コンプライアンスへの取組み

コンプライアンスの基本方針

当金庫は、基本的使命と社会的責任を果たし、お客さまや会員からの信頼・期待に応えるために、徹底した自己責任原則のもとで法令遵守等社会的規範に則った業務運営を行っています。また、ディスクロージャー（情報公開）とアカウンタビリティー（説明責任）を重視し透明性を確保するよう努めることにより、コンプライアンスへの不断の取組みを積み重ねています。

その一環として当金庫では、「倫理憲章」「環境方針」「人権方針」にコンプライアンスの基本方針を定めています。加えて、全役職員に「行動規範」を周知し、事業活動の前提である誠実・公正な業務遂行に向けた判断・行動の基準を示すとともに、「共有価値観」を具体的に実践するための考え方を示し、コンプライアンス・マインドの浸透と業務への反映・実践に取り組んでいます。

また、コンプライアンス・健全なリスクカルチャー浸透にかかる取組み等の適切性に関連する内部監査を定期的に実施しています。さらに、昨今の顧客保護に向けた社会的な要請の高まりを踏まえ、「顧客保護等管理方針」に基づき、お客さまに対する説明、お客さまからの苦情・相談等への対応、顧客情報の管理、お客さまにかかわる外部への業務委託を行っている場合の委託先管理、お客さまとの間で利益相反のおそれのある取引の管理についても、十分な信頼が得られるようコンプライアンスへの取組みの一環として態勢強化に取り組んでいます。

倫理憲章・環境方針・人権方針については以下をご覧ください。
【倫理憲章】https://www.nochubank.or.jp/about/charter.html
【環境方針】https://www.nochubank.or.jp/sustainability/management/policy/pdf/environmental_policy.pdf
【人権方針】https://www.nochubank.or.jp/sustainability/management/policy/pdf/humanrights_policy.pdf

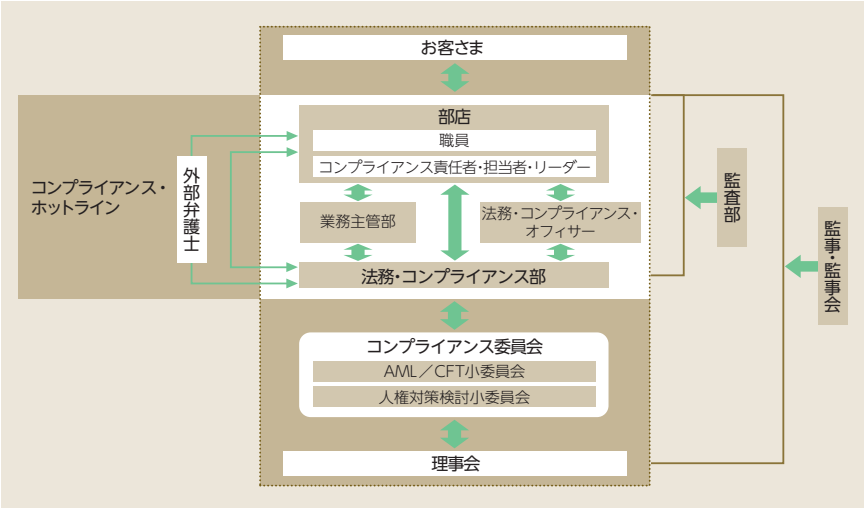
経営に直結したコンプライアンス運営態勢

当金庫のコンプライアンス態勢は、コンプライアンス委員会、コンプライアンス統括部署（法務・コンプライアンス部）、法務・コンプライアンス・オフィサー、部店に配置されたコンプライアンス責任者、コンプライアンス担当者、コンプライアンス・リーダーを中心に運営しています。コンプライアンス委員会は、当金庫のコンプライアンス態勢整備に関する重要な事項等を審議し決定するため、理事会のもとに設置された委員会です。同委員会で協議した重要事項や同委員会の議案については、理事会にも付議・報告しています。同委員会では、オペレーショナル・リスク、アンチ・マネー・ローンダリングやテロ資金供与対策、情報セキュリティに関しても議題として取扱い、これらについての重要な業務執行に関する方針を協議することとしています。

さらに、コンプライアンス委員会の下部委員会であるAML／CFT小委員会および人権対策検討小委員会により、コンプライアンス態勢にかかる協議を充実させるとともに、態勢運営にかかるPDCAサイクルの強化を図っています。

また、RAFにおいても健全なリスクカルチャーの浸透を図り、不適切な行為を組織的に抑止することをリスクの取扱方針として明確にしています。

コンプライアンス運営態勢図



具体的なコンプライアンス等の実践方法

当金庫では、部店におけるコンプライアンス態勢として、コンプライアンス責任者である部店長等とコンプライアンス担当者・コンプライアンス・リーダーを中心に、全職員が取り組むことで運営しています。特にコンプライアンス担当者は、法務・コンプライアンス部長が直接任命しており、部店のコンプライアンス関連事項を総括し、職員からのコンプライアンス相談・質問対応、部店内での教育・指導、法務・コンプライアンス部等への連絡・報告・相談対応などを行う役割を担っています。

食農法人営業本部、リテール事業本部、グローバルインベストメント&バンキング本部およびコーポレート本部のすべての本部に法務・コンプライアンス・オフィサーを設置し、各本部業務をコンプライアンス面からサポートしています。

法務・コンプライアンス部は、コンプライアンス統括部署としてコンプライアンス委員会の事務局になるとともに、コンプライアンス審査、各部店からのコンプライアンスにかかる相談対応や、部店を訪問してコンプライアンスの実践状況を直接確認しながら指導を行うコンプライアンス・モニタリングなどを通じて、当金庫のコンプライアンス態勢の強化に取り組んでいます。

「コンプライアンス・プログラム」について

コンプライアンス態勢および顧客保護等管理態勢の整備をはじめ、取組みの推進や教育研修などの実施計画を「コンプライアンス・プログラム」として年度ごとに策定のうえ、その進捗を管理しながら実行することにより、コンプライアンス態勢などの一層の充実を図っています。

グループ会社との連携

グループ全体としての「健全なリスクカルチャーの醸成・定着」の実現を目指し、主要なグループ会社と行動規範を共通化し、各社における行動規範の浸透、実践活動をサポートしています。グループ会社のコンプライアンス部門との定期会議におけるコンプライアンスの取組みにかかる課題の認識・共有化、各社コンプライアンス・プログラムの策定・実践や研修活動の支援などを通じて、農林中金グループ全体のコンプライアンス態勢強化に取り組んでいます。また、グループでのコンプライアンス・リスク低減のため、グループ共通のハラスメント外部相談窓口の設置や、各社へのオフサイト・モニタリング（一部はオンサイト）などを実施し、課題の早期発見に努めています。

内部通報制度について

当金庫では、コンプライアンス上の問題がある場合に、役職員などが電話や電子メールなどを通じて通報できるよう内部通報制度を整備し、「コンプライアンス・ホットライン」を設置しています。

「コンプライアンス・ホットライン」は、法務・コンプライアンス部および外部弁護士に通報ができる複数の窓口を整備しており、役職員が実名あるいは匿名での通報を選択できる仕組みとしています。また、通報を受け付けた際には、調査を実施して必要な改善・是正対応を行うほか、通報した役職員などに対する不利益な取扱いの禁止、通報に関する秘密保持など、通報者保護を最優先とした運営を行い、制度の信頼性向上にも努めながら取り組んでいます。

2024年度は、当金庫内外の通報窓口で計10件の通報を受け付けていますが、当金庫の経営に重大な影響を及ぼすものはありませんでした。

なお、海外支店については、上記窓口とは別に職員が通報できる窓口を各支店に設置しています。

情報セキュリティの取組み

当金庫は、お客さまとのお取引などにおいて入手した様々な情報を各種業務に活用しています。情報技術（IT）の進展により、情報を取り扱う環境や目的が多様化していくなか、適切にお客さまの情報を保護・管理するため、情報セキュリティの取組みを重視しています。

当金庫では、理事会が情報セキュリティ管理態勢を整備・確立する最終責任を有しています。情報セキュリティの企画・推進・進捗管理を行う統括部署（法務・コンプライアンス部）を中心に、各部店に情報セキュリティ責任者（部店長）・情報セキュリティ担当者を配置し、組織的に情報セキュリティの強化を図っています。また、情報セキュリティ管理態勢の整備にかかる重要な事項はコンプライアンス委員会等で協議しています。

個人情報の取扱いに関しては「個人情報保護宣言」を定めるとともに、個人情報取扱事業者および個人番号関係事務実施者として求められる態勢を構築しています。また、当金庫のみならず、サプライヤー（外部委託先）に対しても、個人情報の取扱いを含む委託を行う場合には、当金庫自身が行う場合と同等のリスク管理の水準を確保しうるプロセス・契約関係を整備する旨を「リスクマネジメント基本方針」で定め、適切な個人情報の取扱いが行われるよう取り組んでいます。

個人情報の適切な取扱いを含めた情報セキュリティに関しては、すべての職員に対して毎年eラーニングを実施するとともに、各階層における研修を行うことにより、情報セキュリティに関する意識向上を図っています。

海外については、当金庫ロンドン支店およびNorinchukin Bank Europe N.V.で適用されるプライバシーポリシー、および米国居住者向けのプライバシーポリシーをそれぞれ策定しています。

サイバーセキュリティ

サイバーセキュリティの取組み

当金庫では、高度化・巧妙化しているサイバー攻撃の脅威について、経営上の重要なリスクのひとつと認識し、サイバーセキュリティ対策の強化に努めています。

サイバーセキュリティの基本方針

当金庫は、サイバーインシデントにより当金庫のお客さまに被害が及ぶリスクや、当金庫の業務ひいては金融システム全体の任務遂行に支障を及ぼすリスク等を最小化することを目的として、「サイバーセキュリティ基本規程」においてサイバーセキュリティ管理の基本的な方針を定めています。

サイバーセキュリティ体制

組織体制においては、IT統括部担当理事を「サイバーセキュリティ統括責任者」とし、サイバーリスクに対する役割や責任を明確化しています。サイバーセキュリティ統括責任者のもと、サイバーセキュリティ担当部署（IT統括部）を中心として、様々な施策を推進しています。

サイバーインシデントの発生状況や脅威動向、ならびにサイバーセキュリティ対策の整備状況等については、理事会や業務インフラ協議会、コンプライアンス委員会などの経営レベルの会議において定期的に報告され、サイバーセキュリティ対策の方針について議論しています。

IT統括部にはサイバーセキュリティの専門部署として「CSIRT: Computer Security Incident Response Team」を設置しています。当金庫のCSIRTは、外部のセキュリティベンダーが担う「SOC: Security Operation Center」と緊密に連携しており、サイバーインシデントの兆候となるイベントを24時間365日体制で監視し、サイバーインシデント発生時の初動対応を担っています。また、CSIRTは国や法執行機関、ISAC等各種団体とも連携し、サイバー攻撃の手口や新たな脆弱性に関する情報を収集のうえ、対策の強化に取り組んでいます。

さらに、サイバーレジリエンスの確保のため、サイバーインシデント発生時の対応手順やコンティンジェンシープランを整備し、定期的なインシデント対応演習を通じて各部門の役割や手順の確認を行っています。

サイバーセキュリティの管理プロセス

当金庫では、公益財団法人金融情報システムセンター(FISC)の「安全対策基準」等を用いて、情報システムの「機密性」・「完全性」・「可用性」についてシステムリスクの評価を行い、必要な管理策を実施しています。

組織横断的なサイバーセキュリティの管理プロセスとしては、NISTの「サイバーセキュリティフレームワーク」を踏まえ、「特定」・「防御」・「検知」・「対応」・「復旧」の切り口で「サイバーセキュリティプログラム」を整理し、攻撃者の手口の変化等の外部脅威や内部の脆弱性を踏まえて必要な施策を見直しています。

こうしたサイバーセキュリティ管理の取組みについては、脆弱性診断やペネトレーションテストのほか、年1回の内部監査、外部監査を通じて有効性を確認しています。

サイバーセキュリティに関する教育

当金庫では、役職員それぞれに求められる知識や意識の向上のため、目的別に教育を行っています。

- 全役職員のセキュリティに関する基礎知識の習得を目的としたeラーニング
- 全役職員のサイバーセキュリティについての意識向上を目的とした、サイバーセキュリティ関連の記事を紹介するニュースレター
- 全役職員を対象とした、標的型攻撃メールへの耐性や意識の向上を目的とした不審メール訓練
- 役員のサイバーセキュリティに関する知見の向上を目的とした有識者講演会
- サイバーインシデント発生時の対応手順確認を目的とした、役員と関係部署の職員参加によるインシデント対応訓練
- CSIRTのフォレンジック技能向上を目的とした、外部有識者による技能トレーニング

また、サイバーセキュリティ専門人材育成のため、外部資格奨励制度等も設け、専門スキルの向上に努めています。

サイバーセキュリティ体制図