リスク管理
業務継続体制・サイバーセキュリティ

リスク管理

基本的な考え方

金融・経済のグローバル化の進展、金融技術やITの向上等を背景にビジネスチャンスが拡大する一方で、それらに伴うリスクはますます多様化・複雑化しております。

このような環境の中、当行ではリスク管理を経営上の最重要課題と位置付け、これに万全の体制で臨むことで、経営の安全性・健全性を維持するとともに安定的な収益確保をはかってまいります。

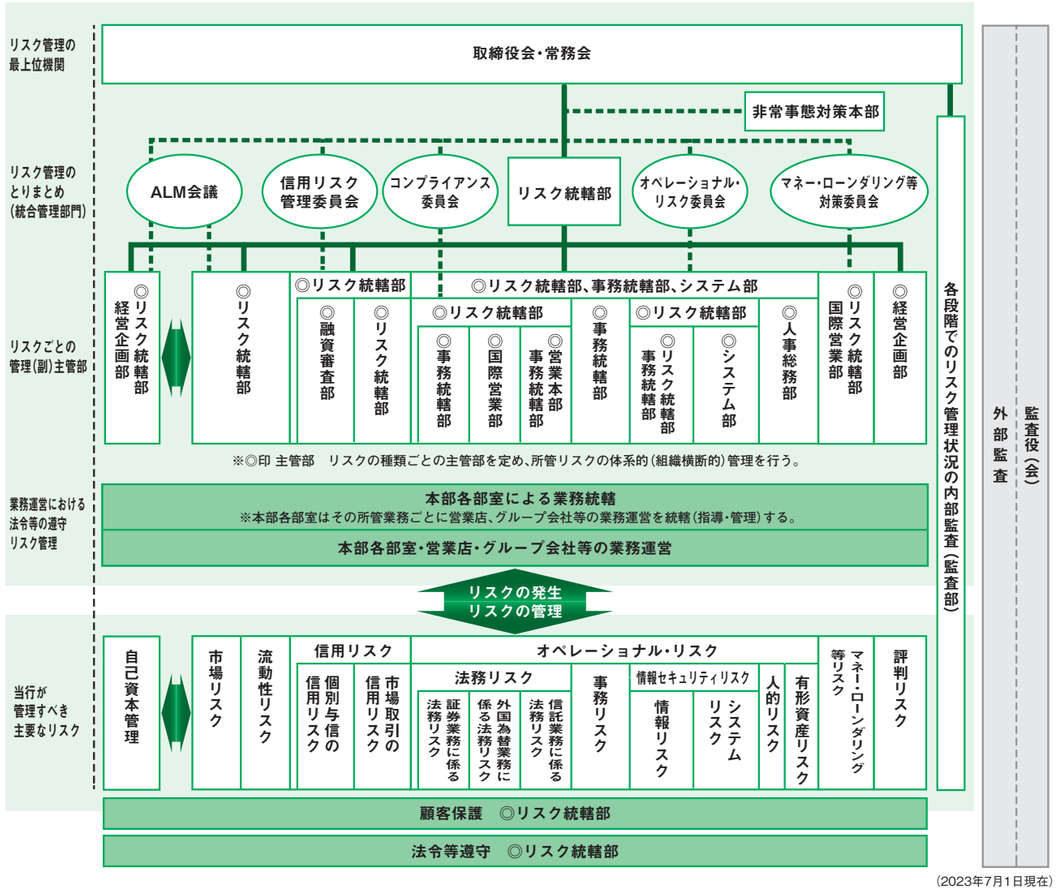
統合的リスク管理

業務において保有するすべてのリスクを的確に把握し、当行の安全かつ健全な経営基盤を確立するため、「統合的リスク管理規程」を定め、総体的に捉えたリスクを当行の経営体力（自己資本）と比較・対照する、自己管理型のリスク管理体制を整備しております。

リスクの種類ごとに本部の主管部を定め、これらが組織横断的に所管するリスクの管理を行うとともに、これらのリスクをリスク統轄部が統合的に管理することにより、リスク管理の一層の強化、充実をはかっております。

同時に当行では、主要なリスク（信用リスク、市場リスク、オペレーショナル・リスク）の計量化を進め、これらに対する資本配賦を行っております。リスク量については、半期ごとに見直しを行うリスク管理方針に基づき、配賦資本額をその限度額として管理しており、算出したリスク量を毎月のALM会議において経営へ報告する体制としております。加えて、リスク包括的なシナリオに基づき、各種リスクが同時に顕在化した場合を想定した統合ストレステストを実施しております。

■当行のリスク管理体制



（2023年7月1日現在）

（※）主要なリスクの詳細については当行ＨＰに掲載の資料編 P.12以降に掲載しております。

業務継続体制・サイバーセキュリティ

業務継続の基本方針

自然災害・感染症の蔓延・事故災害・人為的災害等による大規模な被害発生により、当行の業務継続が脅かされる危機発生時において、速やかに業務の復旧をはかるため、次の方針を定めております。

○被災地等の地域住民のみなさまの生活や経済活動の維持のため、金融サービスの継続に努めます。
○金融決済機能を維持し、経済活動の混乱を抑制することに努めます。
○役職員の安全を確保するとともに、業務の停止に伴うお客さまからの信認低下など、当行の経営面の影響を軽減します。

災害発生時の危機管理態勢

平常時には、BCPに基づく危機管理体制を見直し、改善するための年間計画として業務継続プログラムを策定し、体制整備をはかっております。

また、自然災害・感染症の蔓延等の危機発生時には、「非常事態対策本部」により一元的に指揮・命令を行う体制としており、被災シナリオごとに作成した業務継続マニュアル、業務継続手順書およびコンティンジェンシープランに基づき、早期の業務復旧を目指します。

サイバーセキュリティ

当行は内外の組織や専門家と協力し、コンピュータ・セキュリティ事案の検知、解決、被害局限化および発生の防止をはかることにより、サイバーセキュリティ向上に取り組んでおります。

具体的には、「情報セキュリティポリシー」に基づき、「システムリスク管理規程」ならびに「サイバーセキュリティ対応規程」を定め、サイバー攻撃に関するリスクを適切に管理し、サイバーセキュリティ対応を行うための態勢を整備しております。

当行では、日々高度化・巧妙化していくサイバー攻撃による脅威に対応するため、システム部内にサイバーセキュリティ対策室を設置し、サイバー攻撃の動向や脆弱性等の情報収集・把握、サイバー攻撃事案への対応（検知、解決、被害局限化、対策等）を一元的に実行できるようにしております。

また、定期的にサイバー攻撃事案を想定した訓練を実施し、実効性の向上に努めております。

お客さまに提供するインターネット上のサービスについては、不正アクセスやサービス停止攻撃等への対策を講じるほか、インターネットバンキングの不正利用防止をはかるための対策を実施しております。

事　例

外部評価を活用した取り組み

最大限に発揮できる働きやすい職場環境サイバーセキュリティへの取り組みにおいて、これまでの金融庁から還元される資料を基にした自己評価に加え、NRIセキュアテクノロジーズ株式会社が提供するSecure SketCH の自動診断機能（SecurityScorecard社のリスクレーティング連携）を採用し、客観的かつ俯瞰的な評価を活用した取り組みを行っております。

現時点では5段階評価の最上位評価かつ同業種平均を上回る評価を得ておりますが、発見された課題解決に取り組むとともに、リスク状況の変化に応じた将来的な情報セキュリティの高度化をはかってまいります。

■Secure SketCHによる評価結果（一部抜粋）