特集

経営戦略の遂行に向けた適切なリスク管理の実現

RISK MANAGEMENT

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

創業時から持続的な成長を実現してきたSBIグループにおいては、リスクアペタイト（Risk Appetite, 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う考えが根付いています。そのため、当社グループのリスク管理における役割は、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、経営判断の材料として提供することと捉えています。いかに事業戦略を推進することに貢献したか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についてもその貢献度を指標として置いていることが当社グループのリスクマネジメントの特徴と考えています。

当社グループの事業展開は多岐に渡ることから、事業分野・地域ごとにリスク要因を管理しています。現状の事業区分に再編したことで、リスク管理においても事業の性質に応じた施策を講じることが可能になりました。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となっています。

タイムリーな経営判断に資するリスク管理体制

当社グループにおける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新生銀行グループからの出向者、SBI証券の兼務者といった金融業を営むグループ会社の従業員等を含めて構成されており、当社グループの戦略・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。

同部では他部門との連携も推進しており、経理・財務面では同部を兼務する経理・財務担当役員と、サステナビリティリスクについてはサステナビリティ推進室、またコンプライアンスについては法務コンプライアンス部と連携しつつ取り組んでいます。加えて、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。

また、リスク管理担当役員と同部は随時、密な報告・情報共有体制を確保しています。グループリスクに影響を与える何らかの変化があった事項を中心に、週次などの機動的なタイミングで詳細な情報を共有しており、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。取締役会に対しては毎期、リスク管理計画を報告しており、進捗状況は年に2回報告しています。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。➡ P.45

リスク特定プロセス

当社では、多様な事業を含むグループのリスク管理の特性として、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認識できるよう工夫しています。

当社グループの成長性・レピュテーション・財務に重要な影響を与えるトップリスクの特定のため、トップダウンアプローチとボトムアップアプローチをとっています。トップダウンアプローチでは、各期の事業戦略から想定される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では、各事業種類別に市場・信用・オペレーショナルリスクなどのリスク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。例えば、金利上昇リスクや規制リスク、インターネット事業でのシステムリスク・サイバーセキュリティリスク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。

リスク管理の3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」といったリスク管理手法を三本柱として活用しています。

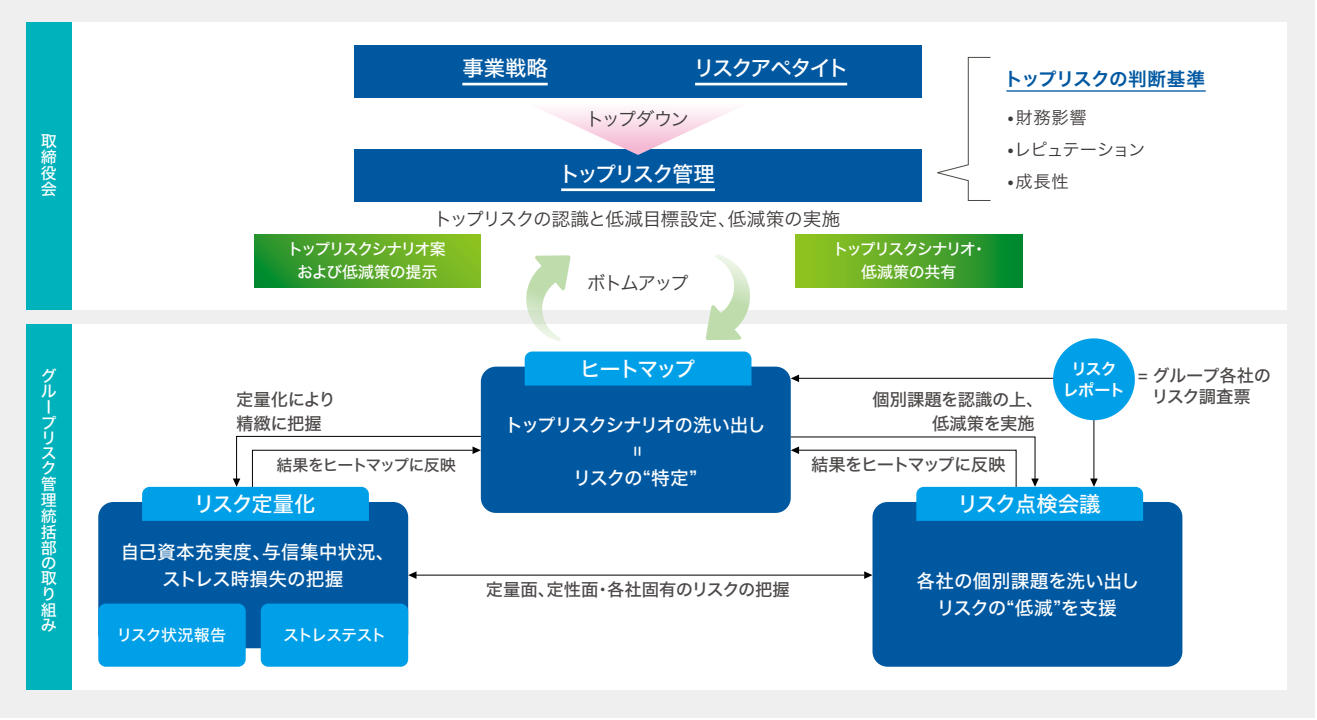
ヒートマップは、業態に合わせ、グループ会社から各種定量的なリスク指標や定性的なリスク情報を吸い上げた結果を、グループ観点で俯瞰的に図示化したものです。リスク点検会議や、子会社からの各種リスク状況報告に則って、定期的に作成しています。

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う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子会社を選定の上、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指導を行うことで、子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。

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

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

日本におけるインターネット金融サービスのパイオニアとして成長を遂げてきたSBIグループにおいて、サイバーセキュリティの強化は経営上の最重要課題の一つと捉えています。

証券・銀行・保険といった金融業を営む会社をグループ内に抱える当社では、グループ全体の規範となる「SBIグループセキュリティスタンダード」を定めています。本規範の制定に当たっては、金融機関がシステムを構築する際の安全対策基準（FISC安全対策基準）や、米国国立標準技術研究所（NIST）、国際的なサイバーセキュリティ規格であるCIS Controls等の各種フレームワークを参考としており、包括的なサイバーセキュリティ対策の強化を行っています。

当社グループのサイバーセキュリティ体制は、当社執行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業務を行っています。更に、IT統括部の事務局のもとにSBI

グループCSIRT(Computer Security Incident Response Team)を設置しています。SBIグループCSIRTは毎月連絡会を開催しており、サイバーセキュリティの知見を有する外部有識者との対話や社内関係部署・子会社との連携、金融業界のサイバーセキュリティに関する情報連携機関である金融ISACやサイバー犯罪に対する産学官の連携機関である日本サイバー犯罪対策センター(JC3)との情報連携を通じ、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、迅速なインシデント対応による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、グループ各社の情報セキュリティ責任者や情報セキュリティ管理担当者が出席するサイバーセキュリティ連絡会を年に4回開催し、グループ全体でのサイバーセキュリティに関する施策や動向等を共有しています。当社グループは会社毎に事業規模や事業分野が大きく異なることから、同連絡会を通しての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ことが重要と認識しています。

社内関連部署との連携については、IT統括部とグループリスク管理統括部とで、週次で情報共有を行っています。インシデントが発生した場合には共同で対策を行う体制としており、両部は日常的に密接な連携を行っています。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連携することで、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。

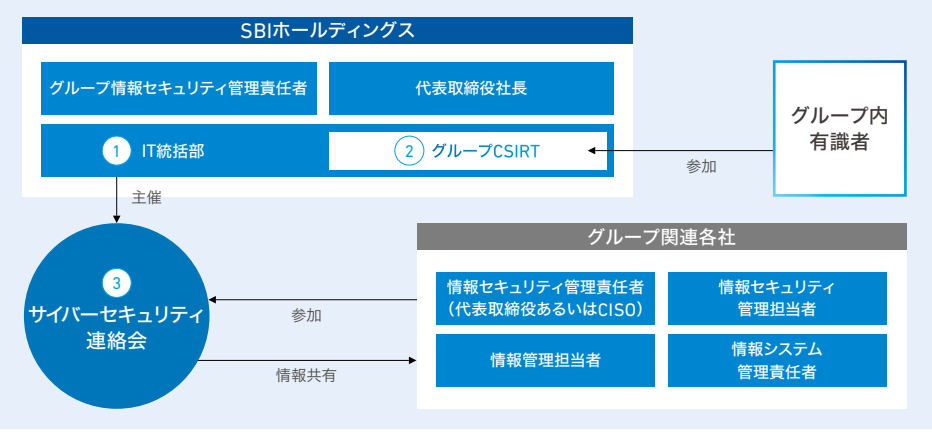
サイバーセキュリティ強化に向けた人材育成

セキュリティ対策としては、IT専門部署だけではなく従業員全員がサイバーセキュリティの重要性を理解し、日常的に対策していくことが不可欠と考えています。SBIグループでは、経営層や管理職、システムの開発や運用担当者、サービスの企画推進や事務、営業にかかわる従業員それぞれに、サイバーセキュリティにかかわる教育プログラムを実施しています。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題に挙げ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、脆弱性の注意喚起や対応策の周知を行い、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、フィッシングメール訓練やサイバー攻撃への注意喚起を周知する他、サイバーセキュリティに関するeラーニングを必修とし、倫理感の醸成や最新のサイバー犯罪およびその対策・対処法に関しての知識の共有化を図っています。

グループ全体を包括するサイバーセキュリティの整備

先進的かつ多様な事業を推進し、規模や成熟度も様々な会社が存在する当社グループにおいては、サイバーセキュリティに関しても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がグループの課題と捉えています。また、デジタル化の進展とともに、サイバー攻撃は巧妙化・高度化しており、従来の対策だけでは、インシデントを完全に防ぐことは難しくなっています。それら課題への解決に資する施策として、当社グループではゼロトラストといわれるセキュリティの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ています。このプラットフォームを利用することで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と認識しています。

サイバーセキュリティ体制図



主な組織の概要

1. SBIグループ全体のサイバーセキュリティを管理
2. 金融業のグループ各社からの参加者も含め、グループ全体でのCSIRTを形成
3. グループ全体でのサイバーセキュリティに関する情報共有を図る会