リスクガバナンス

基本的な考え方

〈みずほ〉はグローバルな金融機関としての責務のもと、お客さま、経済・社会とともに持続的に成長・発展するため、リスクアペタイト・フレームワークを通じて事業戦略・財務戦略の遂行とリスク管理の運営を一体化し、適切なリスクテイクとリスクコントロールを推進します。

「リスクの本質を理解し、立場を超えたオープンなコミュニケーションを通じて、リスクテイクの適切さを常に追求する」それが、リスクに向き合う際の私たちの基本姿勢です

執行役 グループCRO　白石 志郎

2024年度のトップリスクの選定にあたっては、国内外のマクロ環境や金融政策の行方に対するリスク認識に加え、気候変動、自然の損失、人権侵害等の環境・社会課題に対する社会的な目線の一段の高まり、生成AIがもたらすリスク等について議論を重ねてきました。各トップリスクに対しては様々なコントロール策を講じていますが、ここでは中期経営計画の注力テーマとも関連する3つの取り組みをお伝えします。

1つ目は、不透明感の高まる国内および海外の金融経済環境への備えについてです。信用リスクについては、金利上昇がマクロ経済や企業業績に与える影響について様々なシミュレーションにより精査し、適切なリスク・リターンを踏まえたリスクテイクを推進しています。また、ドル円相場が歴史的な円安水準となる等ボラタイルな市場環境となっていますが、市場・流動性リスクについては、各国金融政策の動向を注視し、ここ数年の米欧の急ピッチな利上げによるマーケット変動からの学びも活かしながら、フォワードルッキングなリスクコントロールに取り組んでいます。

2つ目は、グローバルなリスク管理についてです。米州のGreenhill買収等、〈みずほ〉は着実にグローバルCIBビジネスの裾野を広げていますが、グローバルに銀行・証券機能を提供するためのリスク管理態勢についても、米州・EMEA・APACの各地域で強化しています。

最後に、経営基盤強化についてです。サイバーセキュリティリスク等、リスクの高まりが顕著な領域への備えや、AIの急速な普及による新たなリスクの可能性にも意を用いることが必要です。安定的な金融サービス提供のため、オペレーショナル・レジリエンスの観点も踏まえリスク管理の高度化を図ってまいります。

足元では国内外ともに、これまでになく不確実性が高まっています。リスクアペタイト・フレームワークのもとでフォワードルッキングに内外環境を見極め、機動的かつ適切なリスクテイクとリスクコントロールによる戦略遂行が重要な一年です。リスクと機会を俯瞰的に把握・評価し、グループ・グローバルベースで適切なリスク管理を推進してまいります。

トップリスク

米欧のインフレ再燃と景気減速	国内物価・金利上昇と財政懸念の拡大	米中対立の激化と中国経済の低迷
世界の分断と地政学リスクの高まり	気候変動影響の深刻化	システム障害
サイバー攻撃	マネロン・テロ資金供与	役員・職員による不適切な行為・不作為
人材不足等による持続的成長の停滞	競争環境の変化	

（2024年3月時点）

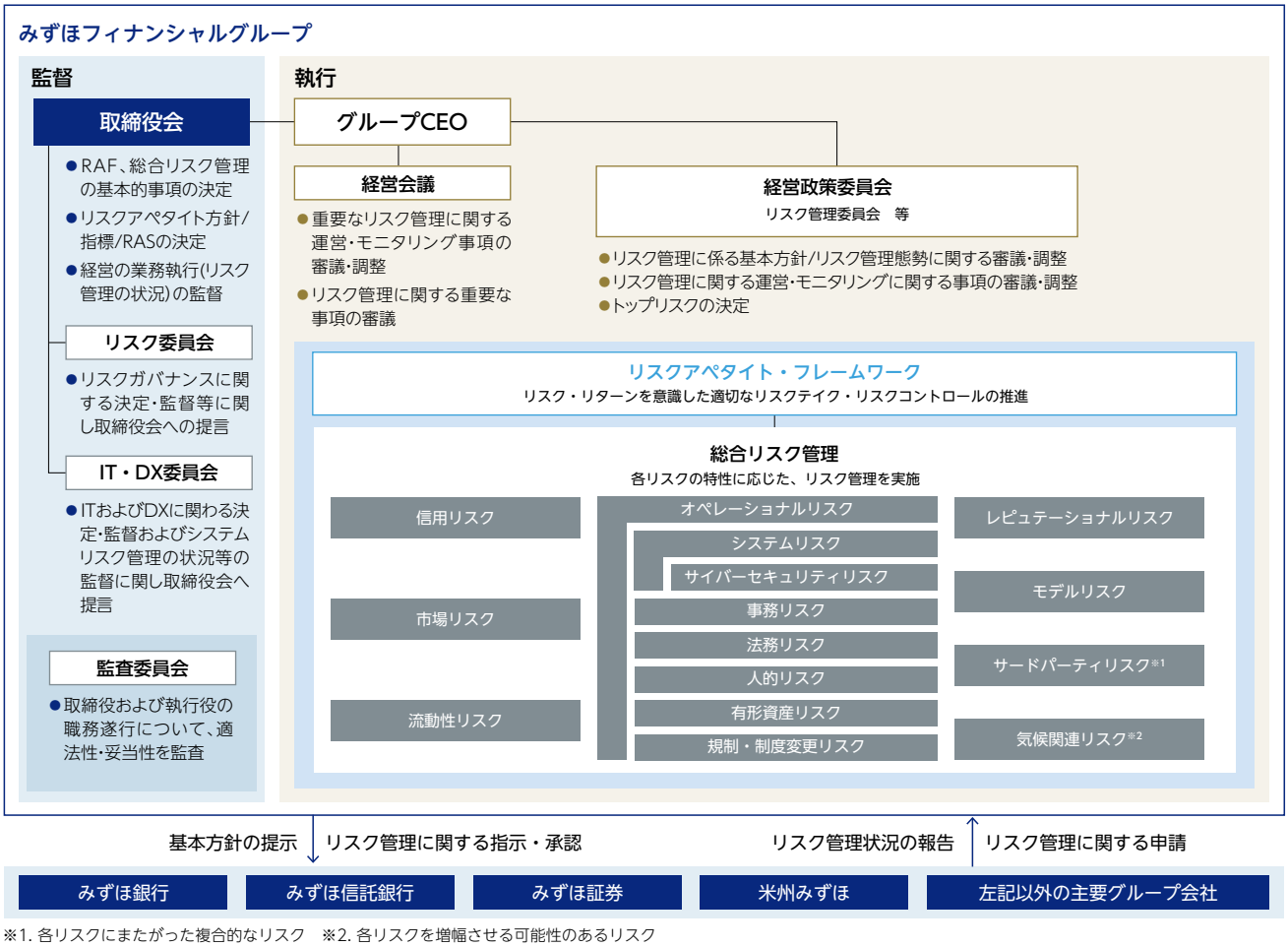
リスクアペタイト・フレームワーク（RAF）

〈みずほ〉はRAFを、リスクアペタイト（事業戦略や財務戦略を実現するために受け入れるリスクの種類と水準）に沿ったリスクテイクを実現するための経営管理の枠組みと位置付けています。RAFにより戦略とリスク管理を一体的に運営し、適切なリスクテイクとリスクコントロールを通じた最適なリスク・リターンの実現をめざしています。

RAFの具体的な運営では、取締役会がRAFに関する基本的事項、およびRAFの運営態勢やリスクアペタイト等を文書化したリスクアペタイト・ステートメント（RAS）を決定し、当該決定に基づく経営の業務執行を監督しています。また、取締役会の諮問機関であるリスク委員会は、RAFに関する事項等について取締役会へ提言を行っています。一方、業務執行では、グループCEOの統括のもと、グループCRO、グループCFOおよびグループCSOがこれを補佐し、事業・財務戦略とリスク管理の一体運営を行っています。

リスクアペタイトの設定では、トップリスク等のリスク事象を経営で議論し、これらを組織内で共有するためのベースラインシナリオおよびリスクシナリオを策定しています。そして、これらの内外環境に関する認識を踏まえて、中期経営計画や業務計画と整合したリスクアペタイト方針を策定します。また、資本力・収益力・流動性等について、定量的なリスクアペタイト指標とその水準を設定しています。リスクアペタイト方針およびリスクアペタイト指標・水準は取締役会で決定します。リスクアペタイトの運営状況は定期的にモニタリングを実施し、取締役会等へも報告を行います。また、環境や戦略に変化があれば、必要に応じてリスクアペタイトの見直しも都度実施します。

〈みずほ〉のリスク管理態勢



※1. 各リスクにまたがった複合的なリスク　※2. 各リスクを増幅させる可能性のあるリスク

ストレステスト

〈みずほ〉では、リスクアペタイトの適切性や業務計画等の妥当性を検証するために、自己資本比率や業績等への影響を算出・評価するストレステストを実施しています。

ストレステストは、足元の経済状況や今後の見通し、〈みずほ〉の事業・財務構造の脆弱性等を踏まえてシナリオを設定し、実施しています。ストレス状況においても必要な自己資本比率や業績等を確保できることを確認し、必要な水準を下回る場合には、リスクアペタイトや業務計画等の見直しを検討・実施します。また、規制資本には含まれていないバンキング勘定の金利リスク等も含めたリスク量への影響を算出し、それらと自己資本とのバランスを確認することで、自己資本充実度の評価に活用しています。

加えて、流動性リスクおよび市場リスク等のリスクカテゴリーごとの管理においてもストレステストを行い、頑健なリスク管理態勢を構築しています。

〈みずほ〉の自己資本関連のストレステスト

1. シナリオの設定	2. 影響の算出	3. 結果の分析・活用
●足元の経済状況や今後の見通し ●〈みずほ〉の事業・財務構造の脆弱性	●リスクシナリオ発生時の当社グループへの影響を算出 ●主要な算出項目：自己資本比率、損失、VAR（Value at Risk）等	●リスクアペタイトの適切性や業務計画等の妥当性検証 ●自己資本充実度の評価

サイバーセキュリティ

基本的な考え方

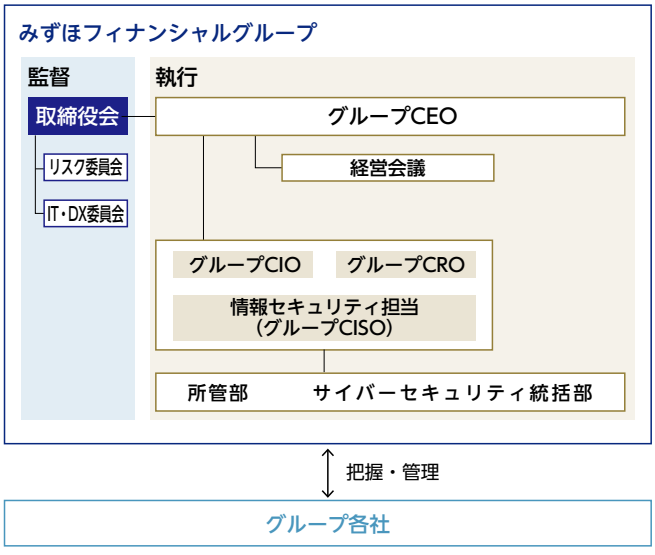
2023年は不正アクセスによる企業の個人情報流出やフィッシングによる不正送金被害額が過去最高額を記録する等、サイバー攻撃手口の高度化による被害が拡大しています。〈みずほ〉では、お客さまに安心してサービスをご利用いただけるよう、「サイバーセキュリティ経営宣言」に基づいて、継続的にサイバーセキュリティ対策を推進しています。

サイバーセキュリティ経営宣言　https://www.mizuho-fg.co.jp/company/activity/cybersecurity/index.html

ガバナンス体制

〈みずほ〉では、当社グループ・グローバルのサイバーセキュリティ管理業務全体を統括するグループCISO※を設置しています。グループCISOをグループCIOに対する2線機能における牽制機能明確化の観点から、グループCIOおよびグループCROに対して報告するダブルレポーティング体制をとることで、サイバーセキュリティ態勢強化を図っています。グループCISOはサイバーセキュリティリスク管理や各種対策の推進における責任者として経営会議・取締役会に報告し、経営と一体となりサイバーセキュリティに関する方針や資源配分を適時適切に見直しています。

また、子会社においてサイバーセキュリティ責任者を設置し、連絡体制を整備することにより、子会社におけるサイバーセキュリティ対策状況の把握やインシデント発生時の迅速な情報集約を実現しています。



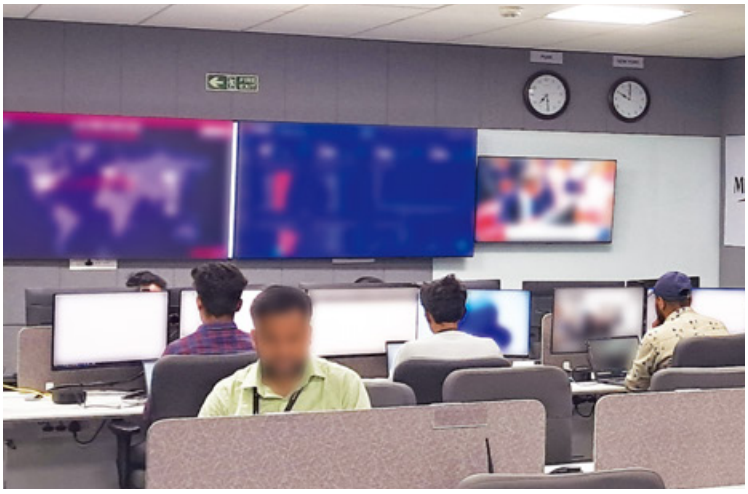
※ Chief Information Security Officer

インシデント発生時の体制

〈みずほ〉ではSOC※1およびMizuho-CIRT※2等の専門部隊を設置し、外部の専門機関とも連携のうえ、インシデント対応を行っています。SOCは24時間365日の監視体制でインシデントの予兆となる不審なログ等を検知しており、Mizuho-CIRTはSOCの検知情報をもとに、社内外への情報連携やインシデント発生時の対応・調査・復旧等を実施します。

これら専門部隊は、有事に備え、日頃からサイバー攻撃手法ごとの対応フローを制定し、手続きに沿った対応ができるよう社内外で訓練・演習を行っています。

※1．Security Operation Center（企業等の組織において、情報システムに対する脅威の監視や分析等を行う役割や専門チーム）
※2．Cyber Incident Response Team（組織内の情報セキュリティ上の問題を専門に扱うインシデント対応チーム）



海外における監視の様子

サイバーセキュリティ対策の取り組み状況

〈みずほ〉ではグループ・グローバルおよびサプライチェーンを含めたサイバーセキュリティ対策を推進しています。サイバーセキュリティリスクの特定・発現の未然防止のため、公的機関や信頼できるコミュニティ・メディア等から脅威インテリジェンスを収集し、当社に与えうる影響を踏まえて、優先度をつけた対策を実施しています。

近年のシステムは絶え間なく多種多様なセキュリティの脅威にさらされるため、システムの企画工程から開発工程、運用工程まで含めたすべてのシステム開発ライフサイクルにおいて一貫したセキュリティを確保するための対策を行っています。

当社システムでは、ウイルス解析や多層的防御体制等を導入しており、これら技術的な対策の有効性や対応プロセスの実効性をテストするためにTLPT※1を実施する等、レジリエンス態勢の強化に取り組んでいます。

〈みずほ〉では、これらサイバーセキュリティ対策の成熟度を評価するため、FFIEC※2 Cybersecurity Assessment Toolによる第三者評価の実施やNIST※3のCybersecurity Framework等を参考にしています。

※1．Threat-Led Penetration Testing（攻撃対象の脅威を分析のうえ、実際の攻撃を模した攻撃を行い、システムや対応プロセスを評価する）
※2．Federal Financial Institutions Examination Council(米国連邦金融機関検査協議会)
※3．National Institute of Standards and Technology（米国立標準技術研究所）

サイバーセキュリティ人材の育成

〈みずほ〉では、サイバーインシデント等が発生した場合に組織的に適切な対応が取れるかを定期的に検証し、認識した課題等を確実に解消することで個人および組織的なインシデント対応力を強化していくことが大切であると考えています。

経営層を含めたインシデント対応訓練や役職レイヤーごとのサイバーセキュリティ研修、全役員・社員向けに半年に1回以上フィッシングメール訓練を実施する等、社内外の研修・訓練・演習を通して必要な意識、知識、スキル等を役員・社員一人ひとりが身につけています。

また、専門資格取得に向けた積極的な支援や専門機関のプログラム受講による社員育成のほか、キャリア採用を積極的に進めるとともに、新卒採用ではITシステムコースを設立する等、高度な専門性を持つ人材を獲得・育成しています。