リスク管理

1. リスク管理の基本方針

当グループは、経営健全性の確保、経営戦略に基づくリスクテイクを通じた収益確保、持続的成長のため、グループ経営方針、内部統制基本方針に基づき、リスクの特定、評価、モニタリング、コントロールおよび削減、高度化検証・見直しなどの一連のリスク管理活動をとおして、リスクの状況を的確に把握し、リスクに対して必要な措置を講じることを基本方針としています。

当グループのリスク管理のフレームワークは、リスクアペタイト・フレームワークを取り込み、一体化してグループ内で有機的に機能しています。

2. 当グループのリスク特性

当グループは、信託銀行グループとして、信託の受託者精神に立脚し、高度な専門性と総合力を駆使して、銀行、資産運用・資産管理、不動産などを融合したトータルソリューション型ビジネスモデルで独自の価値を創出することを目指しています。

当グループの各事業はそのビジネス特性に応じ、信用リスク、市場リスク、資金繰りリスクおよびオペレーショナル・リスクといったさまざまなリスクにさらされています。

こうしたなか、信託業務関連のリスクについては、留意すべき基本的事項を取りまとめたグループベースの「信託業務指針」を管理高度化の礎として制定しているほか、三井住友信託銀行では、信託受託者としての善管注意義務・忠実義務・分別管理義務などの観点も加え、信託業務関連のリスクについて主にオペレーショナル・リスクのカテゴリーで管理しています。

各事業のリスク量を合算した当グループ全体のリスク量が、取締役会が決定したリスクキャパシティ（健全性・流動性）の範囲内におさまっているかどうかなどを定期的に報告しています。

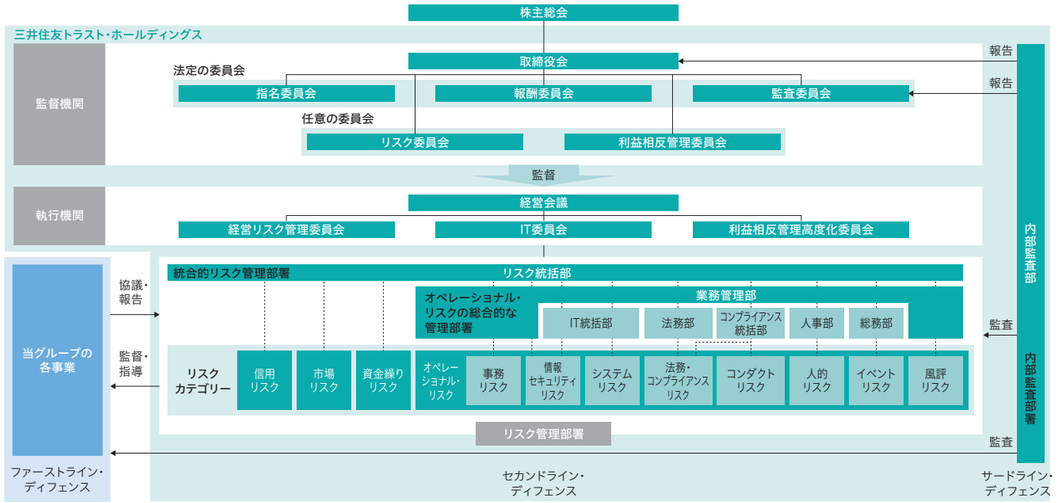
■ リスクの定義

リスクカテゴリー		定　義
信用リスク		信用供与先の財務状況の悪化などにより、資産（オフ・バランス資産を含む）の価値が減少ないし消失し、当グループが損失を被るリスクをいいます。このうち、特に、海外向け信用供与について、取引先の属する国の外貨事情や政治・経済情勢などにより当グループが損失を被るリスクをカントリーリスクといいます。
市場リスク		金利、為替、株式、コモディティ、信用スプレッドなどのさまざまな市場のリスク要因の変動により、保有する資産・負債（オフ・バランスを含む）の価値、あるいは資産・負債から生み出される収益が変動し、当グループが損失を被るリスクをいいます。このうち、特に、市場の混乱などにより市場において取引ができなかったり、通常よりも著しく不利な価格での取引を余儀なくされることにより当グループが損失を被るリスクを、市場流動性リスクといいます。
資金繰りリスク		必要な資金が確保できず資金繰りがつかなくなる場合や、資金の確保に通常よりも著しく高い金利での調達を余儀なくされることにより当グループが損失を被るリスクをいいます。
オペレーショナル・リスク（略称「オペリスク」） （下記はオペリスク内の「リスクサブカテゴリー」）		業務の過程、役員・社員の活動もしくはシステムが不適切であること、または外生的な事象により、当グループ・顧客・市場・金融インフラ・社会および職場環境に対し悪影響を与えるリスクをいいます。
	事務リスク	役員・社員が正確な事務を怠る、あるいは事故・不正などを起こすなど、事務が不適切であることにより当グループが損失を被るリスクをいいます。
	システムリスク	コンピュータシステムのダウン、または誤作動、システムの不備などに伴い当グループが損失を被るリスク、さらにコンピュータが不正に使用されることにより、当グループが損失を被るリスクをいいます。
	情報セキュリティリスク	情報の漏えい、情報が正確でないこと、情報システムが利用できないこと、情報の不正使用など、情報資産が適切に維持・管理されないことにより、当グループが損失を被るリスクをいいます。
	法務・コンプライアンスリスク	取引の法律関係が確定的でないことによって当グループが損失を被るリスク、および法令等の遵守状況が十分でないことにより当グループが損失を被るリスクをいいます。
	コンダクトリスク	グループ各社・役員または社員の行為が、職業倫理に反していること、またはステークホルダーの期待と信頼※に応えていないことにより、当グループ・顧客・市場・金融インフラ・社会および職場環境に対し悪影響を与えるリスクをいいます。 ※合理的な期待水準を把握の上、当グループとして設定する適切なサービスレベル
	人的リスク	人事運営上の不公平・不公正、ハラスメントなど、人事・労務管理上の問題により当グループが損失を被るリスクをいいます。
	イベントリスク	自然災害、テロなどの犯罪、社会インフラの機能障害、感染症の流行など、事業の妨げとなる外生的事象、または有形資産の使用・管理が不適切であることにより当グループが損失を被るリスクをいいます。
	風評リスク	マスコミ報道、風評・風説などによって当社または子会社などの評判が悪化することにより当グループが損失を被るリスクをいいます。

3. リスクガバナンス体制

当グループは、グループ全体のリスクガバナンス体制として、各事業によるリスク管理（ファーストライン・ディフェンス）、リスク統括部およびリスク管理各部によるリスク管理（セカンドライン・ディフェンス）、内部監査部による検証（サードライン・ディフェンス）の三線防御体制（スリーラインズ・オブ・ディフェンス）を構築しています。

■ リスクガバナンス体制



(1) ファーストライン・ディフェンス

グループ各事業は、業務商品知識を活かして自事業の推進におけるリスク特性の把握を行います。各事業は定められたリスクテイクの方針に基づき、リスクアペタイトの範囲内でリスクテイクを行うとともに、リスクを評価し、リスクが顕在化した際には現場レベルでのリスクコントロールを迅速に実行します。また、リスク管理の状況をセカンドラインに適時に報告します。

(2) セカンドライン・ディフェンス

リスク統括部およびリスク管理各部は、各リスクカテゴリーの管理部署として、取締役会によって決定されたグループ全体のリスク管理方針に従い、ファーストラインから独立した立場で、ファーストラインのリスクテイクへの牽制機能を発揮し、リスクガバナンス体制の監督・指導を行います。

リスク統括部は、統合的リスク管理部署として、グループ全体を対象にリスクを特定・評価し、リスク管理プロセスを構築し、リスク限度枠の設定を行うほか、リスクが顕在化した場合の全社リカバリー戦略をあらかじめ策定します。また、リスク管理各部と適切に情報共有を行い、リスクおよびリスク管理全体の状況を統合的にモニタリングし、その状況を経営会議、取締役会へ報告します。

(3) サードライン・ディフェンス

内部監査部は、グループのリスクガバナンス体制およびプロセスの有効性や適切性をファーストライン、セカンドラインから独立した立場で検証します。

(4) 経営会議

経営会議は、代表執行役ならびに執行役社長が指定する執行役をもって構成され、リスク管理に関する事項の決定および取締役会決議・報告事項の予備討議を行います。

(5) 取締役会

取締役会は、取締役全員をもって組織され、当グループの経営方針およびリスクテイクの戦略目標を決定し、リスクの所在と性質を十分認識した上で、戦略目標を踏まえたリスク管理方針などを策定し、適切なリスクガバナンス体制を整備し、実施状況を監督します。また、取締役会は当グループのビジネス戦略やリスクの特性を踏まえ、任意の諮問機関として「リスク

委員会」および「利益相反管理委員会」を設置しています。

•リスク委員会

リスク委員会は、当グループの経営を取り巻く環境認識に関する事項、リスク管理の実効性に関する事項などに関し、取締役会からの諮問を受けてその適切性などを検討し、答申を行います。

•利益相反管理委員会

利益相反管理委員会は、信託の受託者精神に基づき当グループが目指す、お客さまの「ベストパートナー」の基盤となる、フィデューシャリー・デューティーおよび利益相反管理に関する事項に関し、取締役会から諮問を受けてその適切性などを検討し、答申を行います。

4. リスク管理のプロセス

当グループでは、リスク統括部およびリスク管理各部がセカンドラインとして、以下の手順でリスク管理を行います。また、このリスク管理プロセスについては、関連するシステムを含め、サードラインの内部監査部により定期的に監査されます。

(1)リスクの特定

当グループの業務範囲の網羅性も確保した上で、直面するリスクを網羅的に洗い出し、洗い出したリスクの規模・特性を踏まえ、管理対象とするリスクを特定します。この中で、特に重要なリスクを「重要リスク」として管理します。

(2)リスクの評価

管理対象として特定したリスクについて、事業の規模・特性およびリスクプロファイルに見合った適切なリスクの分析・評価・計測を行います。「重要リスク」については、定期的に、「発生頻度」「影響度」および「重要度」を評価し、トップリスク(1年以内に当グループの事業遂行能力や業績目標に重大な影響をもたらす可能性があり、経営上注意すべきリスク)やエマージングリスク(1年超、中長期に重大な影響をもたらす可能性があるリスク)などに該当するかどうかの判断を行います。

(3)リスクのモニタリング

当グループの内部環境(リスクプロファイル、配分資本の使用状況など)や外部環境(経済、市場など)の状況に照らし、リスクの状況を適切な頻度で監視し、状況に応じ、グループ各事業に対して勧告・指導または助言を行います。モニタリングした内容は、定期的にまたは必要に応じて取締役会、経営会議などへ報告・提言します。

トップリスクなどの予兆管理

当グループのビジネスモデルの特徴とリスク特性を踏まえ、内生要因リスクについては「リスクアペタイト指標」を設定し、管理指標をモニタリングしています。また、外生要因リスクについては、トップリスクなどを選定した上で、予兆指標をモニタリングしています。いずれのリスクも、モニタリング結果を踏まえて対応策などを講じています。

トップリスクについては、現状、「新型コロナウイルス感染症の世界的流行に関するリスク」などを選定し、対応策とともに取締役会、経営会議に報告しています。また、エマージングリスクについては、現状、「気候変動に関するリスク」などを選定し、リスクの分析と必要な対応策を検討しています。

当グループの主なトップリスクとエマージングリスクについては、下表をご参照ください。

■主なトップリスクとエマージングリスク

トップリスク	新型コロナウイルス感染症の世界的流行に関するリスク
	政策保有株式等の価格下落に関するリスク
	信用ポートフォリオにおける大口与信先への与信集中リスク
	サイバー攻撃に関するリスク
エマージングリスク	気候変動に関するリスク※
	イノベーションに関するリスク
	日本の少子高齢化の進展に関するリスク

※当グループでは、保有するポートフォリオについて主な気候関連リスクを特定しシナリオ分析を実施するなど、リスク管理の高度化に向けた取り組みを進めています。詳細は、「TCFDレポート」(2020年12月発行)をご参照ください。

(4)リスクのコントロールおよび削減

リスク量がリスク限度枠を超過したとき、もしくは超過が懸念されるなど、経営の健全性に重大な影響を及ぼす事象が生じた場合には、取締役会、経営会議などに対して適切に報告を行い、リスクの重要度に応じ、必要な対応策を講じます。

5. 統合的リスク管理

(1)統合的リスク管理体制

当グループでは直面するリスクに関して、それぞれのリスクカテゴリーごとに評価したリスクを総合的に捉え、経営体力と比較・対照することによって、リスク管理を行っています(統合的リスク管理)。

当グループでは、年に1回、リスク管理やリスクコントロールの実効性を評価し、環境変化などにより必要が生じたと判断した場合は、リスクカテゴリーの体系、リスク管理体制などの見直しを検討することとしています。

また、当グループでは統合的リスク管理における管理対象リスクのうち、VaR※などの統一的尺度で計量可能なリスク値を合算して、経営体力(自己資本)と対比することにより管理しています(統合リスク管理)。※バリュー・アット・リスク(Value at Risk)

(2)資本配分運営

当グループでは、当社が外部環境、リスク・リターンの状況、シナリオ分析および自己資本充実度評価の結果を踏まえ、各リスクカテゴリー(信用リスク、市場リスク、オペレーショナル・リスク)を対象に、グループ各社を含めた各事業へ資本を配分する運営を行っています。資本配分の計画は、取締役会で決議しています。配分する資本の水準は、当グループのリスクアペタイトに基づいて決定されます。

各事業は、リスク量が配分された資本の範囲内、かつリスクアペタイトの範囲内となるように業務を運営します。また、リスク統括部は、月次でリスク量を計測し、配分された資本およびリスクアペタイトに対するリスクの状況を、定期的に取締役会などに報告しています。

(3)ストレステストと自己資本充実度評価

リスク統括部は、資本配分の計画の策定および見直しの都度、預金者保護の視点による自己資本充実度の確保のため、仮想シナリオ、ヒストリカルシナリオおよび発生確率検証の3種類のストレステストを実施し、その結果に基づき自己資本充実度を評価の上、取締役会などに報告しています。

6. サイバーセキュリティとシステム保全

当グループでは、サイバー攻撃をトップリスクに選定の上、「サイバーセキュリティ経営宣言」を策定し、経営主導によるサイバーセキュリティ対策の強化を推進しています。具体的には、社内にSuMi TRUST-CSIRT※1を設置し、グループ内外から脅威情報や脆弱性情報を収集・分析の上、必要なセキュリティ対策を立案し導入、定期的に経営層へ報告を行う管理体制を整備しています。CSIRTを軸に金融ISAC※2やFS-ISAC※3などの情報共有機関を活用し、最新のサイバー攻撃手口や脆弱性情報などを共有・活用するほか、サイバーセキュリティ演習を定期的に実施しサイバー攻撃への対応力強化に努めています。また、グループ共通のインターネット基盤を構築しSOC※4による監視を行うなど、グループ共通のセキュリティ対策を導入するほか、FFIEC-CAT※5など国際的なアセスメントツールを活用しセキュリティ評価のグループ標準化を推進するなど、グループ全体のセキュリティ対策の強化・標準化を図っています。システム保全の観点においては、大規模障害や災害による情報システムへの影響極小化、早期復旧ならびに業務継続へ備えるため、グループの連絡・対応体制を明確化し、代替措置・復旧手順などを整備するとともにオペレーションの教育・訓練などを行い、レジリエンス力強化に努めています。

※1 CSIRT(Computer Security Incident Response Team)
:攻撃予兆情報の収集・分析・対応策を進める社内組織
※2 金融ISAC(Information Sharing and Analysis Center):国内金融機関の情報共有組織
※3 FS-ISAC(Financial Services Information Sharing and Analysis Center)
:米国を中心とする金融機関の情報共有組織
※4 SOC(Security Operation Center)
:ネットワークを監視し、サイバー攻撃の検出や分析を行う組織
※5 CAT(Cybersecurity Assessment Tool):FFIEC(米連邦金融機関検査協議会)が金融機関向けに公表したサイバーセキュリティリスクアセスメントツール

7. 危機管理

当グループでは、金融機関としての公共的使命・社会的責任を踏まえ、自然災害やシステム障害、新種感染症の流行などが発生した場合、迅速かつ適切に緊急事態・危機に対応できる体制を整備し、組織内に周知することに努めています。具体的には、お客さま、役員・社員、その家族の安全を確保した上で、円滑に業務運営が継続できるよう、平時より業務継続プラン(BCP)を整備し、その実効性を確保するため、定期的な訓練と内容の見直しを実施しています。また、危機発生時においては、社長を本部長とする緊急対策本部を設置するなどの対応体制を整備しています。特に、地震のような大規模自然災害などに対しては、想定される影響の大きさを踏まえ、バックアップオフィスやバックアップシステム整備などの対応体制の強化を進めています。

なお、新型コロナウイルス感染症に係る業務継続に関するリスクに対しては、緊急対策本部を設置し、「社員および家族の健康と安全確保」「社会インフラとしての業務継続維持」「社会への感染拡大防止(感染拡大しにくい社会形成への活動を含む)」を基本スタンスと定め、国内外の感染状況、政府要請、お客さまの動向などを踏まえた機動的な対応を行ってきており、BCPに定める各種業務継続策の実施、テレワーク勤務の積極的活用などにより、サービス維持と安全面の両立を図っています。