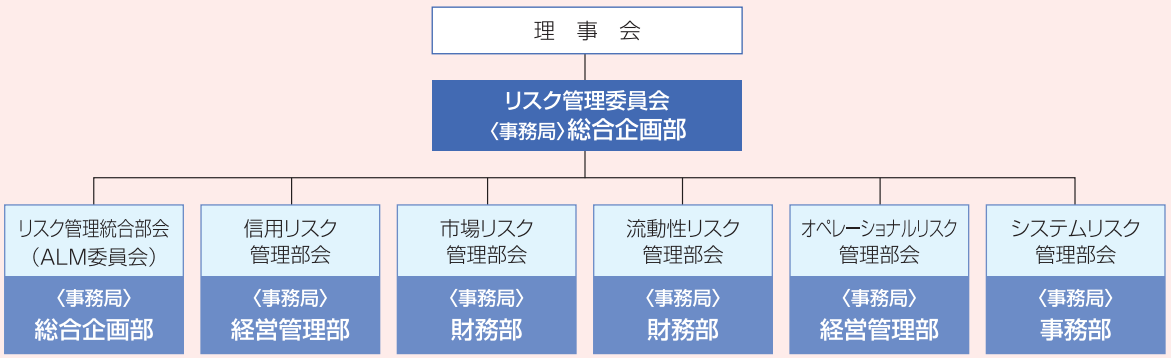
リスク管理

事業活動はさまざまなリスクにさらされています。とくに金融機関はそうであります。
〈にっしん〉は、「事業運営のすべてをリスク管理の観点から見る」という態勢を確立していかねばならないと考えています。リスク管理の手法は急速に発展し高度化しつつありますので、リスク管理態勢を絶えず見直し、積極的に新しい手法の導入に努めています。

理事会の下にリスク管理委員会を設置し、その下にリスク管理統合部会と5つのリスク管理部会を設置しています。



●リスク管理の統合

信用リスク、市場リスク、流動性リスク及びオペレーショナルリスクの全てを数値化し、リスクの総量を明らかにするとともに、リスクごとに自己資本を配賦し、取り得るリスク量の許容範囲を明確にしています。また、営業の各部門の潜在的リスク量がバランスのとれたものになっているかを検証し、金融情勢に変化等があった場合でも健全性が確保できるよう努めています。

●信用リスク

信用リスクは信用供与先の経営内容の悪化等により金庫資産の価値が減少ないし消失するリスクで、貸出金と有価証券が主な対象です。

貸出金のうち、特に重要な案件の審査や大口与信先に対する与信の基本方針等については、常務理事以上、審査部長等で構成する融資審査会で検討、決議するなど、融資審査の独立性、公平性、透明性を確保するようにしています。加えて「融資先特別管理規程」を制定し常時モニタリング先や経営支援先等を定めて融資先の管理の強化を図っています。

また、貸出資産の自己査定を毎月実施することにより、貸出先の業況を早期に把握し貸出資産を的確に管理するよう努めています。

有価証券については、「資金運用規程」及び毎年度定める「余資運用の基本方針」に基づいて投資額を決定しています。投資先の信用状況については、R&I、JCR、Moody's、S&Pの適格格付機関の資料を用いて、毎月モニタリングを行い、その結果を会長、理事長、専務理事、常務理事、監事及び経営管理部長に報告しています。運用資産が投資不適格となった場合は銘柄毎に運用継続又は売却等の対策を講じています。

●市場リスク

市場リスクとは、金利、有価証券の価格、為替等の様々な市場の変動により損失を被るリスクをいいます。有価証券については保有限度枠を定め、リスクを100BPV法、VaR法等を用いて計量することで過度なリスクを取らないようにコントロールしています。また、有価証券運用で発生した損失が金庫経営の持続可能性に直接的かつ多大な影響を与えることを防止するために「損失限度及び金利リスク枠」を定めて日々計測しています。

急激な環境変化を想定したストレステストを毎月実施し、その結果を市場リスク管理部会、ALM委員会に報告しています。これら「有価証券にかかるリスク等の検証結果」を経営管理部が確認することで、リスク管理態勢の強化と相互牽制を図っています。さらに、金庫経営に大きなインパクトがある将来の金利上昇局面等に備えて、「予兆管理及びアクションプランの手引き」を制定し、予兆管理の手法とストレスシナリオ顕在時の対応を定めています。

●流動性リスク

流動性リスクには、風評等により資金繰りがつかなくなる「資金繰りリスク」と、市場の混乱等により取引が不能となる「市場流動性リスク」があります。「流動性リスク管理規程」に基づき、常に資金繰りを管理するとともに情報の収集・分析を行っています。

平成30年度においては流動性危機発生時の訓練を平成31年2月に実施しました。

●オペレーショナルリスク

オペレーショナルリスクには、事務処理が正しく行われないことなどに伴い発生する事務リスク及び金庫業務を遂行するなかで発生する恐れのある種々のリスクをいいます。

事務リスクに対しては、規程類の整備、見直しを絶えず行い、研修指導、内部監査などあらゆる機会を通じて、正しい事務処理を行うように努めています。また、事務部の営業店実地指導により、事務ミスの防止を図っています。本部各部は3ヶ月毎に各部所管の業務のリスクを洗い出し、そのリスクの具体的な処理方法を策定、実施することによりリスクの軽減を図っています。

地震に代表される自然災害、新型インフルエンザ、テロ等の事業継続に多大な影響を与える事態が発生した場合に備え、各カテゴリー別に行動計画を策定し必要な見直しと実効性の強化に努めています。

●システムリスク

システムリスクとは、コンピュータシステムの障害または誤作動、システムの不備、さらにはコンピュータの不正使用などにより損失を被るリスクのことをいいます。〈にっしん〉では、システム障害や災害等の緊急事態に備えた「危機管理・業務継続計画（BCP）」の策定及びシステム障害発生要因の影響度などを把握することにより、緊急時の対応に万全を期しています。また、保有する情報資産を、障害（サイバー攻撃を含む）・紛失・漏えい・不正利用などの脅威から守るため、「セキュリティポリシー（情報及び情報システムを適切に保護するための安全対策に関する統一指針）」に則り、適切な保護対策を講じています。