SBIグループのリスクマネジメント

企業価値向上を支えるリスク管理

SBIグループでは、リスクアペタイト（戦略実現のためにどのようなリスクをどこまでとるか）に基づき、経営管理やリスク管理を行ってきました。当社グループにおけるリスク管理の役割は、グループの成長性を維持しながら、事業の阻害要素や社会に対する負の影響を回避するための施策を特定し、取締役会に経営判断の材料として提供することです。事業戦略推進への貢献度合いはリスクマネジメントの重要な役割と認識しており、リスクマネジメントのKPIにその貢献度を設定していることは特徴の一つです。

当社グループの事業展開は多岐にわたることから、事業分野・地域ごとにリスク要因を管理しており、事業の性質に応じた施策を講じています。また、地政学リスクの重要度が近年一層増しており、地政学リスクが具体的な財務・成長性・レピュテーションに繋がる各種リスクにどのように影響するかという観点も、リスク管理の重要なテーマです。

タイムリーな経営判断に資するリスク管理体制

リスク管理の核となるグループリスク管理統括部は、当社の従業員に加え、SBI新生銀行グループやSBI証券からの出向者等のグループ会社の従業員により構成されており、グループの戦略・風土および銀行業・証券業などの事業特性を踏まえた多様な視点を取り入れていることが特徴です。

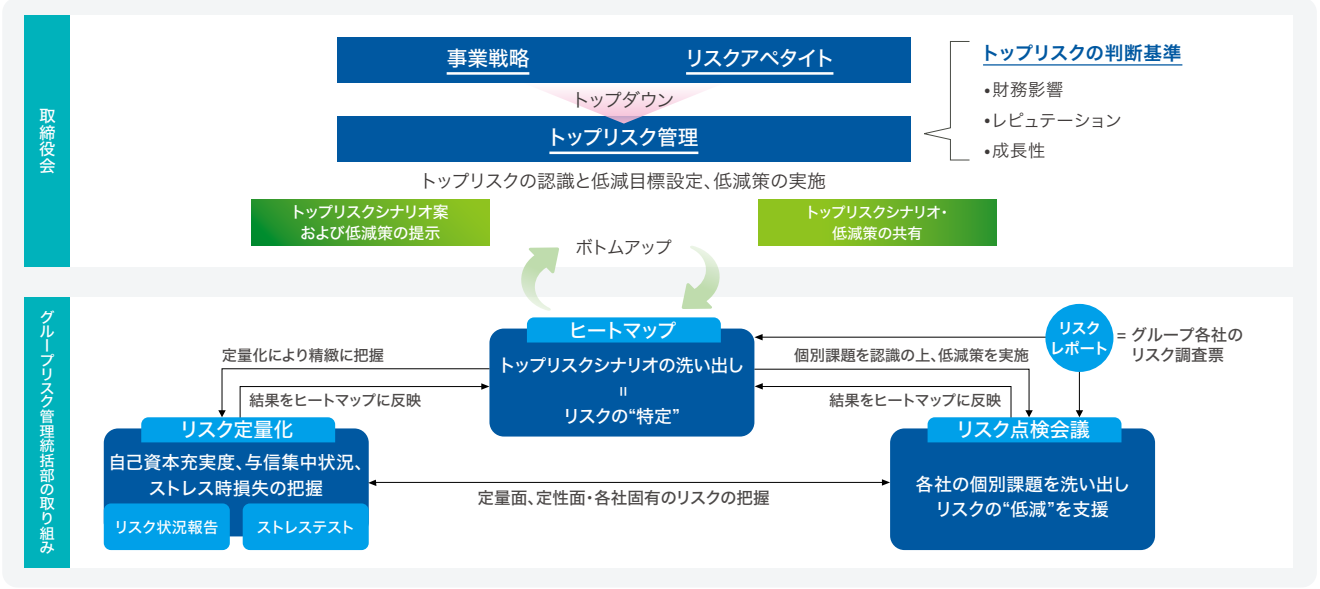
同部では他部門と連携を密にすることでリスク管理の実効性をより高めています。経理部、財務部、サステナビリティ推進室、法務部や、グループガバナンス・コンプライアンス部、また、情報セキュリティリスク・システムリスクに関してはIT統括部と連携を行っています。グループリスクに影響を与える変化を中心に、週次などのタイミングで詳細な情報を共有し、タイムリーに事業戦略に反映できる仕組みを構築しています。取締役会へは毎期、リスク管理計画を報告しており、進捗状況は年に2回報告、また定量的なリスク情報の報告は別途四半期ごとに行っています。

リスク特定プロセス

多様な事業を含む当社グループのリスク管理を行う上では、グループ横断的な「トップリスク」を常にアップデートしています。

トップリスク特定のため、トップダウンアプローチとして、各期の事業戦略から大局的なリスクシナリオを想定します。また、ボトムアップアプローチとして、各事業分野別に市場・信用・オペレーショナルリスクなどのカテゴリーごとの各種指標を集計し、リスクが高いと想定される事項を抽出します。これらによって、情報セキュリティ、不透明な市況による損失、資本管理やシステムキャパシティの逼迫による障害などをトップリスクとして特定し、それらの効果的な低減や、リスクアペタイトの範囲について経営意思決定に資するよう報告しています。

グループリスク管理統括部の活動の全体像



頻度 ［年次］リスクレポート　［四半期］リスク状況報告　［月次・臨時］リスク点検会議

リスク管理の三本柱

こうした大局観のある総合的なリスク管理のために、「ヒートマップ」「ストレステスト」「リスク点検会議」を管理手法の三本柱として活用しています。

ヒートマップは、グループ会社から各種定量的なリスク指標や定性的なリスク情報を吸い上げた結果を、グループの観点で俯瞰的に図示化したものです。リスク点検会議や、グループ会社からの各種リスク状況報告等に基づき、定期的に作成しています。

ストレステストは、主に定量的なリスク管理が可能な分野について、ストレスシナリオ下でどのような財務損失が生じ得るかを試算したものです。

リスク点検会議は、重点モニタリング対象のグループ会社を選定の上、各社と個別に対話し、リスクを具体的に把握するほか、その低減のため、内部管理態勢にかかるアドバイスやサポートを行うことで、グループ会社を支援しつつグループが抱えるリスクを低減させる取り組みです。前者2つが大局的・俯瞰的な管理目線の取り組みであることに対し、リスク点検会議は、個別的でミクロな観点の取り組みです。

これらを複合的に組み合わせることで、大局的でダイナミックでありながら、個別の課題も漏らすことないリスク管理が可能になると考えています。

SBIグループのサイバーセキュリティ

SBIグループのサイバーセキュリティ体制

当社グループでは、サイバーセキュリティを経営上の最重要課題の一つと捉え、「グループ情報セキュリティ規程」および「SBIグループセキュリティスタンダード」を定めています。更に2023年には、生成AIの利用に伴う機密情報等の保護およびセキュリティ確保を図るため、「SBIグループ 生成AI利用ガイドライン」を設け、定期的に見直しを行っています。

サイバーセキュリティ体制は、情報セキュリティ担当役員をグループ情報セキュリティ管理責任者とし、IT統括部が核となってグループ横断的な情報セキュリティ施策を実施しています。更に、IT統括部を事務局としてSBIグループCSIRT（Computer Security Incident Response Team）を設置しており、グループ内の情報セキュリティ管理責任者や有識者が参加する連絡会を毎月開催し、最新の脅威動向把握によるセキュリティインシデントの未然防止や、被害極小化等のレジリエンスの高度化に努めています。また、グループ全体でのサイバーセキュリティの底上げを図るべく、サイバーセキュリティ連絡会を年に4回開催し、グループ各社の情報セキュリティ責任者間で情報共有を図っています。

インシデントが発生した場合には、サイバー攻撃への対処などIT分野に特化して対応するIT統括部と、リスク全般を管理するグループリスク管理統括部が共同で対応を行い、多層的かつ総合的なセキュリティ管理の強化を図っています。両部門は隔週で情報を共有するなど、日常的に密接な連携を行っています。なお、取締役会への報告も定期的に行っています。

サイバーセキュリティ強化に向けた人材育成

当社グループでは役職員それぞれにセキュリティ対策の教育プログラムを実施しており、経営層に対しては外部有識者を招聘し研修を実施する他、取締役会においても定期的に議論を行っています。グループ子会社のシステム運用管理・担当者に対しては、外部講師によるセミナーを定期的に開催する他、サイバーセキュリティに関する専用の情報共有ポータルを通じて、会社の規模や分野によって偏りがちな知識の平準化を行っています。全従業員に対してはeラーニングを毎年必修とし、倫理観の醸成や知識の共有化を図っています。

サイバーセキュリティの整備

規模や成熟度が様々な会社が存在する当社グループでは、サイバーセキュリティに関する体制や人的リソース、知識の蓄積等の状況が不均衡である場合があり、その平準化を図ることを課題と捉えています。近年では、国家支援型の脅威アクターによるサイバー攻撃が国際的に顕在化しており、特に金融セクターが標的となるケースが増加しています。当社グループでは、こうした高度で巧妙な脅威に対しても迅速に対応できるよう、脅威インテリジェンスの導入やゼロトラストといわれる考え方を取り入れたグループ共通のセキュリティプラットフォームを構築し、各社のインシデントの予兆やそのリスクに対して機動的に対応できる環境を整備しています。こうした管理体制整備は、非連続の成長を続ける当社グループのサイバーセキュリティ体制構築に有効な方法であると認識しています。インシデントの予兆を察知するべく定常的なモニタリングを行いながら、DDoS攻撃やランサムウェア攻撃、情報漏洩およびマルウェア感染などに迅速に対応できるよう、検知および監視を強化するとともに、こうした当社の取り組みをグループ全体へ横展開することで対策の徹底を図っています。

このような取り組みが評価され、（一社）日本IT団体連盟が2025年1月9日に公表した「サイバーインデックス企業調査2024」において、「優れた取組姿勢および情報開示が確認できた企業」にも認定されています。