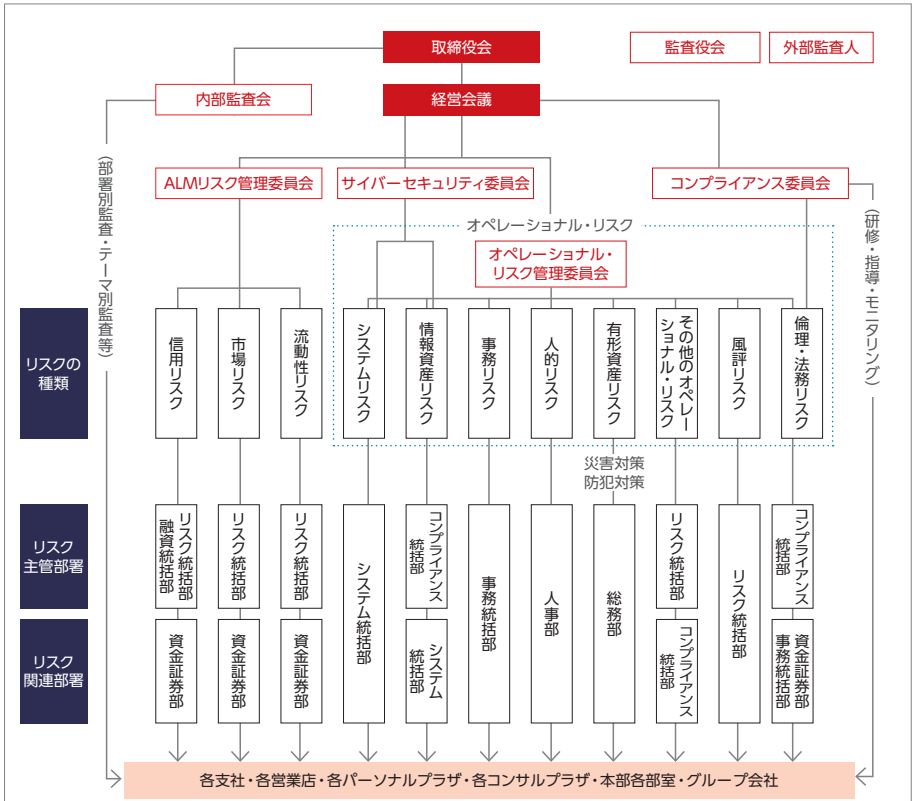
リスク管理

リスク管理の基本方針

金融サービスや業務が多様化するなか、リスク管理の重要性はますます高まっています。当行では、適正なリスク管理態勢を構築し、経営の健全性・適切性を堅持しつつ、安定的な収益を確保することをリスク管理の基本方針として、リスク管理の強化・充実に取り組んでいます。

リスク管理体制図

（2025年6月23日現在）



※ リスク統括部署はリスク統括部リスク統括課

統合的なリスク管理体制

当行では、百五銀行グループのさまざまなリスクを統合的に把握・管理する体制としています。リスクを「信用リスク」「市場リスク」「オペレーショナル・リスク」等に区分し、各リスクに主管部署を定めるとともに、リスク統括部署を設置してリスクを統合的に管理しています。また、「ALMリスク管理委員会」および「オペレーショナル・リスク管理委員会」において、リスクを総合的に把握・評価・監視し、リスク管理の方針や対応策を審議しています。

また、「統合リスク管理」の考え方のもとリスクを定量化し、リスクテイクには限度枠を設定することにより、経営の健全性・適切性確保と安定的な収益確保の両立を図っています。

さらに、業務部門から独立した監査部門による内部監査を実施し、各部門の内部管理の適切性・有効性を検証し、改善を促す仕組みとしています。

信用リスク管理

当行では、信用リスク管理を適切に行うことにより、貸出等の資産の健全性の維持と、資本効率・資産効率の高いポートフォリオの構築をめざしています。

リスクに見合う適正な収益を確保するため、信用格付制度を導入し、信用リスクを統一的な尺度により評価しています。また、融資の基本方針として「百五銀行クレジットポリシー」に特定の企業や業種に貸出が集中しないよう定めるとともに、与信ポートフォリオ全体をモニタリングし、リスクを分散するよう管理しています。

自己資本比率の算定にあたっては、基礎的内部格付手法を採用し、リスク管理の高度化に取り組んでいます。内部管理においては、与信集中リスクを含めた形で信用リスクを計測・管理しています。なお、業況悪化先等に対しては、経営状況等を適切に把握・管理し、必要に応じて再建計画の策定の指導や整理・回収を行っています。

市場リスク・流動性リスク管理

市場リスク管理においては、ポートフォリオの市場変動によるリスクを適正な水準に制御しつつ、収益を安定的に確保することをめざしています。なお、金利、為替、株価等の各種リスクは、主にVaRで計測・管理しています。

流動性リスク管理においては、円貨・外貨の資金繰りの状況や見通しを把握し、資金不足に陥らないよう適切に管理しています。また、不測の事態に備え、流動性の高い資産の確保、市場からの調達可能額の把握、資金繰り逼迫度に応じた対応策の策定・実施等を行っています。

オペレーショナル・リスク管理

オペレーショナル・リスクについては、「事務リスク」「システムリスク」「情報資産リスク」「倫理・法務リスク」「人的リスク」「有形資産リスク」「風評リスク」「その他のオペレーショナル・リスク」からなる幅広いリスクとしてとらえ、影響や改善策の必要性を適切に評価したうえで、リスク削減に取り組んでいます。また、外部委託に関するリスク管理の強化等にも継続的に取り組んでいます。

危機管理

これらのリスク管理体制に加え、銀行業務の公共性に鑑み、地震等大規模災害の発生時や新興感染症の流行時にも、地域の社会・経済活動維持に必要な金融サービスを継続して提供し、あるいは早期に復旧できるよう、「業務継続計画書」を定めています。また、各種コンティンジェンシー・プランを整備し、定期的に訓練を実施する等、危機への対応力の強化に取り組んでいます。

サイバーセキュリティ対策への取組み

当行では、高度化・巧妙化しているサイバー攻撃に対応するため、経営者自らが最新情勢への理解を深めることを怠らず、サイバーセキュリティを投資と位置づけて積極的な経営に取り組みます。

サイバーセキュリティ管理の基本方針

経営陣は、サイバーセキュリティリスクを組織全体のリスク管理の一部としてとらえ、経営陣の主体的な関与のもと、リソースの適切な配賦および平時からの能動的なインシデント対応体制を構築していくとともに有事における対応力を強化し、変化し続けるサイバー攻撃の脅威に組織的・技術的に対応します。

維持するサービス範囲・水準

地域の社会・経済活動維持に必要となる金融サービスを提供しつづけることは当行の社会的使命であり、また、それを果たし得る体制を整備します。

リスク管理体制

サイバーセキュリティ委員会の設置を通じ、取締役会との情報連携を密にし、経営陣を加えたガバナンス体制を確立します。サイバーセキュリティ対策に専門的・集中的に取り組む専担部署として、サイバーセキュリティ統括室を設置し、サイバーセキュリティ管理態勢の高度化に取り組んでいます。

当行では、グループ各社を含めた組織横断的な平時・有事のサイバーセキュリティ対応組織として百五銀行グループCSIRT※1を設置し、サイバーセキュリティにかかる基本方針や管理規則等を制定のうえ、サイバーセキュリティ管理態勢の強化を図っています。また、三重県警察との共同対処協定の締結や外部団体である金融ISAC※2への加盟等、サイバーセキュリティに関する関係機関との連携強化を図り、幅広く情報収集することで、早期の警戒態勢や防止措置につなげています。

※1 CSIRT：Computer Security Incident Response Teamの略で、システムなどセキュリティ上の問題につながる事象の発生時に備えて、平時から活動する組織
※2 ISAC：Information Sharing and Analysis Centerの略で、各業態共同でサイバーセキュリティ対策情報等を共有化する組織

サイバーセキュリティに関する責任者の知見

当行では、サイバーセキュリティ全般の責任者としてサイバーセキュリティ統括責任者を任命し、サイバーセキュリティリスクを統括する体制としています。サイバーセキュリティ統括責任者は、外部の知見を取り入れる研修や訓練等に積極的に参加し、最新の情報を持ってセキュリティ体制を整備することを心がけています。また、経営陣全体の知見向上を目的に、経営陣のみを対象とした勉強会を定期的に開催しています。

資源の確保

サイバーセキュリティは成長投資と並ぶ重要な社内インフラの整備ととらえ、「人材」と「強固なシステム構築」へ積極的な投資を行います。人材については、外部専門組織に行員を派遣し長期トレーニーで育てるとともに、精通する外部人材を中途採用するなど、育成・確保に注力しています。また、全役職員を対象とした標的型攻撃メール訓練やセキュリティ勉強会を定期的に実施し、当行全体のサイバーセキュリティの意識向上に努めています。

リスクの把握と対応計画策定

国家サイバー統括室（NCO※3）、警察庁や金融ISAC等の外部団体から共有される脅威情報・脆弱性情報の収集や自組織の情報資産に対する定期的な脆弱性診断の実施等により、サイバーセキュリティリスクを特定、評価し、自らを取り巻く事業環境、経営戦略およびリスクの許容度を踏まえたうえで、サイバーセキュリティリスクの低減措置を計画的に講じます。

※3 NCO：National Cybersecurity Officeの略で、サイバーセキュリティの確保に関する必要な助言や情報提供等を行うことを目的に内閣官房に設置された組織。

緊急対応体制・復旧体制

有事に備え、サイバーセキュリティ確保のための体制を整備するとともに、金融庁等が主催する訓練への定期的な参加等により、迅速な対応がとれるよう対応力の向上に取り組んでいます。インシデント発生時には、経営陣の関与のもと、業務継続および情報資産保護のために関連部署を招集し、原因調査、被害拡大防止、復旧対応等を行います。

インシデントの発生状況

当行機器に対する不正な通信を遮断するなどの対応により、サイバーインシデントはこれまで発生していません。

TOPICS

サイバーセキュリティ対策セミナーの開催

百五銀行グループは、高度化・巧妙化しているサイバー攻撃に対応するため、サイバーセキュリティ対策の強化に取り組んでいますが、自行グループのみならず、近年多発するサイバー犯罪の危険にさらされている地域企業の皆さまにも情報提供を行っています。

2025年2月、三重県警察本部の協力を得て、百五総合研究所主催、当行および三重県商工会議所連合会共催の「サイバーセキュリティ対策セミナー」を開催しました。

地域の中堅・中小企業の経営者、情報セキュリティ担当者など122社151名の方々を対象にサイバー犯罪に関する最新動向をはじめ、攻撃を防ぐための対策、被害に遭遇した場合の復旧手順や原因の究明方法など、実演を交え企業の大切な情報資産を守るために必要な対策について、事業者の皆さまに有益な情報を提供する機会となりました。

当行は今後も、サイバーセキュリティ対策について地域企業の意識醸成を図るとともに地域におけるさまざまな課題解決に貢献していきます。