連携し、金融業界としてのリスク低減計画を策定することも推奨している。各金融機関においては、こうした推奨事項を踏まえつつ、量子耐性を有するシステムの実現に向けて適切に対応する必要がある。

キーワード： 暗号アジリティ、暗号アルゴリズム移行、暗号インベントリ、公開鍵暗号、耐量子計算機暗号、リスク低減計画、量子コンピュータ

.....  
本稿は 2024 年 11 月 5 日時点の情報に基づいて作成した。本稿の作成に当たっては、松本泰フェロー（特定非営利活動法人日本ネットワークセキュリティ協会）から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

宇根正志 日本銀行金融研究所参事役（E-mail: masashi.une@boj.or.jp）

## 1. はじめに

暗号アルゴリズムは、金融サービスや金融業務のセキュリティを支える重要な要素技術として広く用いられている。暗号アルゴリズムの用途として、例えば、ATMにおけるICキャッシュカードの認証、インターネット・バンキングやモバイル・バンキングにおける通信データの暗号化や認証、金融機関間や金融機関とフィンテック事業者との間の通信データの暗号化や認証が挙げられる。また、出張中や在宅勤務中の職員の端末と金融機関のシステムとの間の通信データを保護する手段としても用いられている。業務でクラウドを使用している場合には、クラウドと金融機関の端末・サーバとの間の通信データや、クラウドのデータを保護する手段として暗号アルゴリズムが採用されている。

こうした暗号化や認証において用いられている公開鍵暗号の代表的なアルゴリズム（RSAや楕円曲線暗号）には、量子コンピュータ<sup>1</sup>による解読のリスクがある（宇根・菅 [2021]）<sup>2</sup>。RSAや楕円曲線暗号を効率的に解読することができるレベルの量子コンピュータ（CRQC）<sup>3</sup>が実現するタイミングは明確になっていない<sup>4</sup>。しかし、仮に、攻撃者がCRQCを用いることができるようになれば、金融取引や顧客に関する情報（暗号化されていたもの）が解読されたり、金融機関のシステムにアクセスする際の認証が破られて不正な処理が実行されたりする可能性がある。したがって、このようなリスクが許容できないと判断されるシステム（量子脆弱性を有するシステム）においては、量子コンピュータでも解読困難な暗号アルゴリズム<sup>5</sup>に切り替えるなどのリスク低減策を事前に適用し、CRQCに対しても十分なセキュリティを確保できるシステム（量子耐性を有するシステム）を実現する必要が

- .....
- 1 量子コンピュータは量子力学の原理を活用したコンピュータの総称であり、超伝導回路方式などさまざまな実現方式の量子コンピュータの研究開発が活発に進められている。
  - 2 一定の規模や機能を有する量子コンピュータを用いて効率よく解読する方法が知られている暗号アルゴリズムは、量子脆弱性を有する（quantum-vulnerable）暗号アルゴリズムと呼ばれる。
  - 3 量子脆弱性を有する暗号を現実的な時間と費用によって解読することが可能なレベルの量子コンピュータはCRQC（cryptographically relevant quantum computer または cryptanalytically relevant quantum computer）と呼ばれている。
  - 4 CRQCが実現する可能性のある時期に関して、ドイツのセキュリティ当局であるBSI（Bundesamt für Sicherheit in der Informationstechnik）が2024年に発表した調査報告では、2040年頃までにCRQCが実現する可能性が示唆されている（Bundesamt für Sicherheit in der Informationstechnik 2025）。
  - 5 こうした暗号アルゴリズムは、量子耐性を有する（quantum-resistant、quantum-safe、quantum-secureなど）暗号アルゴリズムと呼ばれている。アメリカのNIST（National Institute of Standards and Technology）は量子耐性を有する暗号アルゴリズム（群）を標準化しており、それらをPQC（post-quantum cryptography）と呼んでいる。PQCは耐量子計算機暗号と訳されるケースが多い。なお、NISTは、セキュリティ技術をはじめとする各種先端技術の研究開発や標準化を行う商務省傘下の研究機関であり、連邦政府機関が使用する情報技術の標準規格FIPS（Federal Information Processing Standards）の策定を担っている。

ある。

CRQC によるリスクへの対応は金融分野に限られるものではない。海外の主要な国の政府機関では、CRQC によるリスクの評価やリスク低減策に関するガイドランスやホワイト・ペーパーを発表する動きが 2020 年頃からみられている（宇根 [2023]）。アメリカ連邦政府は、2035 年を目途に量子コンピュータによるリスクを可能な限り低減する方針を 2022 年 5 月に表明し、耐量子計算機暗号の標準化、量子脆弱性を有する暗号アルゴリズムの使用停止など、リスク低減に向けたロードマップを発表している（White House 2022）。欧州では、欧州委員会が欧州連合加盟各国に対して、量子耐性を有する暗号アルゴリズムの実装ロードマップを 2026 年 4 月までに策定することを、2024 年 4 月に勧告している（European Commission 2024）。また、欧州連合に加盟している 18 の国のセキュリティ当局は、各国の行政・産業界に向けて、リスク対応に関する検討への早期着手を促す声明を 2024 年 11 月に共同で発表している（Secure Information Technology Center Austria *et al.* 2024）。

このように、欧米では、CRQC が登場するタイミングが不透明ななかにあっても、なるべく早期にリスクを排除するという観点から、量子耐性を有するシステムの実現を政策として促進している。今後、欧米の企業や組織（日本企業の海外支店なども含む）が量子耐性を有するシステムに移行していくとすれば、欧米の企業や組織と通信する必要がある日本国内の企業や組織も量子耐性を有するシステムに移行しなければならなくなる可能性がある。こうした対応に遅れた場合、CRQC によるリスクにさらされるだけでなく、欧米の企業や組織と通信できなくなるというネットワークの接続性の問題にもつながりうることに留意すべきであろう。

金融分野においても、CRQC によるリスクにどのように対応するかについて関心が高まっている。海外の金融関連の団体や当局から、リスク対応に関する調査報告や提言が最近相次いで発表されている。NIST が耐量子計算機暗号の標準化候補となる暗号アルゴリズムの募集を開始した 2016 年 12 月以降に絞ると、主な調査報告や提言として以下が挙げられる。

- ① 2019 年 1 月：ASC X9, Inc.<sup>6</sup> が暗号メッセージ構文<sup>7</sup>（CMS: cryptographic message syntax）に関する報告書を発表した（Accredited Standards Committee X9, Inc. 2019）。
- ② 2022 年 11 月：ASC X9, Inc. が CRQC によるリスクに関する報告書を発表した（Accredited Standards Committee X9, Inc. 2022）。
- ③ 2023 年 3 月：FS-ISAC<sup>8</sup> が CRQC によるリスクへの対応に関する提言を発表し

6 ASC X9, Inc.（Accredited Standards Committee X9, Inc.）はアメリカ国内における金融サービスに関連する標準規格を策定する非営利団体である。

7 暗号メッセージ構文とは、暗号アルゴリズムによる処理（デジタル署名生成、ハッシュ化、暗号化など）の対象となるメッセージの構成要素やフォーマットを指す。

8 FS-ISAC（Financial Services Information Sharing and Analysis Center）は、金融機関におけるサイバー

た（Financial Services Information Sharing and Analysis Center 2023）。

- ④ 2023年6月：国際決済銀行・フランス銀行・ドイツ連邦銀行が量子耐性を有する暗号アルゴリズムを実装・テストするプロジェクト Leap の報告書を発表した（Bank for International Settlements, Banque de France, and Deutsche Bundesbank 2023）。
- ⑤ 2023年11月：UK Finance Limited<sup>9</sup>が CRQC によるリスクへの対応に関する提言を発表した（UK Finance Limited 2023）。
- ⑥ 2024年1月：世界経済フォーラム<sup>10</sup>が CRQC によるリスクに対応するための規制や国際協調に関する提言を発表した（World Economic Forum 2024）。
- ⑦ 2024年2月：シンガポール金融管理局が CRQC によるリスクへの対応に関して金融機関向けの勧告を発表した（Monetary Authority of Singapore 2024）。
- ⑧ 2024年9月：G7 サイバー・エキスパート・グループ<sup>11</sup>が CRQC によるリスクへの対応に関する提言を発表した（金融庁 [2024]；G7 Cyber Expert Group 2024）。
- ⑨ 2024年10月：FS-ISAC が暗号アルゴリズムを円滑に切り替える体制の整備に関するガイダンスを発表した（Financial Services Information Sharing and Analysis Center 2024）。
- ⑩ 2024年11月：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<sup>12</sup>が報告書を発表した（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 [2024a]）。

上記の⑨は、システムにおいて使用する暗号アルゴリズムを円滑に切り替えることを可能にする性質である暗号アジリティ（cryptographic agility）をテーマとしているが、その他の調査報告においても暗号アジリティの重要性が指摘されている。

金融機関においては、こうした報告書などを参照しつつ、CRQC によるリスクに適切に対応していく必要がある。

---

セキュリティや各種インシデントへの対応力の向上を目的として、関連する情報を金融機関間で共有する枠組みなどを提供する国際的な非営利団体である。

- 9 UK Finance Limited はイギリスにおける金融分野の業界団体であり、金融業界内での連携の支援、金融サービスに関連する規制や金融業界内のルールの立案、政府を含むステークホルダーとの調整などの役割を担っている。
- 10 世界経済フォーラム（World Economic Forum）は、社会の発展のために、政治、産業、学術などの各界のリーダーや有識者が課題解決に向けて協力するための枠組みを提供する国際的な非営利団体である。
- 11 G7 サイバー・エキスパート・グループ（G7 Cyber Expert Group）は、サイバーセキュリティに関するポリシーや戦略の調整、関連する情報の共有、インシデント対応などを担当する G7 のワーキング・グループである。
- 12 この検討会（事務局：金融庁）は、金融機関の実務者や有識者が預金取扱金融機関による耐量子計算機暗号への移行における推奨事項、課題、留意点を検討するために、2024年7月から10月にかけて開催された。

本稿では、金融関連の団体や当局による調査報告や提言におけるリスク低減の方針や推奨事項を説明する。

## 2. 金融分野における主な調査報告・提言

1 節で列挙した 10 件の調査報告・提言のうち、②と③は宇根 [2023] で紹介されていることからここでは割愛し、残りの 8 件を紹介する。

### (1) ASC X9, Inc. による暗号メッセージ構文に関する報告

ASC X9, Inc. は、暗号メッセージ構文の暗号アルゴリズムへの CRQC による影響と対応に関する報告書を 2019 年 1 月に発表している (Accredited Standards Committee X9, Inc. 2019)。報告書では、公開鍵暗号に基づくデジタル署名と鍵共有、共通鍵暗号を対象としている。

#### イ. デジタル署名

報告書では、署名アルゴリズムが量子脆弱性を有している場合、CRQC によって署名検証鍵から署名生成鍵が推定され、署名の偽造によって、メッセージの一貫性確認や認証が無効化されうるとしている。また、量子脆弱性を有する署名アルゴリズムが用いられている電子証明書も偽造されうると指摘している。

このようなリスクへの対応として、量子耐性を有していると十分信頼できる署名アルゴリズムを実装することを推奨している。そうした署名アルゴリズムを採用できない過渡期においては、量子耐性を有すると期待されている署名アルゴリズムを既存の署名アルゴリズムと組み合わせて用いる手法 (ハイブリッド手法 (hybrid method)<sup>13</sup>) を推奨している。双方の暗号アルゴリズムによってそれぞれ署名を生成し、署名検証時にはこれらの検証結果を用いて署名の正当性を判断する<sup>14</sup>。

また、別の対応として、物理的にアクセスを制御している場所に署名対象データを保管する方法や、特定の時点で署名対象データが存在していたことを第三者が認めた証となるデータ (タイムスタンプ<sup>15</sup>) を取得・保管する方法も紹介している。

13 ハイブリッド手法は、組み合わせられた暗号アルゴリズムのうち、少なくとも 1 つが安全であれば、保護対象のデータの安全性を維持することができるように設計されている手法である。

14 例えば、双方の署名アルゴリズムのうち、署名検証時に危殆化していないものによって生成された署名に着目し、その検証が成功すれば署名を正当とみなすという方法が挙げられる。

15 タイムスタンプの各種手法については、宇根・松浦・田倉 [2000] を参照されたい。

## ロ. 鍵共有

報告書は、メッセージ本体の暗号化には共通鍵暗号を使用し、その暗号鍵（セッション鍵）を公開鍵暗号によって通信当事者間で共有する形態を前提としている。そのうえで、セッション鍵の共有方法として次の3つを説明している。

- 通信当事者の一方がセッション鍵を生成し、それを通信相手の公開鍵によって暗号化したうえで通信相手に配送する（鍵配送〈key transport〉）。
- 通信当事者が（自分のプライベート鍵を用いて生成した）公開可能なデータをそれぞれ通信相手に送信し、受信したデータと自分のプライベート鍵からセッション鍵を生成する（鍵合意〈key agreement〉）。
- 鍵カプセル化メカニズム（KEM）<sup>16</sup>を使用する。

報告書は、いずれの方法においても、量子脆弱性を有する暗号アルゴリズムが使用されている場合、CRQCを用いる攻撃者によって公開鍵からプライベート鍵が推定され、保護対象のメッセージが盗取されうるとしている。

対応の方針として、報告書は、デジタル署名の場合と同じくハイブリッド手法の採用を挙げている。特に、HNDL 攻撃<sup>17</sup>による暗号解読のリスクが許容できない場合には、多重防御の観点からハイブリッド手法を可能な限り早期に採用することが望ましいとしている。ハイブリッド手法の採用が間に合わない場合には、インターネットとは別の物理的なチャネルなどを介して、セッション鍵の元となるデータを通信当事者間で共有する方法（事前共有鍵〈pre-shared key〉を用いる方法）を紹介している。

また、量子耐性を有する暗号アルゴリズムの多くが鍵カプセル化メカニズムであり、NISTの標準化対象になっていることなどから、鍵配送、鍵合意ではなく、鍵カプセル化メカニズムを推奨している。

## ハ. 共通鍵暗号

報告書は、共通鍵暗号への影響が公開鍵暗号の場合ほど大きくないとしたうえで、セキュリティを維持するために暗号鍵のサイズを約2倍に伸長することを推奨している。

.....  
16 KEM (key encapsulation mechanism) は公開鍵暗号の使用形態の1つである。セッション鍵の共有の流れは、①まず、送信者が受信者の公開鍵を入手する、②送信者は公開鍵などから暗号文とセッション鍵を生成する、③送信者は暗号文を受信者に送信する、④受信者は暗号文と自分のプライベート鍵からセッション鍵を生成するというものである。

17 HNDL (harvest now, decrypt later) 攻撃は、CRQCが登場する前から暗号文を収集しておき、CRQCが登場して使用可能になったタイミングで収集した暗号文を一気に解読するという攻撃である。SNDL (store now, decrypt later) 攻撃、ハーベスト攻撃とも呼ばれる。

## (2) 国際決済銀行・フランス銀行・ドイツ連邦銀行のプロジェクト報告

国際決済銀行、フランス銀行、および、ドイツ連邦銀行は、量子耐性を有する暗号アルゴリズムを中央銀行間の通信ネットワーク・システムに実装・テストするプロジェクト Leap の報告書（フェーズ 1）を 2023 年 6 月に発表した（Bank for International Settlements, Banque de France, and Deutsche Bundesbank 2023）。

### イ. 背景

報告書では、金融機関の業務やサービスで用いられる通信データのセキュリティが暗号プロトコルに大きく依存しているとしたうえで、量子コンピュータを悪用するサイバー攻撃に暗号プロトコルがさらされる可能性があるとの認識を示している。10 年以上の長期間にわたって秘匿する必要があるデータ、特に金融機関以外の場所（クラウドなど）で保管されているものについて、HNDL 攻撃の脅威が既に存在しうることから早急な対応が必要であるとしている。対応として、報告書では、量子耐性を有するシステムを実現する必要があるとしている。また、そうしたシステム向けの新しい暗号プロトコルや暗号アルゴリズムの開発・標準化が NIST などによって進められていることを紹介している。

### ロ. プロジェクトの概要

報告書では、プロジェクトのフェーズ 1 の目標として、量子耐性を有する主な暗号アルゴリズムを実際の通信ネットワーク・システムで動作させ、実装性を把握することを挙げている。具体的には、①暗号アルゴリズムの円滑な切替え（暗号アジリティ）、②処理の速度や安定性（性能〈performance〉）、③セキュリティ・パラメータ<sup>18</sup>を変化させた際の処理の可否（セキュリティ〈security〉）によって実装性を評価している。

プロジェクトでは、通信ネットワーク・システムとして、フランス銀行とドイツ連邦銀行を接続する暗号通信路<sup>19</sup>を使用している。通信当事者は、通信相手を認証した後、共通鍵暗号（AES）用のセッション鍵を公開鍵暗号によって共有し、それを用いてメッセージ（サイズは約 1 メガ・バイト）本体を暗号化して通信する。量子耐性を有する暗号アルゴリズムとして、NIST の標準化対象の暗号アルゴリズム（CRYSTALS-Kyber、CRYSTALS-Dilithium、SPHINCS+、Falcon）に加えて、ドイツ

18 NIST の標準化対象の暗号アルゴリズムでは、5 段階のセキュリティ・レベルが設定されており、それぞれのレベルを達成するためのセキュリティ・パラメータが定められている。

19 暗号通信路には、広く使用されている IPsec VPN が採用されている。IPsec VPN は、通信機器間での暗号化や認証を実現する標準プロトコル IPsec（IP Security）を用いて仮想的な専用の通信網 VPN（virtual private network）を実現する技術である。

のセキュリティ当局などが推奨している鍵カプセル化メカニズムの暗号アルゴリズム FrodoKEM を選択し、これらを市販の暗号ライブラリによって実装している。

上記の暗号アルゴリズムはハイブリッド手法で実装されている。セッション鍵の共有では、既存の暗号アルゴリズムとして RSA を使用し、量子耐性を有する暗号アルゴリズムとして CRYSTALS-Kyber と FrodoKEM を使用している。通信相手の認証に用いられるデジタル署名に関しては、既存の署名アルゴリズムとして RSA を使用し、量子耐性を有する署名アルゴリズムとして CRYSTALS-Dilithium、SPHINCS+、Falcon を使用している。

## ハ. 結果

暗号アルゴリズムの切替えに関して、セッション鍵の共有では、通信当事者間で使用する暗号アルゴリズムを決定する機能が暗号ライブラリに設定されていたため、円滑に切り替えることができた。デジタル署名では、署名アルゴリズムを識別する機能が暗号ライブラリに設定されておらず、署名アルゴリズムを識別する機能を手動で設定した。

処理速度に関して、主に認証・鍵共有の処理と暗号化メッセージの通信にかかる時間をそれぞれ測定した。認証・鍵共有の時間は、既存の暗号アルゴリズム（鍵共有・署名ともに RSA）を使用する場合よりも、量子耐性を有する暗号アルゴリズムを用いる場合（例えば、鍵共有に CRYSTALS-Kyber、署名に CRYSTALS-Dilithium を使用）において長くなった<sup>20</sup>。暗号化メッセージの通信の時間は、いずれの場合も AES を使用したことからはほぼ同じであった。

処理の安定性に関して、暗号通信路の機能が正常に維持されているか否かを 1 時間ごとに確認したところ、24 時間正常であった。

セキュリティ・パラメータを変化させた際の処理の可否に関して、量子耐性を有する暗号アルゴリズムを異なるセキュリティ・パラメータのもとでそれぞれ動作させた結果、いずれのパラメータでも正常に動作した。また、相対的に高いセキュリティ・レベルに対応するパラメータで動作させた場合、処理速度が低下した。これらを踏まえて、実装時にはセキュリティ・レベルと処理速度のトレードオフに留意する必要があるとしている。

## 二. 暗号アルゴリズム移行に向けた対応と今後のプロジェクト

報告書では、今後、中央銀行やその他の金融機関が暗号アルゴリズムの移行において直面する課題として、暗号アルゴリズムの使用状況の調査、量子脆弱性を有する暗号アルゴリズムの使用の特定、リスク評価などを挙げている。また、暗号アル

20 量子耐性を有する暗号アルゴリズムの処理速度に関しては、鍵共有では、CRYSTALS-Kyber が FrodoKEM よりも優れていた。署名では、CRYSTALS-Dilithium と Falcon が同程度であったほか、これらと比べると SPHINCS+ が劣っていた。

ゴリズムの移行が、今回のプロジェクトのような暗号通信路だけでなく、さまざまなシステムにおいて求められるとしたうえで、各種のシステムに対応する新しい暗号プロトコルの開発、それらを実現するハードウェアやソフトウェアの導入、量子耐性を有する暗号アルゴリズムに関する専門的なスキルをもつスタッフの育成・確保が必要であるとの見方を示している。そして、こうした取組みに要する時間を十分確保するという観点から、暗号アルゴリズム移行に向けた検討の早期着手が重要であるとしている。

本プロジェクトの今後について、報告書では、量子耐性を有する暗号アルゴリズムを複雑なシステム環境（例えば、中央銀行とその他の組織との間の通信ネットワーク・システム）において実装・テストすることが考えられるとしている。

### (3) UK Finance Limited による提言

UK Finance Limited は、2023 年 11 月に発表した提言において、量子コンピュータが金融商品のポートフォリオの最適化などに貢献しうると期待されている一方で、金融サービスで使用されている暗号アルゴリズムに深刻な影響を与えるリスクがあるとしている（UK Finance Limited 2023）。そのうえで、量子コンピュータによるメリットを享受するためにも、金融業界全体としてリスクに対応する必要があるとしている。

#### イ. CRQC を用いる攻撃によって生じうる事象の例

提言では、金融機関が使用する暗号アルゴリズムが CRQC によって解読された場合、以下の事象が生じうるとしている。

- ① 金融機関が保持している個人情報（personally identifiable information）が盗取される。
- ② ホールセール決済に関連するシステムにおいて認証が破られ、なりすましによる不正送金などが行われる。
- ③ 金融機関が公開している API（application programming interface）における認証や認可を実行するプロトコルが不正に操作され、なりすましによる不正な金融取引が実行されたり、暗号化されたデータが解読されたりする。
- ④ ブロックチェーンにおける初期ブロック（genesis block）が偽造され、それ以降に生成されたすべてのブロックの内容が信頼できないものとなる。
- ⑤ 金融サービス向けのシステムやインフラの管理者権限が奪取され、システムなどが不正に操作される。
- ⑥ リテール決済のシステムにおける認証が無効化され、なりすましなどによって

不正な取引が実行される。

- ⑦ ソフトウェアやファームウェアの一貫性を確認することができなくなり、不正なソフトウェアなどが金融機関のシステムに組み込まれて不正な動作を引き起こす。
- ⑧ 金融機関内部で管理されている各種データベースが改変される。
- ⑨ 金融取引において参照される公的なデータベース（登記簿のデータベースなど）が改変される。

#### ロ. 金融業界レベルでの検討

提言では、上記の事象への対策として、金融業界のステークホルダーが連携して業界横断的なタスクフォースを設置し、金融業界レベルの移行計画（quantum safe transition plan）を策定することを推奨している<sup>21</sup>。そして、金融業界レベルの移行計画に基づいて各金融機関が自社の移行計画を策定するという対応が効率的であるとしている。また、移行計画を策定する過程において想定される主な作業項目として以下を挙げている。

- タスクフォース内で知見を共有し、量子耐性を有する暗号アルゴリズムの使用に関するガイドラインなどを策定する。
- 学界や研究機関と連携し、量子計算技術（quantum computing）や暗号技術における最先端の動向をフォローするとともに、これらに関するスキルを有するスタッフを育成する。
- 政策立案者などと連携し、量子計算技術の適切な使用を促進しつつリスクを低減させるために望ましい政策や規制のフレームワークを検討する。

#### ハ. 個別の金融機関レベルでの検討

提言では、各金融機関が自社の移行計画を策定する際の検討項目として以下を挙げている。

- 自社のシステムにおける暗号アルゴリズムの使用状況、それに関連する業務プロセスや保護対象の情報などを調査して暗号インベントリを整備する。
- 想定される脆弱性の特定、各システムのリスク評価、保護すべき情報やシステムの優先順位付けなどを実施する。
- 量子計算技術の活用やリスク対応に関するロードマップを立案する。ロードマップには、量子耐性を有するシステムへの移行における中間目標、タイムライン、必要なリソースなどを盛り込む。

.....  
21 ここでの移行計画とは、量子耐性を有するシステムやインフラを実現するための活動内容やそのタイムラインを示すものである。提言では、移行計画を効率的に策定するために、業界団体、金融機関、その他のステークホルダーが連携する必要があるとしている。

- 移行計画を策定する際には、必要に応じて、他の金融機関、ベンダー、当局と情報を共有したり共同でプロジェクトを実施したりする。
- 量子耐性を高めるために有効な技術やソリューションの調査・研究・投資を実施する。
- 量子計算技術の動向をフォローし、リスク対応を必要に応じて強化する。
- 量子計算技術のスキルを有する人材を育成するための訓練・研修を実施する。
- 量子計算技術に関連する規制や政策の変更を注視し、必要に応じて、コンプライアンス対応や移行計画を遅滞なく変更する。

#### (4) 世界経済フォーラムによる提言

世界経済フォーラムは、CRQCによるリスクへの対応のあり方に関して、金融当局のスタッフや産業界の有識者による会議を主催しているほか、各国の金融当局に対してサーベイやインタビューを実施している<sup>22</sup>、<sup>23</sup>。2024年1月発表の提言では、こうした会議での講演や議論、サーベイやインタビューの結果を紹介しつつ、リスク対応を進める際には金融当局と金融業界の連携や国際協調が重要であるとしている（World Economic Forum 2024）。

##### イ. 政府や金融業界におけるリスク対応の現状

提言では、政府のリスク対応方針や関連する規制が国によって異なっており、国際的な調和がとれていないほか、一部の国ではリスク対応方針が明確に示されていないとしている。そのうえで、複数の国でビジネスを展開している金融機関は、各国のリスク対応方針や規制に沿った対応を実施する必要があり、複雑な対応を強いられる可能性があるとしている。また、金融機関のシステムが相互に接続され、そのネットワークがグローバルに広がっている点を踏まえると、金融機関のネットワークのセキュリティは其中最も脆弱なポイントに依存することになると説明している。さらに、政府のリスク対応方針や規制の不備は、ベンダーにおける対応（量子耐性を有する暗号ソリューションの提供）の遅れにつながり、金融機関の対応にも影響が及ぶ可能性があるとしている。

.....  
22 これらの活動は FCA（Financial Conduct Authority）との連携によって実施されている。FCA は、イギリスにおける金融市場の機能の維持・向上や消費者の保護を目的として、金融取引に関する規制やガイダンスの策定、金融市場における不正行為の検知・対応、金融機関の認可・検査などを行う公的機関である。

23 会議やサーベイ、インタビューに協力した有識者（43名）の名前と組織（22件）の名称がそれぞれ提言ペーパーの謝辞に記載されている。

## ロ. リスク対応における4つの原則

提言では、今後、金融当局が金融機関と連携してリスク対応を進める必要があるとしたうえで、以下の4つの原則を示している。

- 既存の手段や枠組みの活用 (reuse and repurpose) : CRQC によるリスクに対応するうえで、既存の技術、ベスト・プラクティス、規制など、既に存在する手段や枠組みを活用することをまず検討する。既存の手段などでは不十分な場合、新しい手段を開発するなどの対応を行う必要がある。
- 交渉不要な要求事項の設定 (establish non-negotiables) : 金融当局と金融機関は、リスク対応の際のベースラインとして共に認識している要求事項を明確化する。例えば、リスク対応に関する既存のベスト・プラクティスや国際標準などに規定されている事項などが挙げられる。
- 情報の開示と共有 (increase transparency) : 金融当局と金融機関は、それぞれの戦略やベスト・プラクティス、その他の関連する情報を可能な限り関係者に開示・共有する。
- 分断の回避 (avoid fragmentation) : リスク対応に関連する規制について金融当局間で調整を行い、国や地域によって規制の内容が異なるといった事態をなるべく回避する。

## ハ. リスク対応のロードマップ

提言では、①準備 (prepare)、②明確化 (clarify)、③ガイド (guide)、④移行・監視 (transition and monitor) からなるリスク対応のロードマップの骨子を示している。

- ① 準備 : リスクに対するステークホルダーの認識レベルの向上、スタッフの啓発・スキルアップ、現状把握 (暗号インベントリの整備)、リスク評価、対応の優先順位付けなどを行う。
- ② 明確化 : ステークホルダー間の協力体制の確立、リスク対応に必要な作業・費用・期間などの見積り、既存の規制の再評価などを行う。
- ③ ガイド : リスク対応に関する戦略の検討、必要な規制の検討やベスト・プラクティスの策定などを行う。
- ④ 移行・監視 : リスク対応に関する戦略の実行、暗号アルゴリズムの管理方法やシステムの開発プロセスの見直し、脅威やリスクの状況の監視、先行きを見通した対応や規制の検討などを実施する。

## ニ. 暗号アジリティ

提言では、移行・監視フェーズにおける暗号アルゴリズムの管理方法の見直しに関して、先行きの潜在的なリスク (例えば、新しく実装した暗号アルゴリズムが危殆化する) に対応できるように準備することが重要であるとしている。そのうえで、

実装する暗号アルゴリズムに合わせてシステムの各要素を最適化する (one-size-fits-all approach) のではなく、暗号アジリティを実現する (cryptographic agile approach) という方針を採用することを推奨している。

## (5) シンガポール金融管理局による勧告

シンガポール金融管理局は、2024年2月発表の勧告において、金融機関が取り扱う重要な情報が今後10年でCRQCによる脅威にさらされる可能性があるとしている。そのうえで、システムやインフラに大きな影響を与えることなく量子耐性を有するシステムへ移行するために、金融機関のシステムやインフラにおける暗号アジリティの向上が必要であるとしている (Monetary Authority of Singapore 2024)<sup>24</sup>。

勧告では、金融機関がCRQCによるリスクへの対応として、①量子計算技術の動向の把握とリスク対応の啓発、②暗号インベントリの管理とリスク対応の優先順位付け、③リスク対応の戦略の立案と実行能力の向上を挙げている。

### イ. 量子計算技術の動向の把握とリスク対応の啓発

- 量子コンピュータの開発状況やそれに伴うリスクを監視するとともに、量子耐性を有する暗号アルゴリズムの適用などを検討する。
- 自社の経営層やベンダーに対して、潜在的な脅威やそれへの対応に必要なサポートを説明し理解を得る。
- ベンダーと協力して量子コンピュータによるサプライチェーン・リスク<sup>25</sup>を評価するとともに、量子耐性を有するシステムの実現に資する暗号製品の提供を依頼する。
- 相互依存関係にある他の産業分野においてリスクが顕在化し、それが金融分野に波及して悪影響を被るリスク (systemic quantum risk) を低減させるために、関連する産業分野などと連携して対応する。

.....  
24 勧告では、リスク低減策の選択肢として、量子鍵配送 (quantum key distribution) などの検討も示唆している。量子鍵配送は、専用の通信機器を用いて暗号化や復号のための鍵を通信当事者間で共有する技術であり、データ本体は共通鍵暗号などによって暗号化することを想定している (菅・佐々木 [2024])。

25 金融機関が使用しているシステムの構成要素が複数のベンダーによるサプライ・チェーンのもとで開発・提供されるケースで生じるリスクとみられる。サプライ・チェーンの上流に位置するベンダーが量子脆弱性を有する暗号アルゴリズムを組み込んだソフトウェアを開発し、下流のベンダーに提供していた場合、金融機関は上流のベンダーが組み込んだ暗号アルゴリズムを把握できず、暗号アルゴリズムを切り替えることができないというリスクが想定される。

#### ロ. 暗号インベントリの管理とリスク対応の優先順位付け

- 金融機関における暗号インベントリを管理するとともに、量子脆弱性を有するシステムやインフラを特定する。
- 暗号インベントリにおける管理対象に以下を含めることが望ましい。
  - 使用している暗号アルゴリズムの名称と鍵サイズ
  - 暗号アルゴリズムが組み込まれているシステムやアプリケーションの名称
  - 暗号アルゴリズムによって保護されている情報、および、その情報を保管・管理する責任を負っている主体の名称
- 量子脆弱性を有する暗号アルゴリズムによって保護されているシステムや情報を特定・分類する。
- 上記の分類に基づいて、リスク対応の優先順位付けを行う。優先順位は、システムや情報に求められる機密度、重要度、保護期間、リスクの大きさなどを考慮しつつ決定することが望ましい。
- 既存のシステムやインフラにおける暗号アジリティを評価する。暗号アルゴリズムの移行を妨げる制約（例えば、計算処理能力の限界、インフラの仕様、ベンダーのサポート切れ）がある場合には、そのシステムやインフラをアップグレードして暗号アジリティを高めることを検討する。

#### ハ. リスク対応の戦略の立案と実行能力の向上

- リスク対応に携わるスタッフに、量子耐性を有するシステムの実現に資するスキルを身につけさせる。
- リスク対応の内容との整合性を保つように、金融機関内部のポリシー、技術標準、各種手続きを見直す。
- 量子耐性を有する暗号アルゴリズムへ移行することが困難なシステムなどがあれば、それに対するリスク低減策を立案する。
- 想定よりも早期にリスクが顕在化した場合における対応のシナリオを立案する。
- 可能であれば、量子耐性を有するシステムの概念実験（proof-of-concept trial）を行い、それを導入した際の業務への影響を評価する。

### (6) G7 サイバー・エキスパート・グループによる提言

G7 サイバー・エキスパート・グループは、2024年9月発表の提言において、CRQCによるリスクに対応するための検討に着手することを推奨している（金融庁[2024]；G7 Cyber Expert Group 2024）。

提言では、CRQCが登場した場合、それがHNDL攻撃に悪用され、量子脆弱性

を有する暗号アルゴリズムによって保護されていた情報が解読される可能性があるとしている。そのうえで、金融機関の顧客情報などが盗取され、関係する組織のレピュテーションや顧客のプライバシーが損なわれるおそれがあるとの見方を示している。また、こうしたリスクへの対応に関してステークホルダー間での調整には相当の時間と経済的負担が必要となる可能性があることから、可能な限り早期に対応に着手することが望ましいとしている。

提言では、リスク対応の3つのステップを挙げている。

- ① リスクと対応方法に関する理解深耕：ベンダーや専門家の協力を得ながら、量子コンピュータとそれによるリスク、対策技術について理解を深める。量子コンピュータの開発スケジュール、脅威となる事象、今後有望とみられる対策技術やアプローチについてもフォローすることが望ましい。
- ② リスク評価：暗号インベントリを整備し、リスクを適切に評価する。
- ③ リスク低減計画立案：リスクを把握・管理するプロセス、ステークホルダーの責任範囲、リスクの把握・管理のための作業と実施時期、リスク対応の優先順位などを検討し、検討結果を盛り込んだリスク低減計画を立案する。

金融当局に対しては、金融機関などと協力し、量子耐性を向上させる技術(quantum resilient technologies)の重要性を広く知らしめることを推奨している。

## (7) FS-ISAC による暗号アジリティのガイダンス

FS-ISAC は、2024年10月に暗号アジリティに関するガイダンスを発表している(Financial Services Information Sharing and Analysis Center 2024)。ガイダンスでは、経営層に対して暗号アジリティとその重要性、暗号アジリティを向上させるプロセスなどを説明するとともに、実務者や技術者に対して暗号アジリティに関連する技術的な課題や留意点を説明している。

### イ. 暗号アジリティとは

ガイダンスでは、冒頭で暗号アジリティを以下のとおり説明している。

#### 【暗号アジリティ】

暗号解読手法の向上、新しい脅威の出現、技術革新、脆弱性の発見などに応じて、迅速かつ効率的に、暗号アルゴリズム(パラメータや鍵を含む)や暗号ソリューションを適応させる組織の能力の度合い(a measure of an organization's ability)

このように、暗号アジリティを、技術的な対応だけでなく組織としての対応を含む概念として記述している。したがって、暗号アジリティを高めるためには、暗号アルゴリズムを切り替える際に必要となる業務・管理プロセスも整備することが求められる。

#### ロ. 暗号アジリティがなぜ重要か

ガイダンスでは、暗号アジリティを重視する背景として、今後、暗号アルゴリズムの切替えが複数回必要となりうることと、対応が求められるシステムの範囲が広がっており切替えの負担が大きくなっていることを挙げている。

1つ目の点については、量子耐性を有すると期待されている暗号アルゴリズムの多くが不安定な開発のサイクル<sup>26</sup>にあることから、そうした暗号アルゴリズムの切替えの頻度が今後高まりうるとしている。そのうえで、今回の暗号アルゴリズムの切替えにおいて暗号アジリティを考慮しなかった場合、将来さらなる切替えが必要になった際に、対応の時間を確保できない可能性があるとの見方を示している。

2つ目の点については、金融機関が既存の暗号アルゴリズムの安全性を信頼し、暗号アルゴリズムの切替えを考慮しないで、さまざまなインフラやアプリケーションに組み込んできたとしている。その結果、暗号アルゴリズムの切替えが必要なインフラやアプリケーションの範囲が拡大したとしている。

こうした点を踏まえ、ガイダンスでは、暗号アジリティを考慮しないで暗号アルゴリズムを切り替えることは長期的には金融業界の安全性（safety）にとって望ましくないとの認識を示している。

#### ハ. 暗号アジリティの度合いをどう把握するか

ガイダンスでは、暗号アジリティの度合いを表現する具体的な指標を示していない。その代わりに、指標を検討するうえで参考になる視点として次の3つを挙げている。

- システム設計の段階における暗号アジリティの考慮の度合い：暗号アルゴリズムの実装・切替えなどの機能がシステムの構成要素（ソフトウェア、ハードウェア

26 ガイダンスでは、不安定な開発のサイクルにあると判断した根拠を明確に示しておらず、NISTのウェブサイト（National Institute of Standards and Technology 2022）を引用している。このウェブサイトは、NISTが標準化対象とした暗号アルゴリズムと継続評価対象とした暗号アルゴリズムをそれぞれ発表するものである。NISTの標準化プロジェクトでは、量子耐性を有する暗号アルゴリズムの評価と改良、標準化が同時並行で進められているほか、将来の脆弱性発見の可能性を想定し（実際に、標準化候補の暗号アルゴリズムのいくつかは脆弱性が発見されて標準化対象外となっている）、さまざまなタイプの暗号アルゴリズムを標準化する方針が示されている。これらを踏まえると、標準化された暗号アルゴリズムであったとしてもセキュリティに対する信頼が十分に醸成されていないとの見方もできる。ガイダンスは、こうした状況を不安定な開発のサイクルと表現したと解釈することができる。

- ア、関連するインフラ) や運用プロセスの設計にどの程度組み込まれているか。
- アーキテクチャにおける変更の度合い：新しい暗号アルゴリズムの導入の前後で、システムのアーキテクチャにどの程度の変更が生じるか。
- 稼働中のシステムへの影響の度合い：新しい暗号アルゴリズムの導入に際して、稼働中のシステムを停止せずに対応できる可能性はどの程度あるか。

## 二. 暗号アルゴリズムを円滑に切り替える手法

ガイドランスでは、暗号アルゴリズムの切替えを円滑に実施するアプローチとして抽象化 (abstraction) を紹介している。

抽象化は、暗号アルゴリズムの処理に関する機能を個々のアプリケーションの一部としてそれぞれ実装するのではなく、アプリケーションとは別のシステムとして実装するという設計方針である。各アプリケーションは、メッセージの暗号化やデジタル署名の生成などを、暗号アルゴリズムの処理に特化したシステムの API を呼び出して実行する。暗号アルゴリズムの切替えに際しては、暗号アルゴリズムの処理に特化したシステムのみ新しい暗号アルゴリズムを組み込むなどの変更を実施し、各アプリケーションでは、API による処理の実行命令を変更するなどの軽微な対応とすることができる<sup>27</sup>。ただし、暗号アルゴリズムの処理に特化したシステムとの間で通信が発生するため、通常よりも暗号アルゴリズムの処理に時間がかかるほか、個々のアプリケーションの事情に応じて暗号アルゴリズムの処理をカスタマイズできなくなるといった留意点がある。

ガイドランスでは、抽象化に基づく手法の例として、クリプト・アズ・ア・サービス (crypto-as-a-service)、暗号ライブラリ、自動化された PKI・認証局 (automated PKI and CA)、通信データ暗号化のためのサービス・メッシュ (service mesh for encryption in transit) を説明している。

- クリプト・アズ・ア・サービス：暗号アルゴリズムの処理をクラウドで実現・提供するサービス。アプリケーションはクラウドにアクセスして処理を依頼し、その結果を受信する形態を主に想定している。
- 暗号ライブラリ：暗号アルゴリズム (群) を実行するソフトウェア。アプリケーションとは別に暗号ライブラリを自組織の内部システムとして準備し、アプリケーションは暗号アルゴリズムの処理を暗号ライブラリに依頼して処理結果を受け取る形態を主に想定している。自組織内で構築することから、クリプト・

.....  
27 API を使用する場合について、ガイドランスでは、API の名称や引数が暗号アルゴリズムの識別情報と独立か否かなどによって暗号アジリティのレベルが異なる旨を説明している。例えば、API の名称や引数がアルゴリズムの識別情報と独立であれば、暗号アルゴリズムの切替えに際して API の名称などを変更する必要がなく、暗号アジリティが相対的に高いといえる。また、暗号アルゴリズムの処理を実行する機器において、暗号アルゴリズムの切替えの際にユーザやその他のシステムとのインタフェースに変更を加える必要がない場合、暗号アジリティが相対的に高いといえる。

アズ・ア・サービスと比べて、暗号アルゴリズムの処理のメンテナンスを柔軟に実行することができる。

- 自動化された PKI・認証局：電子証明書を管理するシステム。暗号アルゴリズムの切替えの際に、既存の電子証明書の失効や新しい電子証明書の発行を効率的に実施することができる。
- 通信データ暗号化のためのサービス・メッシュ：データの暗号化や認証の機能を有する機器（VPN の装置など）を介してアプリケーション間の通信が行われ、各アプリケーションが暗号化や認証に関する処理を実行する必要がないアーキテクチャ。暗号アルゴリズムの切替えの対応は、データの暗号化や認証の機能を有する機器のみで行われ、アプリケーションへの影響が少ない。

## (8) 金融庁の検討会による報告

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は、2024 年 11 月発表の報告書において、金融機関の経営層に対して耐量子計算機暗号への移行に関する対応の重要性、留意点や課題などを説明している（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 [2024a]）。

### イ. リスク対応のポイント

報告書では、エグゼクティブ・サマリーにおいて、CRQC によるリスクに対応するためには長期間にわたって多くのリソースを必要とすることから、経営層がリスクや対応期限を正しく認識する必要があるとしている。そのうえで、リスク対応を適切に進めるためのポイントとして以下の点を示している。

- 経営層は暗号アルゴリズム移行の対応を全社施策として取り扱い、リーダーシップを発揮して移行方針を決定することが望ましい。
- アメリカ連邦政府が 2035 年を目途にアルゴリズムの移行を推進していることなどを踏まえ、重要度の高いシステムでは、2030 年代半ばを目安に量子耐性を有する暗号アルゴリズムを利用可能な状態にすることが望ましい。
- 事前準備として暗号インベントリの整備・管理が必要であるが、構築・運用に相当の時間とリソースを要するため、早期に着手することが望ましい。
- 移行後の暗号アルゴリズムにおいて脆弱性が発見される可能性があるため、暗号アルゴリズムを柔軟に切り替えることを可能にする技術の実装を考慮すること（暗号アジリティを向上させること）が重要である。
- 暗号アルゴリズムの移行の検討を、ベンダー、金融インフラ提供事業者、フィンテック企業などと協力して進めることが重要である。

- 政府とも密に連携しつつ金融業界としてのロードマップを策定するとともに、各金融機関に共通する課題に協力・分担して対応することが望ましい。

#### ロ. 技術面での課題・留意点

報告書では、技術面での課題や留意点を説明している。ポイントを要約すると以下のとおりである。

- 暗号アジリティをどのように実現するかが重要な課題である。暗号アルゴリズムの処理を疎結合とするアーキテクチャの適用、電子証明書や暗号鍵管理の機能の集約、暗号インベントリの整備、暗号アルゴリズムの利用状況を監視するための管理プロセスやツールの整備などが挙げられる。
- 量子耐性を有する暗号アルゴリズムのソリューションの適用に際して、標準化動向や技術の成熟度の把握が重要である。個々の金融機関では把握が困難であることも見込まれるため、金融当局、業界団体などと連携して情報の提供を受けることが望ましい。
- 暗号アルゴリズムの移行の過渡期において、新しい暗号アルゴリズムに対応していないシステムからの接続と対応済みのシステムからの接続が混在する場合が想定されるため、両方の接続を実現する機能を考慮することが望ましい。
- 量子耐性を有する暗号アルゴリズムへの対応はシステムの大規模更改・改修のタイミングに合わせて実施することを基本とし、時間に余裕を持って検討することが重要である。

### 3. 主な推奨事項のまとめ

2節で紹介した調査報告や提言は、いずれも、CRQCによるリスクに関する検討に早期に着手することが望ましいとしている。今後、金融機関による取組みが推奨されている主な事項を要約する<sup>28</sup>と以下のとおりである。

- 金融業界としてのリスク低減計画の策定：金融業界の関係者（当局を含む）が連携し、関連する情報を共有しつつ、金融業界としてのリスク低減に向けた計画を策定することが望ましい。
- 暗号インベントリの整備：リスクを見極めるためには、暗号アルゴリズムの使用状況を明確にする必要があることから、事前準備として、暗号インベントリ

28 リスク対応方針などの国際的な調和についても、世界経済フォーラムの提言において重要な推奨事項とされている。これは、主として各国の政府や金融当局への推奨事項であることからここでは割愛する。

を整備することが必要である。

- **HNDL 攻撃対応**：長期間（例えば 10 年以上）保護する必要がある情報を取り扱っているシステムでは、HNDL 攻撃が既に脅威となっている可能性がある。そのため、リスク評価を早期に実施し、リスク低減の必要性を明らかにすることが望ましい。
- **暗号アジリティに配慮したシステムの実現**：今後、暗号アルゴリズムの切替えを複数回実施することになる可能性があり、切替えを円滑に実施するための技術的な仕組みや体制を整備することが望ましい。
- **ハイブリッド手法の採用**：量子耐性を有する暗号アルゴリズムへの移行の過渡期において、それを既存の暗号アルゴリズムと組み合わせて実装することが望ましい。

#### 4. おわりに

---

本稿では、CRQC による暗号アルゴリズムへのリスクに関して、金融関連の各種組織による最近の主な調査報告や提言のポイントを紹介した。共通する推奨事項として、暗号インベントリの整備などの事前準備に早急に着手することが挙げられている。また、将来、暗号アルゴリズムの切替えが複数回必要となるケースを想定し、暗号アジリティに配慮したシステムの実現も推奨されている。

金融業界として足並みを揃えてリスク対応を進めるという観点からは、金融機関が連携して業界としてのリスク低減計画をまず策定し、それと統合的なリスク低減計画を各金融機関が策定するという対応が推奨されている。こうした対応は、各金融機関がリスク低減計画をそれぞれ独自に策定する場合と比べて、各金融機関における負担の低減につながる。また、一部の金融機関のリスク対応が遅れる可能性も低くなり、金融業界全体としてのセキュリティ・レベルの維持・向上に資すると期待することができる。

金融業界としてのリスク低減計画の策定には、各金融機関が CRQC によるリスクと対応の必要性を認識することが不可欠である。しかし、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におけるメンバーの発言で示されているように、リスク認識が金融業界に広く浸透しているとはいえない（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 [2024b]）。各金融機関の経営層に対して暗号アルゴリズム移行への対応の必要性や緊要性をどのように説明し理解を得ていくかが重要な課題である。アプローチの 1 つとして、金融機関における暗号アルゴリズムの代表的なユースケースを洗い出し、それぞれのユースケースにおいて暗号解読などのリスクを明確化することが考えられる。リスク低減に必要な作業

や課題、費用負担や移行にかかる時間を見積もり、ユースケースに応じた「手触り感」のある説明を行うことが有用であろう。

当面、リスク低減に向けた検討は金融 ISAC において進められるとみられる。各金融機関においては、こうした活動に積極的に参加して金融機関間の連携を一段と強化するとともに、リスクやその対応に関する理解を深めることを期待したい。

## 参考文献

- 宇根正志、「量子コンピュータが暗号に及ぼす影響にどう対処するか：海外における取組み」、金融研究所ディスカッション・ペーパー、No. 2023-J-13、日本銀行金融研究所、2023年
- ・菅 和聖、「量子コンピュータ開発の進展と次世代暗号」、『金融研究』第40巻第4号、日本銀行金融研究所、2021年、55～96頁
- ・松浦幹太・田倉 昭、「デジタルタイムスタンプ技術の現状と課題」、『金融研究』第19巻別冊第1号、日本銀行金融研究所、2000年、105～154頁
- 菅 和聖・佐々木寿彦、「量子鍵配送の安全性証明の進展と普及に向けた課題」、『金融研究』第43巻第4号、日本銀行金融研究所、2024年、123～156頁
- 金融庁、「『量子コンピュータの登場に伴う機会とリスクに備えた計画に関する G7 サイバー・エキスパート・グループによるステートメント』の仮訳」、金融庁、2024年（[https://www.fsa.go.jp/inter/etc/20240926/quantum\\_kariyaku.pdf](https://www.fsa.go.jp/inter/etc/20240926/quantum_kariyaku.pdf)、2025年12月10日）
- 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、「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」、金融庁、2024年 a（<https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf>、2025年12月10日）
- 、「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（第3回）議事要旨」、金融庁、2024年 b（<https://www.fsa.go.jp/singi/pqc/gijiyousi/20241018.html>、2025年12月10日）
- Accredited Standards Committee X9, Inc. 2019. “Quantum Techniques in Cryptographic Message Syntax (CMS).” Accredited Standards Committee X9, Inc. Accessed December 10, 2025. <https://x9.org/wp-content/uploads/2019/03/ASC-X9-TR-50-2019-Quantum-Techniques-in-Cryptographic-Message-Syntax-1.pdf>.
- . 2022. “Quantum Computing Risks to the Financial Services Industry.” Accredited Standards Committee X9, Inc. Accessed December 10, 2025. [https://x9.org/wp-content/uploads/2022/11/X9F-Quantum-Computing-Risk-Study-Group-IR-F01-2022\\_20221129-Published-PDF.pdf](https://x9.org/wp-content/uploads/2022/11/X9F-Quantum-Computing-Risk-Study-Group-IR-F01-2022_20221129-Published-PDF.pdf).
- Bank for International Settlements, Banque de France, and Deutsche Bundesbank. 2023. “Project Leap: Quantum-Proofing the Financial System.” Bank for International Settlements. Accessed December 10, 2025. [https://www.bis.org/about/bisih/topics/cyber\\_security/leap.htm](https://www.bis.org/about/bisih/topics/cyber_security/leap.htm).
- Bundesamt für Sicherheit in der Informationstechnik. 2025. “Status of Quantum Computer Development.” Bundesamt für Sicherheit in der Informationstechnik. Accessed December 10, 2025. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungsstand\\_QC\\_V\\_2\\_1.html?nn=916616](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungsstand_QC_V_2_1.html?nn=916616).

- European Commission. 2024. “Recommendation on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography.” European Commission. Accessed December 10, 2025. <https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography>.
- Financial Services Information Sharing and Analysis Center. 2023. “Preparing for a Post-Quantum World by Managing Cryptographic Risk.” Financial Services Information Sharing and Analysis Center. Accessed December 10, 2025. <https://www.fsisac.com/knowledge/pqc>.
- . 2024. “Building Cryptographic Agility in the Financial Sector: Effective, Efficient Change in a Post Quantum World.” Financial Services Information Sharing and Analysis Center. Accessed December 10, 2025. <https://www.fsisac.com/knowledge/pqc>.
- G7 Cyber Expert Group. 2024. “G7 Cyber Expert Group Statement on Planning for the Opportunities and Risks of Quantum Computing.” U.S. Department of the Treasury. Accessed December 10, 2025. <https://home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf>.
- Monetary Authority of Singapore. 2024. “Advisory on Addressing the Cybersecurity Risks Associated with Quantum.” Monetary Authority of Singapore. Accessed December 10, 2025. <https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf>.
- National Institute of Standards and Technology. 2022. “PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates.” National Institute of Standards and Technology. Accessed December 10, 2025. <https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4>.
- Secure Information Technology Center Austria, Centre for Cybersecurity Belgium, National Cyber and Information Security Agency Czech Republic, Centre for Cyber Security Denmark, Information System Authority Estonia, Finnish Transport and Communication Agency, French National Agency for the Security of Information Systems, Federal Office for Information Security Germany, National Cyber Security Authority Hellenic Republic, National Cyber Security Centre Ireland, National Cybersecurity Agency Italy, Ministry of Defense Latvia, National Cyber Security Centre Ministry of Defense Lithuania, High Commission for National Protection Luxemburg, Netherlands National Communication Security Agency, Ministry of Interior and Kingdom Relations Netherlands, National Cyber Security Centre Ministry of Security and Justice Netherlands, Research and Academic Research Center Poland, Government Information Security Office Slovenia, and National Cryptologic Center Spain. 2024. “Securing Tomorrow, Today:

- Transitioning to Post-Quantum Cryptography.” Bundesamt für Sicherheit in der Informationstechnik. Accessed December 10, 2025. <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.html>.
- UK Finance Limited. 2023. “Minimising the Risks: Quantum Technology and Financial Services.” UK Finance Limited. Accessed December 10, 2025. <https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/minimising-risks-quantum-technology-and-financial>.
- White House. 2022. “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems.” White House. Accessed December 10, 2025. <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems>.
- World Economic Forum. 2024. “Quantum Security for the Financial Sector: Informing Global Regulatory Approaches.” World Economic Forum. Accessed December 10, 2025. [https://www3.weforum.org/docs/WEF\\_Quantum\\_Security\\_for\\_the\\_Financial\\_Sector\\_2024.pdf](https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf).

# 貿易取引の為替リスクヘッジにおけるディープ・ヘッジングの活用

みわ ゆきや  
三輪幸哉

## 要 旨

本稿では、企業の為替リスク管理における新たなアプローチとして、機械学習の活用を提案する。具体的には、企業の外貨建て貿易取引に関して、機械学習をヘッジに応用した技術である「ディープ・ヘッジング」を活用することで、実務上重要な取引コストや内外金利差を考慮したヘッジ戦略の構築を試みる。そのうえで、提案手法によるヘッジ戦略の特性を考察する。その結果、以下の3つの特性を明らかにする。第1に、簡便な金融市場を想定した2項モデルを検証モデルとして用いて提案手法のパフォーマンスを確認すると、提案手法から導出された戦略は検証モデルの理論的な最適戦略と一致する。第2に、提案手法は既存手法と比べて、特に取引コストが高い環境下において、下方リスクを抑制しつつ期待収益向上を実現するという点で優れたヘッジ効果が得られる。これは、提案手法が取引コストに応じた最適戦略を構築できることを示している。第3に、提案手法は、下方リスク抑制と期待収益向上のどちらをより重視するかといった、企業固有のリスク選好をヘッジ戦略に反映することができる。

キーワード： ディープ・ヘッジング、為替リスク管理、機械学習、動的ヘッジ戦略

.....  
本稿の作成に当たっては、篠潤之介准教授（早稲田大学）、鷹岡澄子教授（成蹊大学）、吉羽要直教授（東京都立大学）、渡部敏明教授（一橋大学）ならびに日本銀行のスタッフ等から有益なコメントを頂いた。本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

三輪幸哉 日本銀行金融研究所  
(現 三井住友銀行、E-mail: Miwa\_Yukiya@dn.smbc.co.jp)

## 1. はじめに

グローバル企業にとって為替リスク管理は重要な課題である。伊藤ほか [2024] が実施した日本の製造業上場企業を対象としたアンケート調査によれば、日本企業の輸出における米ドル建て比率は 60% を超えており、適切な為替リスク管理の重要性が示唆される。もっとも、為替ヘッジを行っている企業の 46% はヘッジ割合について明確な社内ルールがないと回答しており、自社に適した為替リスク管理は容易ではないことが推察される。また同調査では、為替ヘッジを行っている企業の 84% が先物為替予約を利用している一方、通貨オプションを利用している企業は 14% にとどまっており、主に先物為替予約がヘッジ手段として定着していることが示唆される。この背景の 1 つとして、通貨オプションは相場上昇時に収益機会を享受できる一方、契約時に支払うオプション料が高く、企業はその支払いを忌避する傾向にあることが考えられる。

このような状況下、機動的に先物為替予約を取引するダイナミックヘッジと呼ばれる手法に注目が集まっている。その中でも特に、下方リスクを抑制しながら収益機会を享受するという通貨オプションと類似の特性を、オプション料を支払わずに実現するヘッジ戦略への関心が高まっている。もっとも、多くのダイナミックヘッジ戦略には、実務に適用するうえで、取引コストが考慮されていない、市場環境変化に応じた戦略の調整が難しいなどの課題 (Balder *et al.* 2009; Weng 2014) が指摘されている。

そこで、本稿では、機械学習の手法を用いて、これらの課題に対応する新たなヘッジ戦略を提案する。具体的には、機械学習をヘッジに応用した技術である「ディープ・ヘッジング」(篠崎 [2023]; Buehler *et al.* 2019)<sup>1</sup> を使い、先物為替予約を用いたダイナミックヘッジ戦略を導出する。そのうえで、下方リスクの抑制と期待収益の向上という観点から既存手法と比較し、提案手法を実務に応用する際の課題や論点を明確化する。

分析の結果、提案手法のヘッジ戦略について、以下の 3 つの特性が明らかにされる。第 1 に、提案手法から導出されたヘッジ戦略は、検証モデルの理論的な最適戦略と整合的である。ここで用いた検証モデルは、2 項モデルで表現できる簡便な金融市場を前提としているものの、この結果は提案手法のヘッジ戦略が機能することを示唆している。第 2 に、提案手法は、ヘッジ戦略を導出する際に取引コストを明示的に組み込んでいることから、取引コストの変化に適応できる柔軟性を持つこと

.....  
1 ディープ・ヘッジングは、もともとデリバティブのヘッジ手法として研究されてきたが、近年では、広範なリスク管理に応用する研究が増えている (Krabichler and Teichmann 2020; Fernandez-Arjona and Filipović 2022)。

が示される。提案手法は、特に取引コストが高い環境下において、ヘッジ比率の変動を抑制して取引コストを抑える戦略を提示するなど、下方リスクを抑制しつつ期待収益向上を実現するという点で優れたヘッジ効果を発揮する。第3に、提案手法は、リスク尺度の設計を調整することで、企業のリスク選好をヘッジ戦略に反映することができる。例えば、為替レートフロア（下限）割れ回避度パラメータを小さくすると、提案手法は、フロア割れリスクよりも期待損益向上をより重視する戦略を導出することになる。

本研究は、下方リスクを抑制しながらも収益機会を享受するダイナミックヘッジについての研究と深く関連している。ダイナミックヘッジの伝統的なアプローチとしては、オプションのペイオフを模倣する戦略である OBPI (Option-Based Portfolio Insurance; see Leland and Rubinstein 1988) や、ポートフォリオ金額と最低保証額（フロア）の差額に、あらかじめ定めておいた乗数を掛けることでヘッジ比率を決定する戦略である CPPI (Constant Proportion Portfolio Insurance; see Black and Jones 1987) などが挙げられる。これらの手法は、オプション料を支払わずに実現できる一方で、理論上の最適戦略が取引コストを考慮しないという問題点がある。

近年は、機械学習を活用したダイナミックヘッジのアプローチが提案されている。Heaton *et al.* (2017) や Niaki and Hoseinzade (2013) は、将来価格の予測モデルを構築しその予測値に基づいて戦略を導出するアプローチを、Du *et al.* (n.d.) や Jiang *et al.* (2017) は、強化学習を用いて直接的に最適な戦略を導出するアプローチを提案している。前者には、取引コストなどを理論的に組み込むことが難しいという課題 (Jiang *et al.* 2017)、後者には、強化学習によって導出された戦略の結果を適切に評価するための報酬関数の設計が難しいという課題 (Hambly *et al.* 2023)、学習が不安定になりやすいという課題 (Pippas *et al.* 2025) が指摘されている。本稿は、ディーブ・ヘッジングを活用することで、これらの課題点を回避したダイナミックヘッジのアプローチを提案する。

本稿の構成は以下の通りである。2節では、ディーブ・ヘッジングの概要を解説したうえで、企業の為替リスク管理への応用について示す。3節では、単純な2項モデルにおいて、提案手法で得られるヘッジ戦略と理論的な最適戦略との整合性を確認する。4節では、シミュレーション分析により、既存のダイナミックヘッジの手法で得られるヘッジ戦略との比較を通じて、提案手法の有効性を検証する。5節では、まとめと考察を行う。

## 2. ディープ・ヘッジングの理論的枠組みと為替リスク管理への応用

本節では、まずディープ・ヘッジングの理論的枠組みを整理したうえで、本研究における応用について論じる。

### (1) ディープ・ヘッジングの理論的枠組み

Buehler *et al.* (2019) によって提案されたディープ・ヘッジングは、デリバティブのヘッジ問題を凸リスク最小化問題として深層学習により解く枠組みである。以下では、その枠組みを簡潔に整理する。

対象期間を時点 0 から満期時点  $T$  までとし、その間の取引可能時点を  $t_0 < t_1 < \dots < t_n = T$  とする。確率空間を  $(\Omega, \mathcal{F}, P)$ 、離散フィルトレーションを  $\{\mathcal{F}_k\}_{k=0, \dots, n}$  とし、ヘッジ対象の原資産の価格過程  $\{S_k\}_{k=0, \dots, n}$  は  $\mathcal{F}_k$ -適応な実数値確率過程とする。このとき、ヘッジ戦略とは、 $\mathcal{F}_k$ -適応な実数値確率過程  $\delta = \{\delta_k\}_{k=0, \dots, n}$  で示されるヘッジ手段の各時点でのポジション量（保有量）である。この設定のもとで、デリバティブでショートポジションを取った場合、満期時点での損益は以下のように表現される。

$$PL(Z_T, p_0, \delta) = p_0 - Z_T + \sum_{k=0}^{n-1} \delta_k (S_{k+1} - S_k) - \sum_{k=0}^n c_k (\delta_k - \delta_{k-1}) \quad (1)$$

ここで、 $p_0$  は初期時点でのデリバティブ売却益、 $Z_T$  は満期時点で支払う必要のあるペイオフを表す。また、右辺第 3 項はヘッジ取引による損益、右辺第 4 項は取引コストを表現している。取引コスト関数  $c_k(\cdot)$  については、例えば取引量に比例する形で  $c_k(\delta_k - \delta_{k-1}) = \varepsilon |\delta_k - \delta_{k-1}| S_k$  などが考えられる。

上記の損益に対するリスクを定量化するために、凸リスク尺度  $\rho$  を導入する。凸リスク尺度は、単調減少性、凸性、現金不変性という 3 つの性質を満たす関数として定義される。単調減少性は、すべての状況でポートフォリオ 1 の損益がポートフォリオ 2 の損益を上回る場合、ポートフォリオ 1 のリスク尺度はポートフォリオ 2 のリスク尺度を超えないことを表す。凸性は、分散効果を公理化したものであり、2 つのポートフォリオに分散投資したポートフォリオのリスク尺度は、個別のポートフォリオのリスク尺度を加重平均したものを超えないことを意味する。現金不変性は、確実なペイオフがリスク尺度を同額だけ減らす性質を示している。

この設定の下で、最適ヘッジ戦略は以下の最小化問題の解として定式化される。

$$\delta^* = \operatorname{argmin}_{\delta \in H} \rho(PL(Z_T, p_0, \delta)) \quad (2)$$

ここで  $H$  は実行可能なヘッジ戦略の集合を表す。

ディープ・ヘッジングでは、ヘッジ戦略をニューラルネットワークによりモデル化し、損失リスクを最小化するようにネットワークを訓練する。具体的には、時点  $t_k$  におけるヘッジ戦略  $\delta_k$  を以下のような形でモデル化する。

$$\delta_k = F^{\theta_k}(x_k) \quad (3)$$

ここで、 $F^{\theta_k}(\cdot)$  は時点  $t_k$  におけるヘッジ戦略を記述するニューラルネットワーク関数、 $\theta_k$  はニューラルネットワーク  $F^{\theta_k}$  のパラメータ、 $x_k$  は時点  $t_k$  における入力特徴量である。 $F^{\theta_k}(\cdot)$  は2~3層の浅いニューラルネットワークとするのが通例となっている（篠崎 [2023]）。なお、Buehler *et al.* (2019) では時点  $t_k$  ごとに異なるパラメータ  $\theta_k$  を使用する設計を採用しているが、本研究では、実装の簡素化と計算効率の観点から、全時点で共通のパラメータ  $\theta$  を使用してモデル化している。その代わりに、時点の情報を入力特徴量に含めることで、パラメータ数を削減しつつも、時間軸に沿ったヘッジ戦略の導出を可能としている。この設計は、今木ほか [2021] の No-Transaction Band ネットワークなどでも採用されている。入力特徴量  $x_k$  には、現在の原資産価格  $S_k$ 、直前のヘッジポジション  $\delta_{k-1}$ 、および市場環境変数（ボラティリティ指標、金利など）が含まれる。

パラメータ  $\theta$  の最適化は、リスク尺度  $\rho$  を目的関数として行われ、以下のように表現される。

$$\theta^* = \operatorname{argmin}_{\theta} \rho(PL(Z_T, p_0, \delta)) \quad (4)$$

この最適化は、通常、確率的勾配降下法などの深層学習の標準的な学習アルゴリズムを用いて行われる。

ヘッジ戦略の実行においては(3)式より、学習させたパラメータ  $\theta_k^* = \theta^*$  のニューラルネットワーク  $F^{\theta_k^*}$  に、実現した入力特徴量  $x_k$  を代入することで、時点  $t_k$  におけるヘッジ戦略  $\delta_k^*$  を求めることができる。

## (2) 為替リスク管理への応用

本研究では、ディープ・ヘッジングの理論的枠組みを、先物為替予約を用いた輸出企業の外貨建て債権の為替リスクヘッジに応用する。市場環境に応じて先物為替

予約の保有量を動的に調整することで、下方リスクを抑制しつつ期待収益の向上を追求するヘッジ戦略の構築を目指す。以下では、その際に考慮すべき点について説明する。

まず、先物為替予約を行う際のコストとして、通常取引コストに加えて、内外金利差による直物レートと先物レートの差額（直先差額）をコストとして考慮する。学術研究では一般的に、内外金利差による直先差額は、将来キャッシュフローを現在価値に割り引いたものであり、実質的なコストとして扱わないものの、企業の為替リスク管理においては契約時の為替レートを基準にすることが一般的であるため、内外金利差による直先差額もコストに含めることが多い。この要因の1つとしては、直先差額が会計上の為替差損益として計上されてしまうことが挙げられる。例えば、ドル建て輸出債権が発生し3ヵ月後に入金予定で、現時点の為替レートが150円/ドル、現時点の3ヵ月先物レートが149円/ドルという状況を想定する。この1円/ドルの直先差額は、学術的には将来キャッシュフローの現在価値への割引を反映したものと解釈されるが、実際にこの先物為替予約を締結すると、会計上の為替差損として1円/ドル計上されることになる。以降本稿では、この直先差額を取引コストとは区別して、ディスカウントコストと表記する。

次に、コストの支払いタイミングについて考える。Buehler *et al.* (2019) のモデルでは取引コストは満期にまとめて清算する形式を採用しているのに対し、本研究では為替予約取引の実務に即して、各取引時点で元本から即時に支払う形式を採用している。これは、一般的に企業が取り組む為替予約取引では、金融機関から提示される為替予約レートにコストが織り込まれており、実質的に取引時点で元本からコストを支払うためである。

また、Buehler *et al.* (2019) のモデルでは、デリバティブ（オプション）のヘッジを想定し、ヘッジ手段のポジション量を導出する設計となっている一方、本研究では、ヘッジ比率（ヘッジ対象のポジション量に対するヘッジ手段のポジション量の割合）を導出する設計としている。これは、為替リスク管理の実務において、ポジション量よりもヘッジ比率の方が実務担当者にとって解釈しやすく、また取引コストにより元本が変動する環境下では、比率表記の方が異なる手法間・時点間でのヘッジ度合いの比較が容易なためである。

さらに、下方リスクを抑制しつつ期待収益の向上を追求したいという企業の要望に応えるため、リスク尺度の設計においては、以下の特性を考慮することが重要となる。

- 1) 期待収益の最大化
- 2) 下方リスクに対するペナルティ
- 3) 企業によるリスク選好度の柔軟な反映

従来リスク尺度は、期待収益とリスクのトレードオフを考慮したものが多いが、企業における為替リスク管理の文脈では、目標下限損失（フロア）からの乖離に注目して、リスク尺度を考えることが重要である。これは、一般的に企業は確保したい採算水準を持っており、為替変動による損失額をその採算水準内に抑えたい意向があるためである。このため、実務的には取引ごとに、採算確保の観点から意識されるフロアが存在している。

### 3. ディーブ・ヘッジングの理論的整合性の検証

本節では、ディーブ・ヘッジングを活用した提案手法が適切に機能するかを検証する。具体的には、単純な2項モデルにおいて、ディーブ・ヘッジングにより得られる数値解が、動的計画法により導出される理論的最適解と一致するかどうか考察する。

#### (1) 検証モデルの設定

検証に用いる2項モデルを以下のように設定する。

- 外貨建て債権：1単位（1ドル）
- 初期為替レート：150円/ドル
- 取引可能時点： $t_0, t_1, \dots, t_n = T$ （ここでは  $n = 3$ ）
- 各取引可能時点における為替変動： $\pm 5$ 円（上昇または下落）
- 上昇確率： $p = 0.4$ 、下落確率： $1 - p = 0.6$
- ヘッジコスト： $c(h_k, t_k) = \alpha(t_n - t_k) |h_k - h_{k-1}|$  を期末に支払う

ここで、ヘッジコストは、取引コストとディスカウントコストの合計である。 $\alpha$  はコスト係数（ヘッジコストの大きさを決定するパラメータ）、 $t_n - t_k$  は時点  $t_k$  における満期までの残存期間、 $h_k$  は時点  $t_k$  におけるヘッジ比率（ $0 \leq h_k \leq 1$ ）を表す<sup>2,3</sup>。ヘッジコストが残存期間に応じて増加するのは、内外金利差によるディスカウントコストが、残存期間が長いほど大きくなることを簡略化して表現するものである。

2 本稿では、 $h_{-1} = 0$  および  $h_n = h_{n-1}$  としている。これは、初期時点でヘッジ比率を  $h_0$  にする際のコストを加味することと、満期時点ではヘッジ取引を行わないことを意味する。

3 2節(2)において、ヘッジポジション量  $\delta_k$  ではなくヘッジ比率  $h_k$  を導出する理由について述べたが、本検証の設定においては  $h_k = \delta_k$  となる。

なお、本検証では簡単化のため、ヘッジコストは期末にまとめて支払う設定としている。

これに加え、理論的最適解を導出する際には、解析的な解を得るために以下の追加的な制約を設ける。

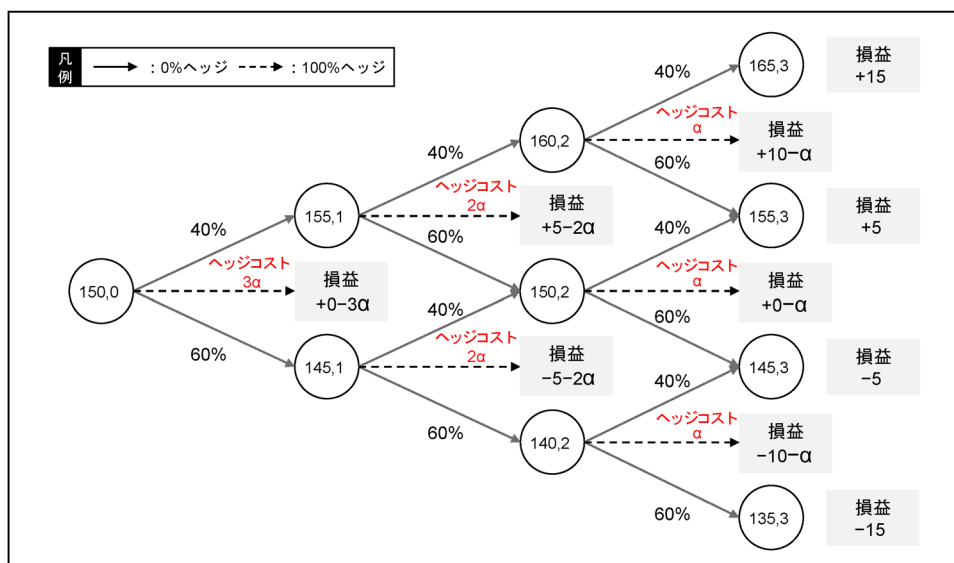
- ヘッジ比率： $h_k \in \{0, 1\}$  の 2 値
- 終端条件：一度ヘッジを実行すると ( $h_k = 1$  の場合)、損益が確定する

一方、ディープ・ヘッジングによる数値解の導出では、これらの制約を課さず、連続的で柔軟なヘッジ比率を許容する。そのため、ディープ・ヘッジングではより広い範囲を探索することとなる。

本検証では、上述の設定のもと、満期時点での損益の期待値  $\mathbb{E}[PL]$  を最大化するヘッジ戦略  $h^* = \{h_k^*\}_{k=0,1,2,3}$  を導出する。ここで  $PL$  は満期時点  $t_n$  における累積損益を表す。この単純化された環境でディープ・ヘッジングを用いた数値解と理論的最適解の一致を確認することで、より複雑な環境における提案手法の妥当性を検証する基盤とする。

図 1 には、検証モデルの概念図を示している。初期時点から始まり、各時点で為替レートが上昇または下落する 2 項ツリー構造となっている。各ノードは状態（為替レートと時点）を表し、エッジは状態遷移を表している。図 1 では単純化のために、理論的最適解の導出における制約付きの状態遷移（2 値のヘッジ比率や終端条

図 1 検証モデルの概念図



件)を示しているが、ディーブ・ヘッジングを用いて数値解を導出する際には、連続的なヘッジ比率の選択やヘッジ実行後の状態遷移が可能である。各状態において最適ヘッジ比率を比較することが本検証の目的である。

## (2) 理論的最適解の導出

本節(1)の設定下での最適ヘッジ戦略は、ベルマン方程式を用いた動的計画法により導出できる。価値関数  $V(S_k, t_k)$  を以下のように仮定する<sup>4</sup>。

$$V(S_k, t_k) = \max_{h_k \in \{0,1\}} \{E[V(S_{k+1}, t_{k+1})], S_k - S_0 - c(h_k, t_k)\} \quad (5)$$

ここで、 $S_k$ は時点  $t_k$ における為替レート、 $E[V(S_{k+1}, t_{k+1})]$ は  $h_k = 0$  の場合の価値、 $S_k - S_0 - c(h_k, t_k)$ は  $h_k = 1$  の場合の価値を表す。このベルマン方程式を末端から帰納的に解くことで、各状態における最適ヘッジ比率  $h^*(S_k, t_k)$  が決定される<sup>5</sup>。実際に(5)式を解くと、ヘッジコストが  $c(h_k, t_k) = \alpha(t_n - t_k)|h_k - h_{k-1}|$  で与えられることから、コスト係数  $\alpha$  の値に応じて  $h_k$  の最適解が 0 か 1 のどちらかに分かれることが理論的に示される。具体的には、 $\alpha$  が臨界値(本検証モデルでは 1)より小さい場合は、全状態でフルヘッジ ( $h_k = 1$ ) が最適となり、 $\alpha$  が臨界値より大きい場合は、全状態で無ヘッジ ( $h_k = 0$ ) が最適となる。

## (3) ディーブ・ヘッジングの実装

ディーブ・ヘッジングの実装においては、4層の隠れ層からなる順伝播型ニューラルネットワークを採用した。このネットワークは、為替レート  $S_k$  と時点  $t_k$  を入力として受け取り、ヘッジ比率  $h_k^\theta$  を出力する。形式的には、以下のように表現できる。

$$h_k^\theta = F^\theta(S_k, t_k) \quad (6)$$

.....  
 4 図1は実測度下での確率変動を示したものであり、(5)式の期待値は実測度下での期待値を表している。  
 5 例として、図1右上の  $V(160, 2)$  の算出例を以下に示す。なお、ここでは  $t_k = k, k = 0, 1, 2, 3$  としている。 $h_2 = 0$  の場合、40%の確率で  $V(165, 3)$ 、60%の確率で  $V(155, 3)$  に遷移することから、期待値  $E[V(S_3, t_3)]$  は  $0.4 \times V(165, 3) + 0.6 \times V(155, 3) = 0.4 \times (+15) + 0.6 \times (+5) = 9$  と計算される。 $h_2 = 1$  の場合、 $S_2 - S_0 - c(h_2, t_2)$  は、 $c(h_2, t_2) = c(h_2, 2) = \alpha(3 - 2)|h_2 - h_1|$  で  $h_1 = 0$  であるから、 $S_2 - S_0 - c(h_2, t_2) = 160 - 150 - \alpha = 10 - \alpha$  と計算される。このことから、 $\alpha \geq 1$  の場合は  $V(160, 2) = 9$ 、 $\alpha < 1$  の場合は  $V(160, 2) = 10 - \alpha$  と算出される。同様の計算を帰納的に繰り返すことで、 $V(150, 0)$  まで算出することができる。

ここで、 $F^\theta$  はパラメータ  $\theta$  を持つニューラルネットワーク関数を表し、 $h_k^\theta$  は時点  $t_k$  におけるヘッジ比率である。ネットワークアーキテクチャとしては、各隠れ層に 32 ユニットを配置し、活性化関数には ReLU を用いた<sup>6</sup>。最終層にはシグモイド関数を適用することで、出力を 0~1 の範囲に正規化している。この設計により、ヘッジ比率は常に 0~100% の間の値になる。入力特徴量としては以下を使用した。

- 為替レート  $S_k$  : 時点  $t_k$  における為替レート
- 時点  $t_k$  : 取引可能時点

学習データとしては、2 項モデルに従う為替レートのシナリオを 1,000 本生成した。最適化には Adam 最適化手法を採用し、学習率は 0.001、エポック数は 1,000 に設定した<sup>7</sup>。損失関数としては期待損益の負値を使用しており、これを最小化することで期待損益を最大化する戦略を導出した。この損失関数は以下のように定義される。

$$J(\theta) = -\mathbb{E}[PL(h^\theta)] \quad (7)$$

ここで  $PL(h^\theta)$  は単一シナリオにおけるヘッジ戦略  $h^\theta$  を適用した場合の損益を表し、以下の式で計算される。

$$PL(h^\theta) = \sum_{k=0}^{n-1} (S_{k+1} - S_k) - \sum_{k=0}^{n-1} h_k^\theta (S_{k+1} - S_k) - \sum_{k=0}^{n-1} c(h_k^\theta, t_k) \quad (8)$$

右辺第 1 項は外貨建て債権の損益、右辺第 2 項は先物為替予約の損益、右辺第 3 項はヘッジコストを表す。この損失関数  $J(\theta)$  を最小化することで、期待損益を最大化する最適なヘッジ戦略を導出した。

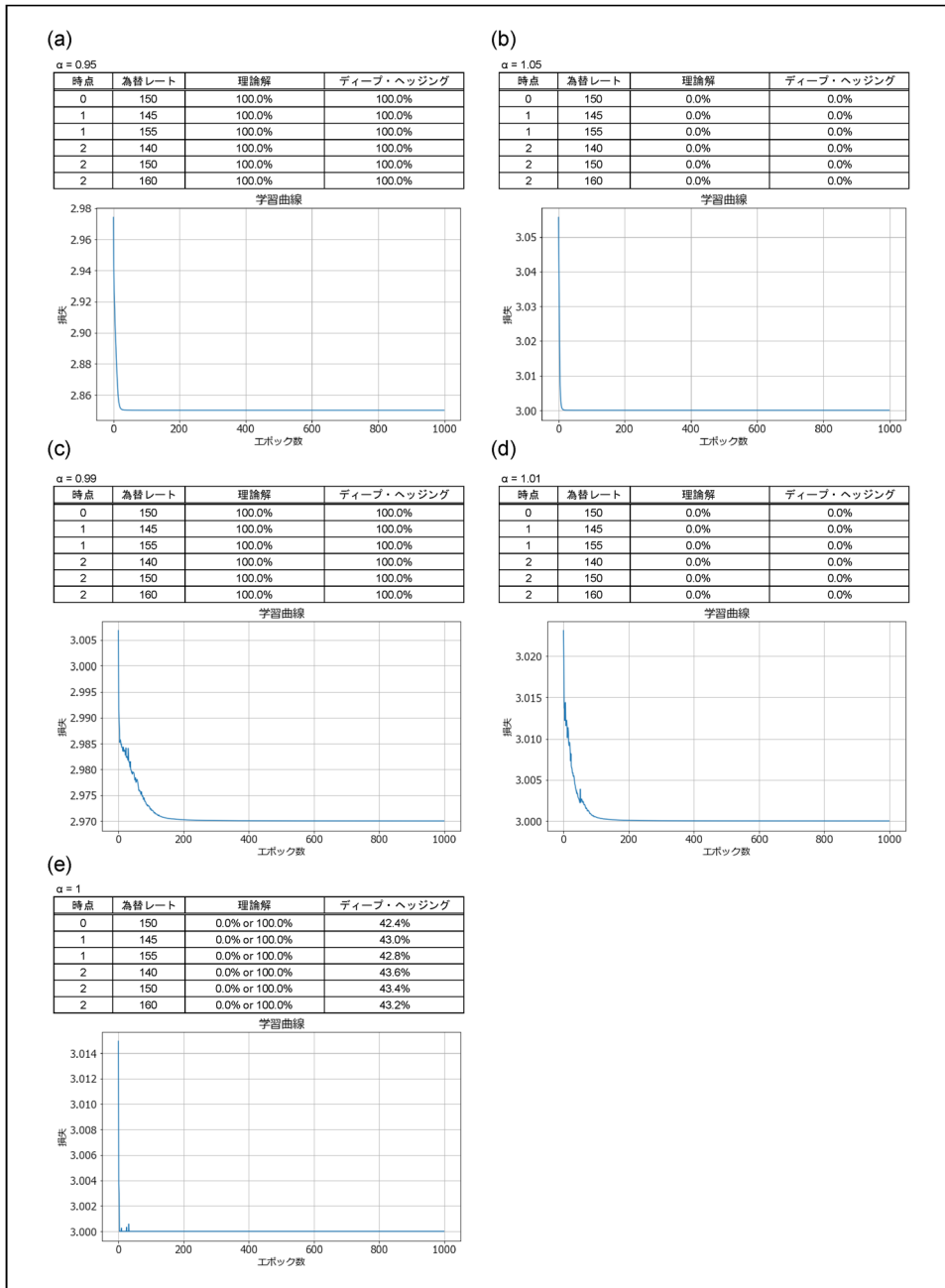
#### (4) 数値検証結果

コスト係数  $\alpha$  の臨界値近傍で、理論的最適解とディープ・ヘッジングによる数値解を比較した (図 2)。その結果、以下の特徴が確認された。

.....  
6 ReLU (Rectified Linear Unit) は、 $f(x) = \max(0, x)$  で定義される活性化関数である。計算効率が高く、深層学習において広く採用されている。

7 Adam 最適化アルゴリズムとは、機械学習モデルの学習において、パラメータを効率的に更新するための手法の 1 つである。学習率とは、学習する際のモデルの更新幅を表し、値が大きすぎると学習が不安定になり、小さすぎると学習に時間がかかる。エポック数とは、学習データ全体を用いてモデルを訓練する回数を意味する。

図2 各コスト係数におけるヘッジ比率の学習結果と収束過程



- 1) コスト係数  $\alpha$  が 1 より小さい場合 (図 2a) :  
ディープ・ヘッジングによる数値解は、全状態で理論的最適解のヘッジ比率 100% に一致する。ディープ・ヘッジングの学習曲線は即座に収束する。
- 2) コスト係数  $\alpha$  が 1 より大きい場合 (図 2b) :  
ディープ・ヘッジングによる数値解は、全状態で理論的最適解のヘッジ比率 0% に一致する。ディープ・ヘッジングの学習曲線は即座に収束する。
- 3) コスト係数  $\alpha$  が 1 に近い場合 (図 2c、図 2d) :  
ディープ・ヘッジングの学習曲線は、収束に時間を要するものの、最終的な解は、理論的最適解と一致する。
- 4) コスト係数  $\alpha$  が 1 の場合 (図 2e) :  
ヘッジの有無によって期待値が変わらないため、理論的最適解は不定。ディープ・ヘッジングによる数値解は即座に収束する<sup>8</sup>。

これらの結果は、2 項モデルの期待値最大化問題において、ディープ・ヘッジングを用いた提案手法が、理論的最適解と整合的なヘッジ戦略を導出できることを示している。これは、本研究の主眼である、より現実に即した状況においても、提案手法が有効なヘッジ戦略を導出できる可能性を支持する 1 つの根拠となる。

## 4. 為替リスク管理におけるディープ・ヘッジングの有効性の検証

本節では、シミュレーションに基づいて、為替リスク管理における提案手法の有効性を検証する。特に、既存手法である CPPI モデルとの比較分析を行うことで、提案手法の下方リスク抑制効果および期待収益向上効果について検証する。

### (1) ディープ・ヘッジングモデルと CPPI モデルの実装

ディープ・ヘッジングモデルの実装では、4 層の隠れ層からなる順伝播型ニューラルネットワークを採用する。このネットワークは、入力特徴量ベクトル  $x$  を受け

.....  
8 ヘッジすることによる期待値上昇効果と、支払うヘッジコストが同等であるため、理論的な最適解は不定となる。ただし、ディープ・ヘッジングでは、柔軟なヘッジ比率選択を許容しているため、 $h_{k-1} \leq h_k$  を満たす適当な値に収束すると考えられる。

取り、ヘッジ比率  $h$  を出力する。形式的には、以下のように表現できる。

$$h_k^\theta = F^\theta(x_k) \quad (9)$$

ここで、 $F^\theta$  はパラメータ  $\theta$  を持つニューラルネットワーク関数を表し、 $h_k^\theta$  は時点  $t_k$  におけるヘッジ比率、 $x_k$  は時点  $t_k$  における入力特徴量ベクトルである。ネットワークアーキテクチャとしては、各隠れ層に 32 ユニットを配置し、活性化関数には ReLU を用いた。最終層にはシグモイド関数を適用することで、出力を 0~1 の範囲に正規化している。この設計により、ヘッジ比率が常に 0~100% の間の値となり、実務に即した出力を行うことができる。モデルの学習には Adam 最適化アルゴリズムを採用し、学習率は 0.001、最大エポック数は 1,000 に設定した。ただし、過学習を防ぐため早期停止条件を設け、損失が 10 エポック連続で改善しない場合には学習を終了する仕組みを導入している。

ニューラルネットワークへの入力特徴量としては、時点  $t_k$  における以下の 5 次元のベクトル  $x_k$  を使用した。

- 時点  $t_k$  から満期までの残存期間  $t_n - t_k$
- 時点  $t_k$  における為替レート  $S_k$  とフロアレート（設定した目標下限損失を超過する損失が発生する為替レート）との差
- 直近 63 時点の為替レート ( $S_{k-62}$  から  $S_k$ ) から計算したヒストリカル・ボラティリティ
- 時点  $t_k$  におけるディスカウントファクター  $d_k$ （時点  $t_k$  における直物レートに対する残存期間  $t_n - t_k$  の先物レートの比率）
- 時点  $t_{k-1}$  におけるヘッジ比率  $h_{k-1}$

これらの特徴量は学習前に標準化処理を施して、モデルの学習安定性を向上させた。

2 節 (2) で記載したコストの取扱いを反映するため<sup>9</sup>、本分析では以下の表記法と数式モデルを採用する。

- $V_k$  : 時点  $t_k$  におけるヘッジ取引前の債権価値
- $V_k^+$  : 時点  $t_k$  におけるヘッジ取引後の債権価値

すなわち、右肩の + 記号は、ヘッジ取引を実行しコストを差し引いた後の状態を意味する。この表記法を用いて、時点  $t_k$  から  $t_{k+1}$  への債権価値の状態遷移を以下のよ

.....  
 9 本節の検証では、各取引時点でコストが元本から即時に差し引かれることを想定する。これにより元本が変動するため、ヘッジ比率  $h_k$  はヘッジポジション量  $\delta_k$  と異なる値になる。

うに定式化する。

$$V_{k+1} = (1 - h_k) \cdot V_k^+ \cdot \frac{S_{k+1}}{S_k} + h_k \cdot V_k^+ \quad (10)$$

$$V_{k+1}^+ = V_{k+1} - \varepsilon |\Delta U_{k+1}^D| - (1 - d_k) \Delta U_{k+1}^D \quad (11)$$

$$\Delta U_{k+1}^D = (1 - h_k) \cdot V_k^+ \cdot \frac{S_{k+1}}{S_k} - (1 - h_{k+1}) \cdot V_{k+1}^+$$

ここで、 $h_k$  は時点  $t_k$  におけるヘッジ取引後のヘッジ比率、 $\varepsilon$  は取引コスト率、 $d_k$  は時点  $t_k$  におけるディスカウントファクター、 $\Delta U_{k+1}^D$  は時点  $t_{k+1}$  におけるヘッジ取引前後の非ヘッジ部分の変化量を表す。(10) 式は、時点  $t_{k+1}$  におけるヘッジ取引前の債権価値  $V_{k+1}$  が、時点  $t_k$  の債権価値  $V_k^+$  から為替変動のみを反映した値になることを示している。右辺第 1 項は非ヘッジ部分が為替変動の影響を受けていることを表し、右辺第 2 項はヘッジ部分が為替変動の影響を受けていないことを表す。(11) 式は、時点  $t_{k+1}$  でヘッジ取引を行う際の状態遷移を示している。右辺第 1 項は、ヘッジ取引前の債権価値を表す。右辺第 2 項は、取引コストを表す。右辺第 3 項はディスカウントコストを表す。満期時点での損益は、(12) 式で計算される。

$$PL(h) = V_n - V_0 \quad (12)$$

リスク尺度については、下方リスクとして特にフロア割れを抑制しつつも、期待収益の向上も追及したいという為替リスク管理の実務における要望に応えるため、以下のリスク尺度を設計した。

$$\rho(PL(h)) = -\mathbb{E}[PL(h)] + \lambda \cdot P(PL(h)) \quad (13)$$

ここで、右辺第 1 項は期待損益の最大化を表し、右辺第 2 項はフロア割れに対するペナルティを表す。 $\lambda$  はフロア割れ回避度を表すパラメータであり、値が大きいほどフロア割れに対する回避傾向が強くなる。関数  $P$  はフロア割れに対するペナルティ関数であり、あらかじめ設定した許容損失額  $L$  (フロア) を超える損失に対してペナルティを課す形で以下のように設計する。

$$P(PL(h)) = \mathbb{E}[f(\max(-PL(h) + L, 0))] \quad (14)$$

ここで、 $f(x)$  はリスクの大きさに応じて異なるペナルティを課すため、以下のような区分関数として定める。

$$\begin{cases} f(x) = x & (x < 1 \text{ の場合}) \\ f(x) = x^k & (x \geq 1 \text{ の場合}) \end{cases} \quad (15)$$

この区分関数により、フロアを大きく下回るとペナルティが指数関数的に増加するため、フロアを大幅に割り込むことを抑制できる。以上の設計により、フロア割れ

回避度を表すパラメータ  $\lambda$  やフロア  $L$ 、ペナルティの強度を調整するパラメータ  $k$  を適切に設定することで、企業ごとの異なるリスク選好に柔軟に対応することを可能にしつつ、期待損益の最大化とフロア割れの抑制を両立する戦略の導出を図る。本稿の (15) 式では、パラメータ  $k=2$  とする。

比較対象とする CPPI モデルは、取引コストを考慮した離散時間モデルである Balder *et al.* (2009) のモデルを参考に作成した。CPPI の基本的な概念は、資産価値（本研究では外貨建て債権の円換算価値） $V$  とあらかじめ設定した資産価値の最低保証額  $F$  との差額である「クッション」 $C$  の一定割合を、リスク資産（本研究では非ヘッジ部分）に配分する戦略である。

最も単純な形式では、時点  $t_k$  における非ヘッジ部分への配分額  $E_k$  は以下の式で決定される。

$$E_k = mC_k \quad (16)$$

$$C_k = V_k - F \quad (17)$$

ここで、 $m$  は「乗数」と呼ばれるパラメータで、値が大きいほど非ヘッジ部分への配分額が増えるため、上昇相場では収益が増加し下落相場では損失が増加する。

次に、ヘッジコスト（取引コストとディスカウントコスト）を考慮した CPPI モデルを示す。具体的には、(18) 式によりヘッジコスト調整後クッション  $C_k^+$  を計算し、(19) 式によりヘッジ比率を決定する。

$$\begin{aligned} C_{k+1}^+ &= C_{k+1} - \varepsilon \left| \Delta U_{k+1}^C \right| - (1 - d_k) \Delta U_{k+1}^C \quad (18) \\ \Delta U_{k+1}^C &= mC_k^+ \cdot \frac{S_{k+1}}{S_k} - mC_{k+1}^+ \end{aligned}$$

ここで、 $\varepsilon$  は取引コスト率、 $d_k$  は時点  $t_k$  におけるディスカウントファクター、 $\Delta U_{k+1}^C$  は時点  $t_{k+1}$  におけるヘッジ取引前後の非ヘッジ部分の変化量を表す。時点  $t_k$  におけるヘッジ比率  $h_k$  は、ヘッジコスト調整後クッションを用いて、以下のように決定される。

$$h_k = 1 - \min(\max(mC_k^+/V_k^+, 0), 1) \quad (19)$$

ここで、 $V_k^+$  は時点  $t_k$  におけるヘッジ取引後の債権価値を表す。

## (2) シミュレーションの設定

為替レート過程は Heston モデル (Heston 1993) に従うと仮定し、以下のような確率微分方程式で記述する。

$$dS_t = S_t (\mu dt + \sqrt{v_t} dW_t^s) \quad (20)$$

$$dv_t = k_v (\theta_v - v_t) dt + \sigma_v \sqrt{v_t} dW_t^v \quad (21)$$

ここで、 $S_t$  は為替レート、 $v_t$  はボラティリティ、 $\mu$  はドリフト項、 $W_t^s$  と  $W_t^v$  は相関  $\rho$  をもつ標準ブラウン運動である。パラメータ  $k_v$  はボラティリティの平均回帰速度、 $\theta_v$  は長期平均ボラティリティ、 $\sigma_v$  はボラティリティのボラティリティを表す。

Heston モデルのパラメータは以下の通り設定する<sup>10</sup>。

- $\mu = 0$
- $k_v = 1.37585$
- $\theta_v = 0.01445$
- $\sigma_v = 0.16485$
- $\rho = -0.43105$

$\mu$  以外のパラメータは、Lin *et al.* (2024) により推定された 2006 年～2023 年におけるパラメータの平均値としている。

金利については、以下のような平均回帰過程を仮定する。

$$dr_t = k_r (\theta_r - r_t) + \sigma_r dW_t^r \quad (22)$$

ここで、 $r_t$  は金利、 $k_r$  は金利の平均回帰速度、 $\theta_r$  は長期平均金利、 $\sigma_r$  は金利のボラティリティ、 $W_t^r$  は  $W_t^s$  や  $W_t^v$  とは無相関な標準ブラウン運動である。日本円金利と米ドル金利について、パラメータはそれぞれ以下の通り設定する<sup>11</sup>。

日本円金利：

- $\theta_r = 0.3238\%$
- $k_r = 0.15$
- $\sigma_r = 0.8\%$

米ドル金利：

- $\theta_r = 4.311\%$
- $k_r = 0.25$
- $\sigma_r = 1.5\%$

10 為替レートの初期値  $S_0$  は 156.875 円/ドル (2025 年 1 月 1 日時点の為替レート)、ボラティリティの初期値  $v_0$  は長期平均  $\theta_v$  と同じ 0.01445 とした。

11 それぞれの初期金利は 2025 年 1 月 1 日時点の TONA および SOFR の 3 ヶ月スワップレートに基づき設定した。長期平均  $\theta_r$  は初期金利と同じとした。

金利に基づくディスカウントファクター  $d_k^Q$  は、金利平価説に従い算出されるとする。具体的には、時点  $t_k$  における満期までの残存期間  $t_n - t_k$ 、国内金利  $r_d$  と外国金利  $r_f$  を用いて、以下の式で計算される。

$$d_k^Q = \frac{1 + r_d(t_n - t_k)/252}{1 + r_f(t_n - t_k)/252} \quad (23)$$

時間は営業日（年間 252 日）で調整されている。さらに、市場における為替リスクプレミアムを適切に反映させるため、リスクの市場価格  $\alpha$  を考慮した調整を行い、以下のようにディスカウントファクター  $d_k^P$  を定義する。

$$d_k^P = d_k^Q + \alpha(t_n - t_k)/252 \quad (24)$$

ここで添え字の  $Q$  はリスク中立確率測度、 $P$  は実確率測度を表し、 $\alpha$  は本シミュレーションでは 0.015 と設定した。このディスカウントファクターは各時点で計算され、先物為替予約により為替ヘッジする際のコストとして作用する。

モデル共通のパラメータや条件としては、以下の通り設定する。

- 外貨建て債権：1 単位（1 ドル）
- 満期  $T$ ：63 営業日（約 3 カ月）
- 時間単位：日次（ $t = 1, 2, \dots, 63$ ）
- シミュレーションシナリオ数：10,000 本
- 取引コスト率  $\varepsilon$ ：0.05%
- フロア  $L$ ：-5 円（為替レートの初期値から 5 円下落相当の損失額）
- ヘッジ比率の制約：0~100%
- ヘッジ取引頻度：日次（各営業日  $t = 1, 2, \dots, 63$  において取引可能）

ディーブ・ヘッジングモデル固有のパラメータとしては、以下を設定する。

- フロア割れ回避度パラメータ  $\lambda$ ：20

CPPI モデル固有のパラメータとしては、以下を設定する。

- 乗数  $m$ ：15

以降本稿では、本節（2）のシミュレーション設定を通常環境と表記する。

### (3) シミュレーション結果

以下では、通常環境下における提案手法（ディーブ・ヘッジング）と既存手法（無ヘッジ戦略、フルヘッジ戦略、CPPI）の分析結果を提示する。評価指標として、期待損益、損益の標準偏差、95%-期待ショートフォール（95%-Expected Shortfall: 95%-ES）<sup>12</sup>、フロア割れ率およびフロア割れ時の平均超過損失を採用した。

表1は、各手法の分析結果を示している。無ヘッジ戦略は、期待損益（-0.1978）は最も高いものの、損益の標準偏差（9.498）や95%-ES（-21.0789）、フロア割れ率（29.06%）、フロア割れ時の平均超過損失（-6.5352）が最も悪く、下方リスク抑制の観点からは大きな問題を抱えている。フルヘッジ戦略は、フロア割れのリスクはないものの、期待損益は最も低い（-1.0372）。これは主に日米金利差に起因するディスカウントコストの影響であり、完全なリスク回避には相応のコストが伴うことを示している。ディーブ・ヘッジングとCPPIは、無ヘッジ戦略やフルヘッジ戦略と比べて、期待損益と下方リスク抑制のバランスが取れている。そのうえで両手法を比較すると、期待損益は、ディーブ・ヘッジング（-0.7164）がCPPI（-0.8119）より高い一方、損益の標準偏差、95%-ES、フロア割れ率、フロア割れ時の平均超過損失といった下方リスクに関する指標は、全般としてCPPIの方が優れている。特に、CPPIではフロア割れが完全に防止されているのに対し、ディーブ・ヘッジングでは0.91%のフロア割れが生じている。これは、通常環境下をベースとしたシミュレーション分析において、ディーブ・ヘッジングが厳密なフロア保証を犠牲にしても期待損益の向上を目指す戦略を学習した結果と解釈できる。

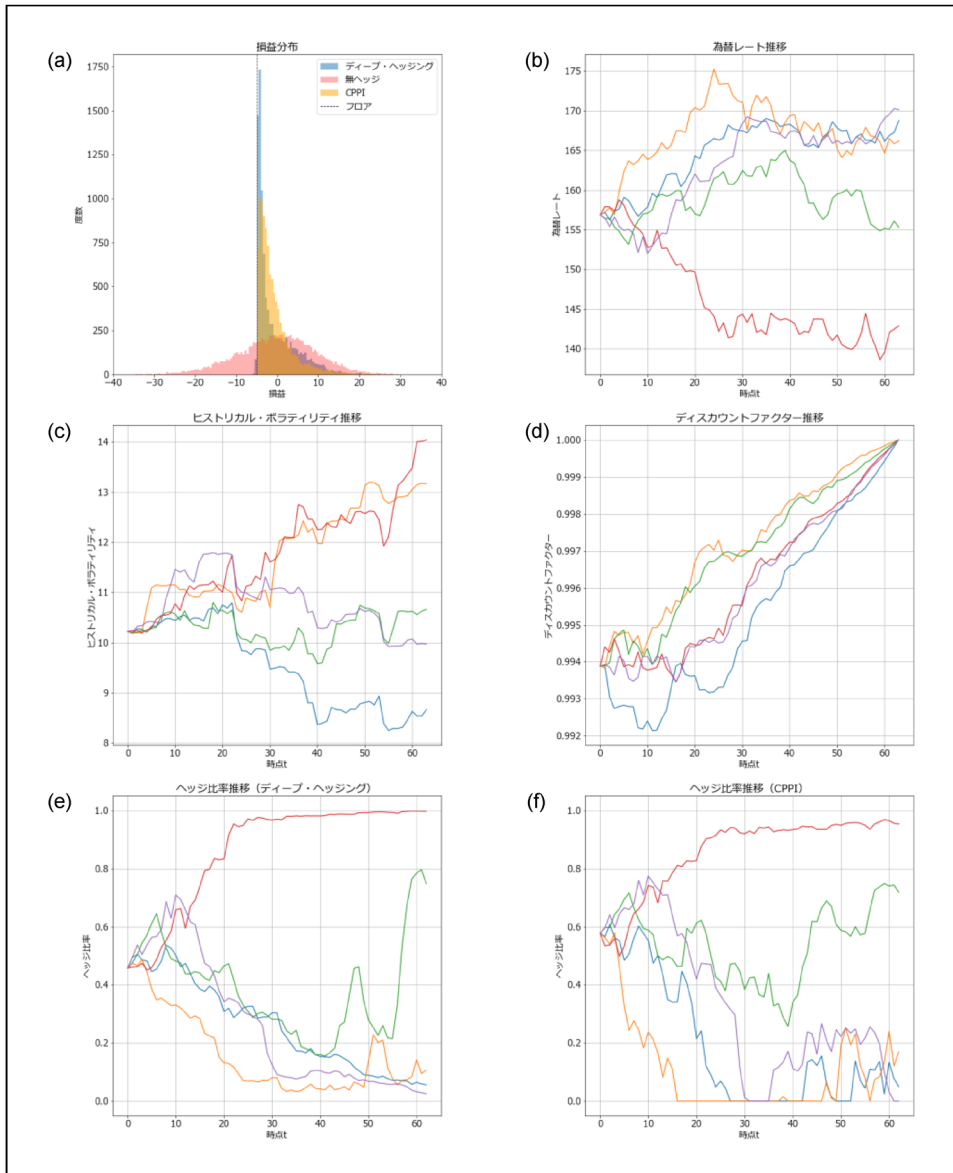
表1の結果をより直感的に理解するために、損益分布および5つのシミュレーションシナリオを図3に示す。図3aは、各手法における損益の分布（フルヘッジ戦略を除く）を表している。これを見ると、無ヘッジ戦略が最も広範囲に分布して

表1 通常環境下における各手法の比較

	ディーブ・ヘッジング	CPPI	無ヘッジ	フルヘッジ
期待損益	-0.7164	-0.8119	-0.1978	-1.0372
損益の標準偏差	4.926	4.1537	9.498	0
95%-ES	-4.9246	-4.7657	-21.0789	-1.0372
フロア割れ率	0.91%	0.00%	29.06%	0.00%
フロア割れ時の平均超過損失	-0.1513	0	-6.5352	0

.....  
12 本稿では、損益の下側5%の平均値を95%-ESとして表す。

図3 通常環境下における損益分布と代表的なシナリオ



おり、大きな上振れと下振れの可能性を示している。一方、ディープ・ヘッジングと CPPI は似たような分布形状であり、ともにフロア割れを抑制しつつも、収益機会を相応に残していることが確認できる。図 3b~3d は、代表的な 5 つのシミュレーションシナリオにおける為替レート (図 3b)、為替レートのヒストリカル・ボラティリティ (図 3c)、ディスカウントファクター (図 3d) の推移を示している。

これらのシナリオに対して、ディープ・ヘッジング（図 3e）と CPPI（図 3f）におけるヘッジ比率は、似たような動きをしていることが確認できる。

これらの結果から、本シミュレーションの設定においては、ディープ・ヘッジングは既存手法である CPPI と比較して、下方リスク抑制効果と期待損益向上効果に若干の違いはあるものの、実務的な為替リスク管理において同等程度のヘッジ効果を得られることが示された<sup>13</sup>。

#### （4） 頑健性の検証

提案手法の有効性をさらに検証するため、通常よりも厳しい市場環境下での分析や実データを用いた分析を行う。具体的には、高ボラティリティ環境下でのシミュレーション分析と、1991 年から 2024 年までの実際の市場データを用いた分析の 2 点について検証する。

##### イ. 高ボラティリティ環境下での検証

提案手法が極端な市場環境下でも有効に機能するかを検証するため、学習データは本節（2）の設定のままとし、評価データについては Heston モデルのパラメータをリーマンショック時の 2008 年のパラメータに変更して生成した。具体的には、以下のパラメータ設定を使用した。

Heston モデルのパラメータ：

- $k_v = 2.9333$
- $\theta_v = 0.0210$
- $\sigma_v = 0.3510$
- $\rho = -0.5856$

これは、高いボラティリティ ( $\theta_v = 0.0210$ ) と強い平均回帰性 ( $k_v = 2.9333$ ) を持ち、ボラティリティのボラティリティも高い ( $\sigma_v = 0.3510$ ) 状態での為替レートシミュレーションとなっている。その他のパラメータは学習データと同一である。この高ボラティリティ環境下での各手法の分析結果を、本節（3）と同様に比較した。

各手法の分析結果の比較を表 2 に示す。通常環境下での結果である表 1 と比較して、無ヘッジ戦略は、損益の標準偏差（11.3561）や 95%-ES（-27.6214）、フロア割れ率（29.57%）、フロア割れ時の平均超過損失（-8.9158）が悪化しているほか、期

13 なお、2025 年 1 月 1 日時点で、行使価格 151.875 円（直物レート -5 円）の 3 ヶ月満期ヨーロッパ・プット・オプションのプレミアムは、約 2.09 円であり、完全なフロア保証と収益機会の享受には相応のコストが必要となる。

表2 高ボラティリティ環境下における各手法の比較

	ディーブ・ヘッジング	CPPI	無ヘッジ	フルヘッジ
期待損益	-0.742	-0.8122	-0.2276	-1.0372
損益の標準偏差	5.0355	4.5292	11.3561	0
95%-ES	-5.0008	-4.9427	-27.6214	-1.0372
フロア割れ率	1.72%	0.02%	29.57%	0.00%
フロア割れ時の平均超過損失	-0.1509	-0.0035	-8.9158	0

期待損益 (-0.2276) もわずかに悪化している。フルヘッジ戦略は、ボラティリティ変化の影響を受けないため、通常環境下と変わらない結果となっている。ディーブ・ヘッジングと CPPI は、両手法とも通常環境下と比較して概ね悪化する結果となったが、両手法の相対的な関係性は維持されている。具体的には、期待損益は、ディーブ・ヘッジング (-0.742) が CPPI (-0.8122) と比較して優れた値を実現している一方、損益の標準偏差、95%-ES、フロア割れ率、フロア割れ時の平均超過損失といった下方リスクに関する指標は、全般として CPPI の方が優れた値となっている。ディーブ・ヘッジングについて、通常環境下と比較すると、フロア割れ率は悪化しているものの、フロア割れ時の平均超過損失はわずかに改善するなど、高ボラティリティ環境下でも大幅なフロア割れは抑制されている。

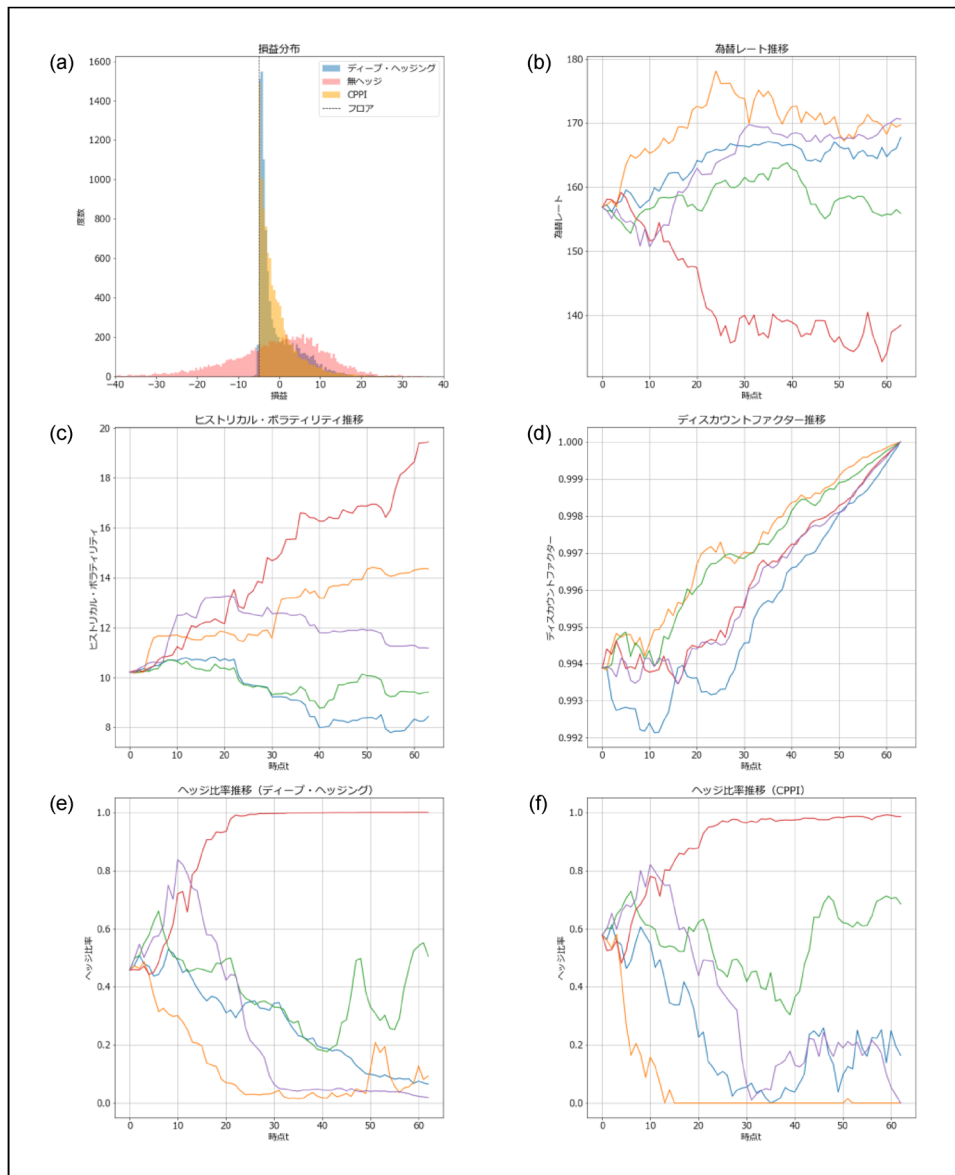
表2の結果をより直感的に理解するために、高ボラティリティ環境下における損益分布および5つのシミュレーションシナリオを図4に示す。図4aの損益分布から、高ボラティリティ環境下では、特に無ヘッジ戦略の分布がより広がっていることが確認できる。他方、ディーブ・ヘッジングと CPPI の損益分布は、通常環境下と似たような形を取っており、下方リスクを抑制できていることが示唆される。為替レート推移(図4b)やヒストリカル・ボラティリティ推移(図4c)からも、通常環境下より急激な変動が発生していることが観察できるが、このような厳しい市場環境下でも、ディーブ・ヘッジングと CPPI はいずれも、為替レートの変動に応じてヘッジ比率を適応的に調整している(図4e、図4f)。

ロ. 実データによる検証

次に、学習データは本節(2)の設定のままとして、評価データとしては、1991年1月1日から2024年12月31日までの日次の市場データを用いることで、提案手法の有効性を検証した<sup>14</sup>。実データを用いた検証では、以下の方法を採用した。

.....  
 14 市場データは LSEG Workspace より取得した。

図4 高ボラティリティ環境下における損益分布と代表的なシナリオ



- 1) 実データから連続する3ヵ月(63営業日)の期間をムービングウィンドウ方式で抽出し、各期間を1つの評価シナリオとして扱う。
- 2) ディスカウントファクターについては、金利差ではなく3ヵ月先物レートの値から、満期までの日数に応じて算出する。
- 3) 各シナリオの初日のレートを初期値として、その後63日間の市場変化に対す

る各手法の期待損益や下方リスクに関する指標を評価する。

この方法により抽出できる評価シナリオは 8,260 個であり、これらのシナリオに対する各手法の分析結果を、本節 (3) と同様に比較した。

各手法の分析結果を表 3 に示す。通常環境下での結果である表 1 と比較して、無ヘッジ戦略では、期待損益 (0.1352) が大きく増加しており、これは評価データの為替レートが円安進行していることを反映していると考えられる。また、損益の標準偏差 (6.0988)、95%-ES (-14.2787)、フロア割れ率 (17.25%)、フロア割れ時の平均超過損失 (-4.1062) も、通常環境下と比べて改善している。フルヘッジ戦略は、通常環境下と比べて、損益の標準偏差 (0.6742) や 95%-ES (-2.1225) が若干悪化しているが、期待損益 (-0.7537) は改善しており、これは評価データのデイスカウントファクターが低いことを表している。

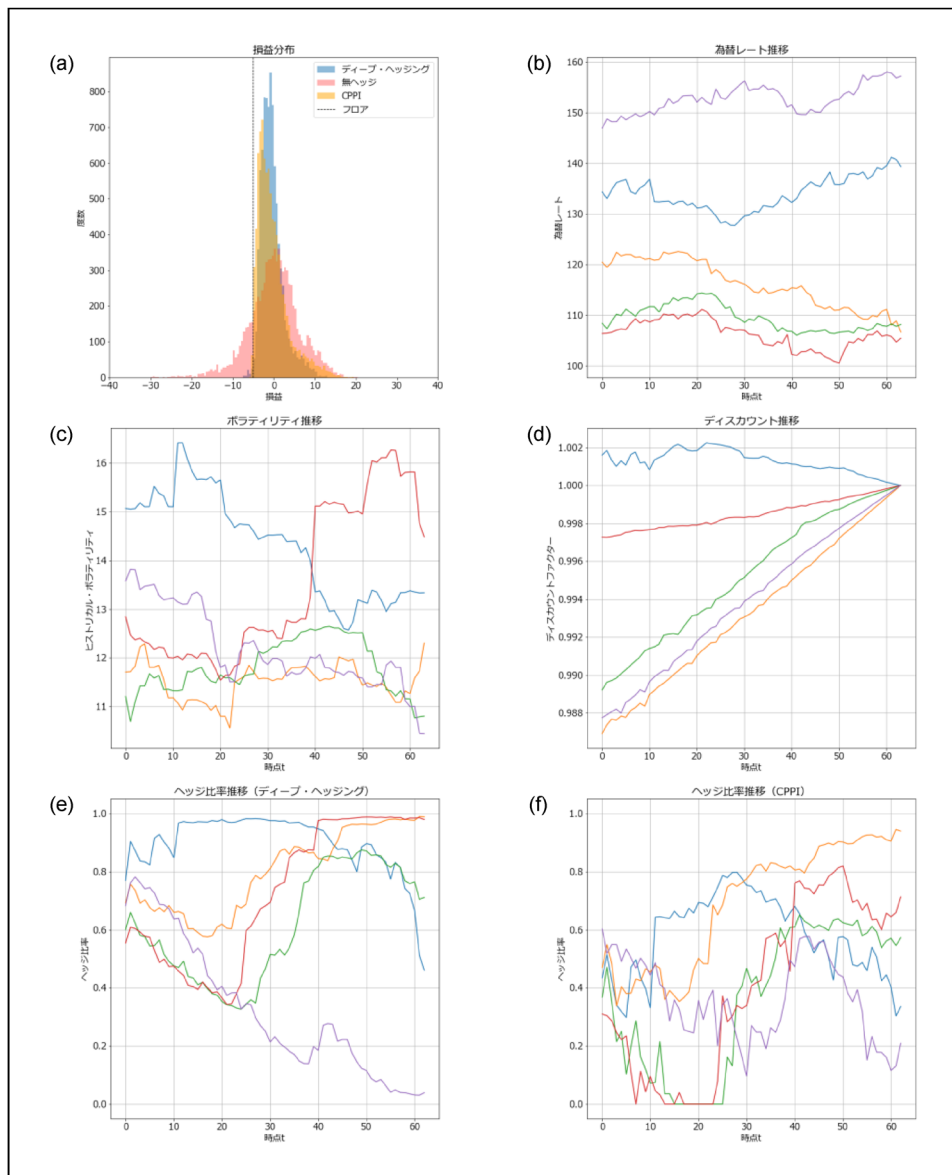
ディーブ・ヘッジングと CPPI の結果も、通常環境下と比べて多くの指標が改善している。具体的には、期待損益、損益の標準偏差、95%-ES は両手法ともに改善している。一方、フロア割れ指標については、ディーブ・ヘッジングでは、フロア割れ率は改善したものの、フロア割れ時の平均超過損失は大幅に悪化している。CPPI では、フロア割れ率とフロア割れ時の平均超過損失ともに悪化している。また、両手法の相対的な関係にも違いが見られる。シミュレーション環境下 (通常環境下、高ボラティリティ環境下) とは異なり、期待損益は、ディーブ・ヘッジング (-0.4068) が CPPI (-0.2199) に比べて劣後するようになっているほか、損益の標準偏差や 95%-ES はディーブ・ヘッジングの方が優位になっている。ディーブ・ヘッジングや CPPI のフロア割れ指標が悪化している点は、これらの手法が実データ環境下では十分には機能しない可能性を示唆している。この背景としては、例えば、実データにおいては、急激な為替や金利変動などシミュレーションでは捉えきれない市場の複雑性が存在している可能性が考えられる。ただし、両手法ともフルヘッジより、期待損益が高く、95%-ES はフロア内に収まっている。

表 3 実データ環境下における各手法の比較

	ディーブ・ヘッジング	CPPI	無ヘッジ	フルヘッジ
期待損益	-0.4068	-0.2199	0.1352	-0.7537
損益の標準偏差	2.723	3.8025	6.0988	0.6742
95%-ES	-4.3517	-4.7508	-14.2787	-2.1225
フロア割れ率	0.74%	0.72%	17.25%	0.00%
フロア割れ時の平均超過損失	-0.8583	-0.1113	-4.1062	0

表3の結果をより直感的に理解するために、実データ環境下における損益分布および5つのシナリオを図5に示す。図5aの損益分布から、多少の違いはあるものの、実データ環境下においてもディープ・ヘッジングとCPPIの分布形状は似ており、下方リスクを抑制しつつも一定の収益機会を享受していることがわかる。図5b~5dで示す市場データを見ると、シミュレーションでは捉えられない動きが観

図5 実データ環境下における損益分布と代表的なシナリオ



察できる。特に図 5d のディスカウントファクター推移の一部は、現在の日米金利差をもとに計算しているシミュレーション環境下の推移とは明確に異なっている。こうした実データ環境下においても、ディープ・ヘッジングと CPPI はいずれも、ヘッジ比率を適応的に調整している（図 5e、図 5f）。

## (5) 取引コストがヘッジ戦略に与える影響の検証

取引コストの違いがヘッジ戦略に与える影響を検証するため、取引コスト率  $\varepsilon$  をこれまでの 0.05% から 0.5% に引き上げた想定のもとで、シミュレーション分析を実施した。その他のパラメータは本節 (2) の設定と同一である。この分析により、ヘッジ取引に関するコスト負担が増大した状況下で、各手法のヘッジ効果がどのように変化するかを検証する。特に、取引コストをヘッジ戦略の導出に明示的に組み込んでいるディープ・ヘッジングと、そうでない CPPI との間にどのような差異が生じるかに着目する。

取引コストが高い場合における各手法の分析結果を表 4 に示す。通常環境下での結果である表 1 と比較して、無ヘッジ戦略は結果に変化がなく、フルヘッジ戦略は取引コストの増加分だけ結果が悪化している。これに対し、ディープ・ヘッジングと CPPI の結果を比較すると、期待損益は、ディープ・ヘッジング (-1.5218) が CPPI (-2.3594) を大きく上回り、その差は通常環境下と比べて拡大している。さらに、通常環境下とは対照的に、損益の標準偏差と 95%-ES もディープ・ヘッジングが優位となっている。他方、フロア割れ率とフロア割れ時の平均超過損失に関しては、CPPI が完全なフロア保証により引き続き優位性を保っているものの、ディープ・ヘッジングも通常環境下より改善している。これらの結果から、CPPI がフロア割れを完全に防止する特性を示す一方で期待損益を大幅に犠牲にしているのに対し、ディープ・ヘッジングは下方リスクを適切に抑制しながらもより高い期待損益

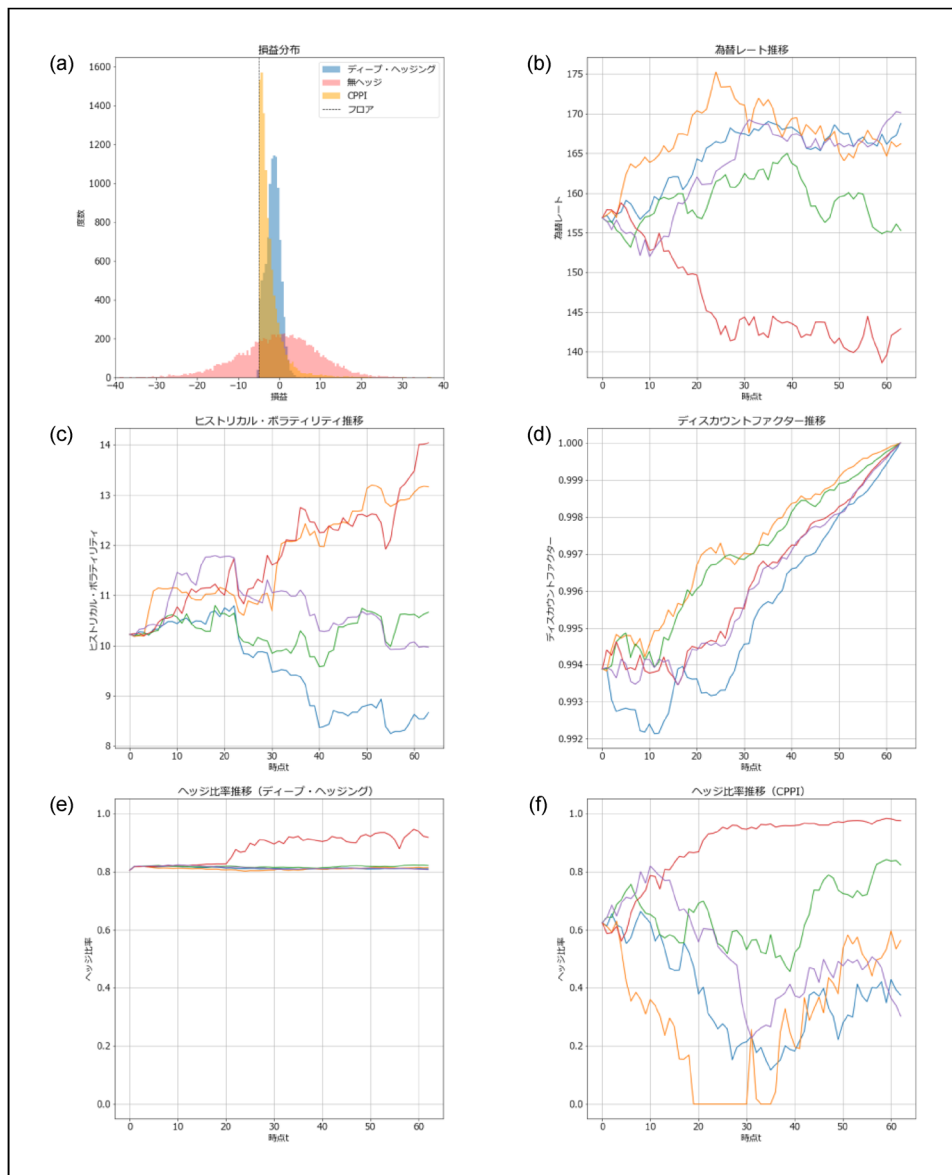
表 4 高コスト環境下での各手法の比較

	ディープ・ヘッジング	CPPI	無ヘッジ	フルヘッジ
期待損益	-1.5218	-2.3594	-0.1978	-1.7431
損益の標準偏差	1.6937	2.9636	9.498	0
95%-ES	-4.7148	-4.883	-21.0789	-1.7431
フロア割れ率	0.39%	0.00%	29.06%	0.00%
フロア割れ時の平均超過損失	-0.1095	0	-6.5352	0

を実現していることが分かる。

表4の結果をより直感的に理解するために、高コスト環境下における損益分布および5つのシミュレーションシナリオを図6に示す。図6aの各手法における損益分布から、高コスト環境下では各戦略の差異がより鮮明になっていることがわかる。ディープ・ヘッジングの損益分布はCPPIと比較して正規分布に近く、フロア

図6 高取引コスト環境下における損益分布と代表的なシナリオ



付近の頻度が小さくなることで、表4に示される期待損益の優位性と標準偏差の縮小が実現されている。為替レートや金利のシナリオ（図6b～6d）は通常環境下でのシナリオ（図3b～3d）と同一であっても、高コスト環境下では各手法のヘッジ戦略には明確な違いが生じている。CPPIのヘッジ比率推移（図6f）は通常環境下と類似しているのに対し、ディーブ・ヘッジングのヘッジ比率推移（図6e）は、高コスト環境に適応して取引頻度を抑制し、より安定的なヘッジ比率を維持しながらも、図中赤線で示されているシナリオのように為替レートが大きく下落する局面では、選択的にヘッジ比率を調整している様子が観察できる。

ディーブ・ヘッジングが取引コストの違いに適応的に対応できる点は、本研究の重要な発見である。図3eと図6eの比較から明らかなように、通常環境下では積極的な取引戦略を採用していたディーブ・ヘッジングが、高コスト環境下では必要最小限の取引に絞った慎重な戦略へと自律的に調整している。これは、提案手法が取引コストをヘッジ戦略の導出に明示的に組み込んでいることにより実現された特性である。

## (6) リスク尺度がヘッジ戦略に与える影響の検証

リスク尺度の違いがヘッジ戦略に与える影響を検証するため、フロア割れ回避度パラメータ $\lambda$ を本節(2)の20から1に下げたシミュレーション分析を実施した。その他のパラメータは本節(2)の設定と同一である。この分析により、リスク尺度のフロア割れペナルティを小さくした場合に、提案手法のヘッジ効果がどのように変化するかを検証する。

フロア割れペナルティが小さい場合における各手法の分析結果を表5に示す。通常環境下での結果である表1と比較して、無ヘッジ戦略、フルヘッジ戦略、CPPIの結果は変化しない。ディーブ・ヘッジングは、通常環境下と比べて、期待損益

表5 ペナルティが小さい場合における各手法の比較

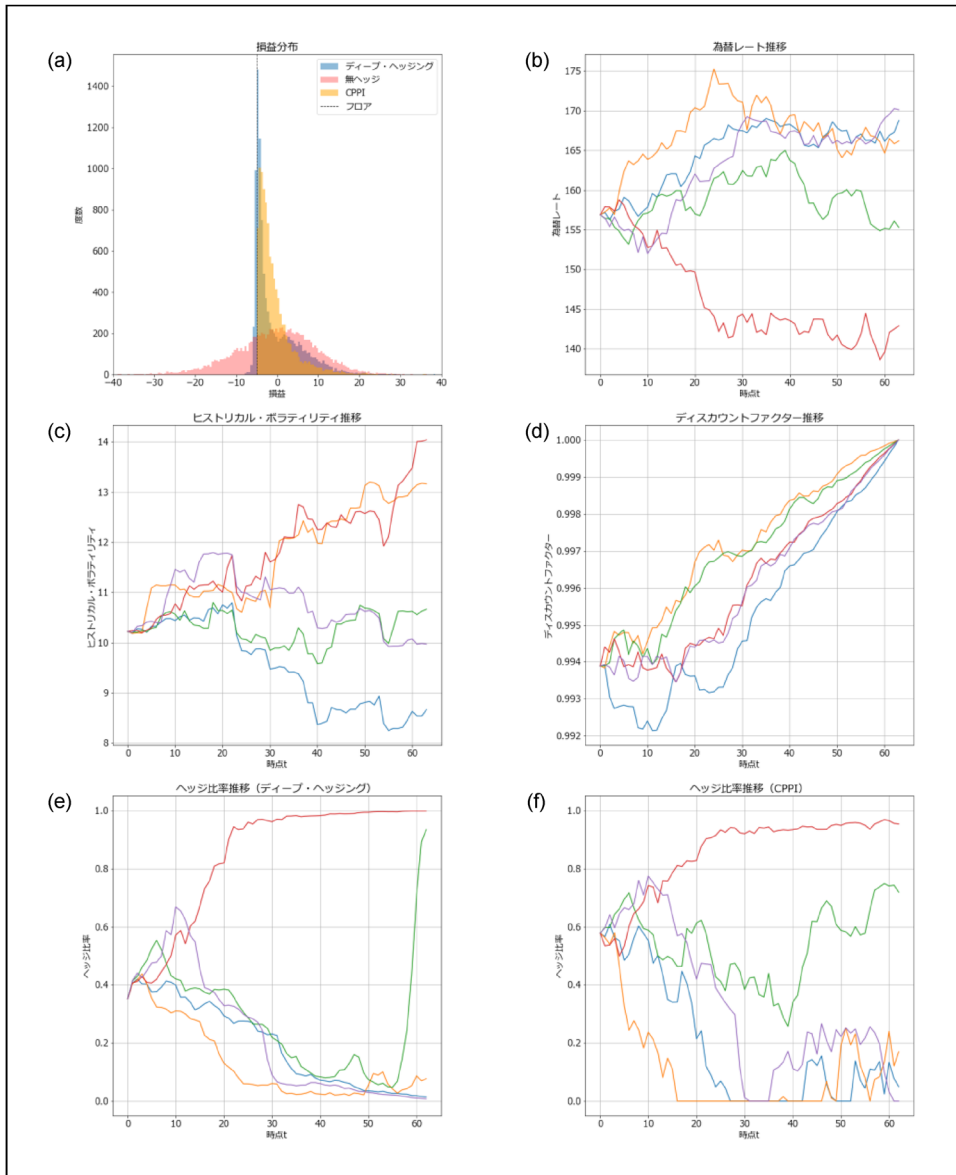
	ディーブ・ヘッジング	CPPI	無ヘッジ	フルヘッジ
期待損益	-0.6335	-0.8119	-0.1978	-1.0372
損益の標準偏差	5.4289	4.1537	9.498	0
95%-ES	-5.6897	-4.7657	-21.0789	-1.0372
フロア割れ率	12.92%	0.00%	29.06%	0.00%
フロア割れ時の平均超過損失	-0.3614	0	-6.5352	0

(-0.6335)が改善する一方、損益の標準偏差(5.4289)、95%-ES(-5.6897)、フロア割れ率(12.92%)、フロア割れ時の平均超過損失(-0.3614)といった下方リスクに関する指標は、悪化している。特に、フロア割れ率は通常環境(0.91%)と比較して大幅に悪化している。これは、ディープ・ヘッジングが、フロア割れペナルティを小さくしたことで、フロア保証よりも期待損益向上をより優先する戦略を学習した結果と解釈できる。

表5の結果をより直感的に理解するために、フロア割れペナルティが小さい場合における損益分布および5つのシミュレーションシナリオを図7に示す。図7aの各手法における損益分布から、フロア割れペナルティが小さい場合では、フロア割れが多くなっていることがわかる。為替レートや金利のシナリオ(図7b~7d)は通常環境下でのシナリオ(図3b~3d)と同一としている。この環境下において、ディープ・ヘッジングのヘッジ比率推移(図7f)は、通常環境(図3f)やCPPIのヘッジ比率推移(図7e)と大きく変わらないことが観察できる。

ディープ・ヘッジングが、フロア割れ回避度パラメータを小さくした場合に、フロア保証よりも期待損益向上をより優先する戦略を学習した点は、手法の理論的枠組みから期待される通りの結果である。この結果は、フロア保証に対する企業固有のリスク選好度をヘッジ戦略に反映できることを示している。さらに、リスク尺度の設計次第で、よりカスタマイズされたヘッジ戦略を構築できる可能性も示唆される。

図7 ペナルティが小さい場合における損益分布と代表的なシナリオ



## 5. まとめと考察

本研究では、企業の為替リスク管理における新たなアプローチとして、機械学習の活用を提案した。具体的には、企業の外貨建て貿易取引に関して、ディープ・ヘッジングを活用することで、取引コストや内外金利差を考慮したヘッジ戦略の構築を試みた。そのうえで、提案手法のヘッジ戦略の特性を考察し、次の3つの特性を明らかにした。

第1に、簡便な金融市場を想定した2項モデルを検証モデルとして提案手法のパフォーマンスを確認すると、検証モデルの理論的な最適戦略と一致する。第2に、提案手法は既存手法と比べて、特に取引コストが高い環境下において、下方リスクを抑制しつつ期待収益向上を実現するという点で優れたヘッジ効果が得られる。これは、提案手法が取引コストに応じた最適戦略を構築できることを示している。第3に、提案手法は、下方リスク抑制と期待収益向上のどちらをより重視するかといった、企業固有のリスク選好をヘッジ戦略に反映することができる。

本研究にはいくつかの限界があり、これらは今後の課題である。第1に、ディープ・ヘッジングを用いてヘッジ戦略を構築する場合、学習データと評価データが大きく乖離すると、既存の手法よりも結果が大幅に悪くなる可能性がある。このため、学習データの選択は重要な論点と考えられる。この点、学習データを生成する際にジャンプ過程を加えるなど、より現実に近いデータを生成することは改善策となりうる。第2に、ディープ・ヘッジングを含む機械学習モデルは、入力と出力の関係性がブラックボックスになりやすく、導き出されたヘッジ戦略の背景を解釈することが難しい。実務に使う場合には、実務者の理解と信頼を高め、ヘッジ戦略が得られたメカニズムをより透明化することが重要である。第3に、本研究ではドル円における63日間のヘッジ戦略を対象としているが、実務で使うには、さまざまな通貨や期間を対象としたヘッジ戦略が求められ、取り組むべき課題である。今後は、こうした課題に取り組むことで、より実務に根差した為替リスク管理の実現が期待される。

参考文献

- 伊藤隆敏・鯉淵 賢・佐藤清隆・清水順子・吉見太洋、「日本企業の為替リスク管理とインボイス通貨選択：2021年度『日本企業の貿易建値通貨の選択に関するアンケート調査』結果概要」、『RIETI Discussion Paper』24-J-004、独立行政法人経済産業研究所、2024年
- 今木翔太・今城健太郎・伊藤克哉・南 賢太郎・中川 慧、「効率的な Deep Hedging のためのニューラルネットワーク構造」、『人工知能学会第二種研究会資料』No. FIN-026、人工知能学会、2021年
- 篠崎裕司、「深層学習によるファイナンスの新展開—ディープ・ヘッジングとディープ・キャリブレーション—」、『日本銀行金融研究所ディスカッション・ペーパー・シリーズ』No. 2023-J-6、日本銀行金融研究所、2023年
- Balder, Sven, Michael Brandl, and Antje Mahayni. “Effectiveness of CPPI Strategies under Discrete-Time Trading.” *Journal of Economic Dynamics and Control* 33, no. 1 (2009): 204–220.
- Black, Fischer, and Robert Jones. “Simplifying Portfolio Insurance.” *Journal of portfolio Management* 14, no. 1 (1987): 48–51.
- Buehler, Hans, Lukas Gonon, Josef Teichmann, and Ben Wood. “Deep Hedging.” *Quantitative Finance* 19, no. 8 (2019): 1271–1291.
- Du, Xin, Jinjian Zhai, and Koupin Lv. “Algorithm Trading Using Q-Learning and Recurrent Reinforcement Learning.” unpublished manuscript, n.d. (available at <https://cs229.stanford.edu/proj2009/LvDuZhai.pdf>, 2024年12月17日).
- Fernandez-Arjona, Lucio, and Damir Filipović. “A Machine Learning Approach to Portfolio Pricing and Risk Management for High-Dimensional Problems.” *Mathematical Finance* 32, no. 4 (2022): 982–1019.
- Hambly, Ben, Renyuan Xu, and Huining Yang. “Recent Advances in Reinforcement Learning in Finance.” *Mathematical Finance* 33, no. 3 (2023): 437–503.
- Heaton, James B., Nicholas G. Polson, and Jan Hendrik Witte. “Deep Learning for Finance: Deep Portfolios.” *Applied Stochastic Models in Business and Industry* 33, no. 1 (2017): 3–12.
- Heston, Steven L. “A Closed-Form Solution for Options with Stochastic Volatility with Applications to Bond and Currency Options.” *The Review of Financial Studies* 6, no. 2 (1993): 327–343.
- Jiang, Zhengyao, Dixing Xu, and Jinjun Liang. “A Deep Reinforcement Learning Framework for the Financial Portfolio Management Problem.” arXiv:1706.10059, 2017. <http://arxiv.org/abs/1706.10059>.
- Krabichler, Thomas, and Josef Teichmann, “Deep Replication of a Runoff Portfolio.”

- arXiv:2009.05034, 2020. <https://arxiv.org/abs/2009.05034>.
- Leland, Hayne E., and Mark Rubinstein. "The Evolution of Portfolio Insurance." In *Portfolio Insurance: A Guide to Dynamic Hedging*, edited by Donald L. Luskin. Wiley, 1988.
- Lin, Shih-Kuei, Kendro Vincent, Chung-Jen Lin, and Zong-Wei Yeh. "Delta Hedging in the USD/JPY Options Market: Insights from Implied Stochastic Volatility." *Management Review* 43, no. 3 (2024): 1–17.
- Niaki, Seyed Taghi Akhavan, and Saeid Hoseinzade. "Forecasting S&P 500 Index Using Artificial Neural Networks and Design of Experiments." *Journal of Industrial Engineering International* 9, no. 1 (2013): 1–9.
- Pippas, Nikolaos, Elliot A. Ludvig, and Cagatay Turkay. "The Evolution of Reinforcement Learning in Quantitative Finance: A Survey." arXiv:2408.10932, 2025. <https://arxiv.org/abs/2408.10932>.
- Weng, Chengguo. "Discrete-Time CPPI under Transaction Cost and Regime Switching." 2014 (available at SSRN: <https://ssrn.com/abstract=2432233>).

## 金融研究所の概要

金融研究所（Institute for Monetary and Economic Studies, IMES）は1982年10月に日本銀行創立百周年を記念して、日本銀行の内部組織の1つとして設立されました。その主な目的は、(1) 金融経済の理論、制度、歴史に関する基礎的な研究の充実を図り、日本銀行の政策の適切な運営に役立てること、(2) 学界等との交流を促進すること、(3) 外部の研究活動の便宜に資する各種情報、資料等を公に提供することです。

### 主な活動

#### 研究活動

- ・ 金融経済の基本的問題に関する理論・実証的研究。
- ・ 金融関連の制度基盤（法律・会計・中央銀行制度等）に関する研究。
- ・ 金融関連の情報技術に関する研究。
- ・ 金融経済の歴史に関する研究。
- ・ 金融経済に関する歴史的資料の収集・保存・公開（アーカイブ・貨幣博物館）。

#### 顧問および客員研究員の招へい

- ・ 国内外の有力学者若干名に研究所顧問（非常勤）を委嘱し、研究所の運営、研究活動の進め方、内外学界との交流等に関する助言を受けています。
- ・ 国内外より学者数名を客員研究員として招へいし、研究活動の強化を図っています。

#### 会議の開催

- ・ 海外中央銀行、国際機関の研究者や内外の著名学者を交えた会議を開催。
- ・ 外部の研究者、専門家を交えた研究会、セミナー等を適宜開催。

#### 刊行物の発行

金融研究、Monetary and Economic Studies、IMES Discussion Paper Series、日本銀行の機能と業務、国際コンファランス議事録等を公刊（刊行物の一覧は後掲）。

#### 貨幣博物館

国内を中心とした貴重な貨幣や貨幣にかかわる資料を貨幣博物館に展示するとともに、貨幣に関する歴史資料をホームページ等で公開（博物館の案内は後掲）。

#### 歴史的公文（歴史的文書）の公開

日本銀行に関連する歴史的資料のうち、歴史的価値を有するものについて、日本銀行金融研究所アーカイブで保管・整理し、一般に公開（アーカイブの案内は後掲）。

#### 研究の委託

人員面、資料面の制約等から所内での研究が困難なテーマについて外部の学者等に研究を委託。

## 主な刊行物

### 金融研究

邦文機関誌、年4回程度発行。金融研究所の研究論文や各種ワークショップの様式、研究会報告等を公表。

### Monetary and Economic Studies

英文機関誌。『金融研究』と同様、金融研究所の研究論文等を公表（『金融研究』掲載論文の英訳のほか、英文オリジナル論文を含む）。

### IMES Discussion Paper Series (E-Series：英語版、J-Series：日本語版)

金融研究所スタッフおよび外部研究者による研究成果の未定稿を随時公表。学界、金融機関、関係者等から、広くコメントを求めることを目的としている。

### 国際コンファランス議事録

- ・ *Growth, Integration, and Monetary Policy in East Asia* (*Monetary and Economic Studies*, Vol. 25, No. S-1, 2007年)
- ・ *Financial Markets and the Real Economy in a Low Interest Rate Environment* (*Monetary and Economic Studies*, Vol. 24, No. S-1, 2006年)
- ・ *Incentive Mechanisms for Economic Policymakers* (*Monetary and Economic Studies*, Vol. 23, No. S-1, 2005年)
- ・ *Challenges for Sustained Economic Growth under Changing Economic, Social, and International Environments* (*Monetary and Economic Studies*, Vol. 22, No. S-1, 2004年)
- ・ *Exchange Rate Regimes in the 21st Century* (*Monetary and Economic Studies*, Vol. 20, No. S-1, 2002年)
- ・ *The Role of Monetary Policy under Low Inflation: Deflationary Shocks and Policy Responses* (*Monetary and Economic Studies*, Vol. 19, No. S-1, 2001年)
- ・ *Monetary Policy in a World of Knowledge-Based Growth, Quality Change and Uncertain Measurement* (Palgrave, 2001年)
- ・ *Towards More Effective Monetary Policy* (Macmillan Press, 1997年)
- ・ *Financial Stability in a Changing Environment* (Macmillan Press, 1995年)
- ・ *Price Stabilization in the 1990s: Domestic and International Policy Requirements* (Macmillan Press, 1993年)
- ・ *The Evolution of the International Monetary System: How Can Efficiency and Stability Be Attained?* (University of Tokyo Press, 1990年)
- ・ *Toward a World of Economic Stability: Optimal Monetary Framework and Policy* (University of Tokyo Press, 1988年)
- ・ *Financial Innovation and Monetary Policy: Asia and the West* (University of Tokyo Press, 1986年)
- ・ *Monetary Policy in Our Times* (MIT Press, 1985年)

なお、2008年以降に開催された国際コンファランスについては、議事要旨等を *Monetary and Economic Studies* に所収。

**日本銀行の機能と業務**（有斐閣、2011年発行）

日本銀行がどのような役割・機能を担い、また、これを果たすため、どのような業務を行っているのかについて、網羅的かつ具体的に解説。

**貨幣博物館 常設展示図録**（ときわ総合サービス、2017年発行）

貨幣博物館の展示資料を紹介した図録です。

日本銀行金融研究所（IMES）

〒103-8660 東京都中央区日本橋本石町 2-1-1

TEL：03-3279-1111

E-mail：imes.journals-info@boj.or.jp

ホームページ：https://www.imes.boj.or.jp

## 資料公開サービス

以下の資料公開サービスを行っておりますので、ご利用下さい。

### (1) 貨幣博物館の公開

2015年11月、貨幣博物館はリニューアルオープンしました。日本の貨幣を中心に、和同開珎や大判・小判の実物、貨幣に関する絵画など、貴重な資料を多数展示するとともに、所蔵資料を貨幣博物館ホームページ等で一般に公開しています。20名以上の団体で見学を希望される場合は予め電話でご連絡下さい。

開館時間：9時30分～16時30分（入館は16時まで）

休館日：月曜日（ただし祝休日は開館）

年末年始（12月29日～1月4日）

※最新の情報は下記の当館ホームページで

お知らせいたしますので、ご確認下さい。

貨幣博物館ホームページ：<https://www.imes.boj.or.jp/cm/>

〈連絡先〉金融研究所 貨幣博物館

TEL：03-3277-3037（直通）

### (2) 日本銀行が保有する歴史的公文（歴史的文書）の公開

金融研究所では、日本銀行に関連する歴史的資料のうち、歴史的価値を有するものについて保管・整理し、一般に公開しています。閲覧をご希望の方は、当館ホームページ掲載の目録で検索のうえ、予めメール・電話にてご連絡下さい。

歴史的公文の目録：<https://www.imes.boj.or.jp/archives/hozon.html>

〈連絡先〉金融研究所 アーカイブ

E-mail：[imes.archives@boj.or.jp](mailto:imes.archives@boj.or.jp)

TEL：03-3277-2151（直通）

金 融 研 究 (第45巻第2号)

ISSN 2759-5099

2026年4月20日 発行

日本銀行金融研究所長

編集兼発行者 渡 辺 真 吾

発 行 所 日本銀行 金融研究所

郵便番号 103-8660

東京都中央区日本橋本石町 2-1-1

電 話 : (03) 3279-1111 (大代表)

国際文献社

本誌に関する照会は、日本銀行金融研究所までお寄せ下さい。

