リスクマネジメント

リスクマネジメントの考え方

企業の安定的・持続的な発展と企業価値の増大、そして会社としての社会的責任を果たすためには、企業活動に重大な悪影響を及ぼすリスクへの的確な対処が必要不可欠です。リコーリースグループでは当社グループを取り巻くリスクを網羅的・統括的にとらえて整理・対処することにより、実効性・効率性のあるリスクマネジメントを実現しています。

リスクマネジメント体制の見直し・構築

リスクマネジメントに取り組む体制は、刻一刻と変化する環境に適応するよう継続的な見直しと改善が求められます。これまで、当社グループのリスクマネジメントは、グループ各社がそれぞれ自律的に推進してきました。今後、グループ経営を強化していくにあたっては、グループ全体の利益最大化を目指すべく、最適な判断が求められます。その実現を阻害する要因をリスクとして識別、分析および評価する必要があり、リスクマネジメント体制の見直しを実施しています。

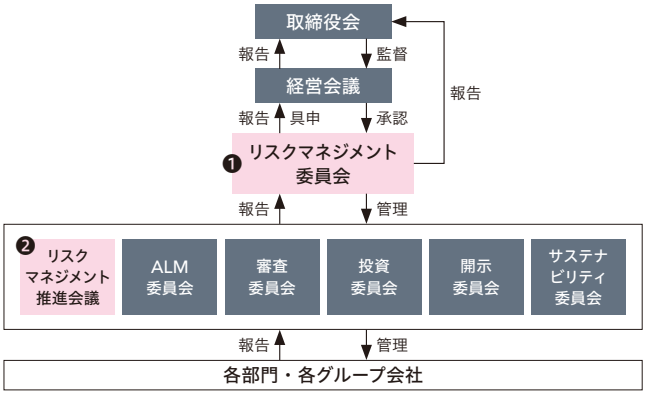
❶リスクマネジメント委員会

グループの事業に重大な影響を与えるリスクを管理すべく、当社の社長執行役員を委員長とし、経営会議メンバーおよびグループ各社の社長で構成するリスクマネジメント委員会を設置しています。当社グループ経営において、重要度が高いと考える管理項目を「グループ重点管理リスク」と定め、管理・監視を行うことでリスクマネジメントの強化に取り組んでいます。重要事項については、当委員会で討議後、経営会議に具申され、取締役会に報告されます。

<リスクマネジメント委員会の役割>

①リスクマネジメント方針および年度計画の決定
②グループ重点管理リスクおよびリスク主管区の決定
③リスク対策計画の決定
④リスク対策実施状況の確認およびフィードバック

リスクマネジメント推進体制図



❷リスクマネジメント推進会議

当社およびグループ各社相互において、緊密な連携、協調のもとグループリスクマネジメントを円滑に推進するためにリスクマネジメント推進会議を新たに設置しました。グループ重点管理リスクの主管区責任者とグループ会社のリスクマネジメント推進責任者により構成されます。グループ重点管理リスクに対する計画や対応状況はもとより、各社のリスク情報、対策状況などを共有し、討議を行った上で上位機関であるリスクマネジメント委員会へ報告します。

リスクアセスメント

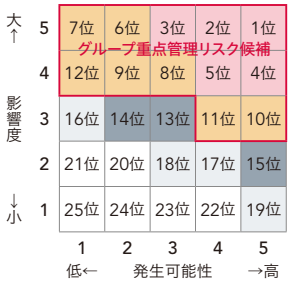
当社およびグループ各社におけるリスクを、内部環境、外部環境、経営戦略などの観点から洗い出し、リスク分析およびリスク評価を行うことで優先順位づけした「リスクマップ」を作成しました。

リスクが発生した時の「影響の大きさ：影響度」と「確率：発生可能性」の2軸でリスクの大きさを測り、リスクが高い項目をグループ重点管理リスクと定めています。

リスクマップとリスク評価基準

ランク	影響度評価基準
5	500億円超
4	500億円以下100億円超
3	100億円以下10億円超
2	10億円以下1億円超
1	1億円以下

ランク	発生可能性評価基準
5	毎年1回以上は発生する可能性がある
4	1年～5年に1回以上は発生する可能性がある
3	5年～10年に1回以上は発生する可能性がある
2	10年～30年に1回以上は発生する可能性がある
1	30年超に1回以上は発生する可能性がある



リスクマネジメント

グループ重点管理リスク

リコーリースグループにおいて、特に重要視する重点管理リスクは、グループ全社のリスクを横断的に管理するグループリスク主管区が、リスク対策計画を策定・推進し、グループ各社や関連する部門に対して、リスク対策指示と実施状況の確認を行い、リスクマネジメント推進会議へ報告を行います。

また、グループ会社では、各社固有の重点管理リスクを設定し、リスクマネジメントを実施します。固有の重点管理リスクの計画や実施状況などは、各社において経営判断がなされたあと、リスクマネジメント推進会議に報告・共有されることで統合的なグループリスクマネジメントを実現しています。

グループ重点管理リスク（グループリスク主管区およびグループ各社における位置づけ）

リスク分類	グループ重点管理リスク項目	グループリスク主管区	リコーリース	テクノレント	エンプラス	Welfareすずらん
自然災害	噴火／地震・津波	総務部／経営企画部	◎	◎	◎	◎
債権回収	大口顧客の貸し倒れ	審査本部	◎	○	◎	
対企業犯罪	サイバー攻撃	グループIT統括本部	◎	◎	◎	○
情報システム	情報システム障害・破壊	グループIT統括本部	◎	○	◎	○
経済	金利変動	財務部	◎			
ビジネス戦略	買収・合弁・提携の失敗	戦略投資本部	◎			
ESG対応	ESG対応不備・遅れ	経営企画部	◎	○	○	○
資金調達	資金繰り悪化・支払い遅延	財務部	◎			

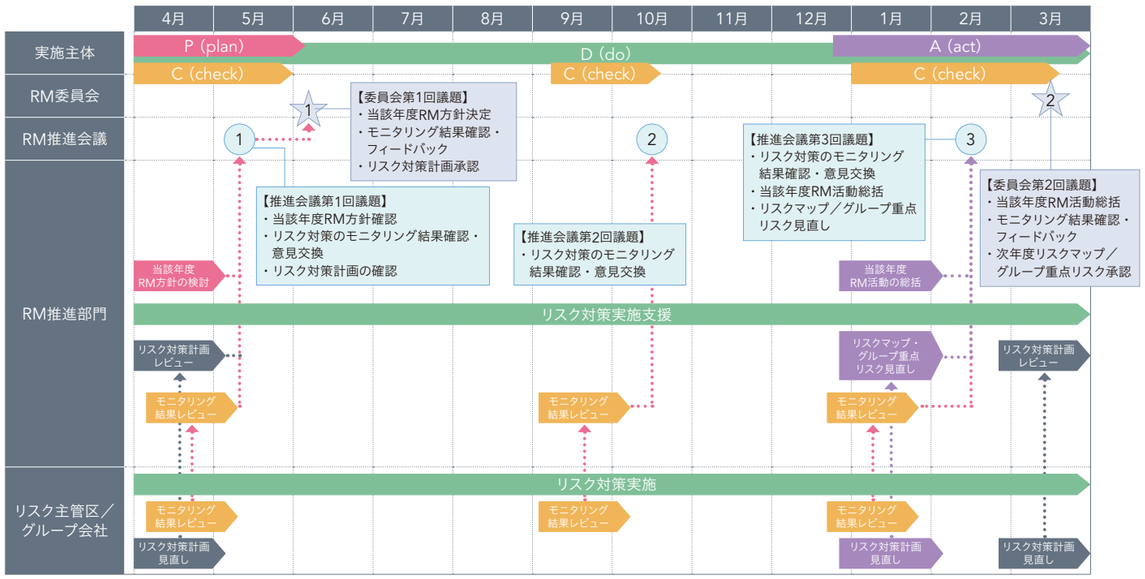
※ ◎：自社が主体となって重点的に取り組むべきリスク
　○：リコーリースの指示や指導のもとに取り組むべきリスク

リスク管理プロセス

当社グループでは、単年度では対策を完了できないリスクが多いことを考慮して、リスク管理プロセスを3年単位とし、対策計画を立て実施、監視していくことでPDCAサイクルを回しています。実行から評価・監視、改善に関する期間を十分に確保することで、対策の実効性を高めることにつながります。リスクマネジメント推進会議は、年に3回開催され、5月に当年度の対策計画が決定し、中間報告を経た後の2月には年度総括および次年度のグループ重点リスクが確定され、リスクマネジメント委員会にて最終判断がされます。

会議体の運営とリスクマネジメント活動のPDCAサイクル

※表内のRMは、すべてリスクマネジメントを指す



BCP・災害対策

東日本大震災の教訓を踏まえ、災害時に社員一人ひとりが的確に行動できるように行動マニュアルをそのときの状況に合わせ再整備するとともに、地域ごとの防災訓練を毎年実施し、2023年度からはリコーリースグループ合同の災害対応訓練を実施しました。

訓練では、実際の災害発生時にスムーズに対応できるよう「災害時の初動対応（現地活動）」と「BCP（本部活動）」を分けて活動することにしています。

「一斉帰宅抑制推進モデル企業」認定を機に、通常の備蓄品はもちろん、本社のほか、全国の主要拠点に出社全員分をカバーできる数の寝袋・枕を配布し、帰宅ができなくても安心な環境を用意しています。また、災害情報収集用テレビ・蓄電池も配布し、インフラ復旧までの活動が可能な環境も確保しています。

各拠点との通信手段については、IP無線を導入したことで、当社グループ各社と被災状況の確認や対策の検討が可能になりました。

安否確認システムについては、新システムを導入し、グループ各社社員の災害時安否情報が収集できるよう整備を行いました。また、台風や大雨・大雪予報の際にも無理な出勤・外出はしないよう通知をするなど、社員の安全を第一に考え、グループとしての防災を進めています。

年度	主な取り組み
2018	● リコーグループ防災訓練実施　● リコーリース各拠点災害対応訓練実施　● リコーグループ合同災害対応訓練（南海トラフ地震を想定：応用訓練）
2019	● リコーグループ防災訓練実施　● リコーリース各拠点災害対応訓練実施　● リコーグループメッセージボードをリニューアル
2020	● リコーグループ防災訓練実施　● リコーリース各拠点災害対応訓練実施 ● 在宅勤務下を踏まえた防災マニュアルの全面的な見直し　● 営業車防災バッグ導入
2021	● リコーグループ防災訓練実施　● リコーリース各拠点災害対応訓練実施 ● 地震発生時 事業所対応マニュアル作成（本社・豊洲） ● Webサイト上での消防学習導入 ● 災害発生時、teamsでの安否情報共有開始 ●「一斉帰宅抑制推進モデル企業」認定取得 ● 災害発生時当日宿泊セット用意（本社150個・豊洲250個） ● 車両防災バッグ備蓄品追加（食料飲料水1日→3日分・トイレ・毛布） ● 帰宅用防災バッグを肩掛け鞄からリュックサックに変更
2022	● 災害時利用通信機器として、IP無線導入 ● 主要拠点用、災害情報収集用テレビ・災害時利用蓄電池購入 ● 寝袋・枕購入（本社150セット・豊洲250セット） ● 社内掲示板にて防災通信発信開始
2023	● グループ各社に安否確認新システムおよび災害利用IP無線機を導入 ● グループ各社と共通システムにて災害情報の共有を開始 ● 本社および主要拠点に寝袋・枕を購入 ● 本社および豊洲事業所にて火災VR体験会を実施 ● コンセントの発火防止、コピー機走り出し・プリンター転倒防止対策を実施

情報保護管理体制と情報セキュリティ対策の強化

当社は2003年にリース業界で初めてISMS認証を取得、2005年にはプライバシーマークを付与され、情報セキュリティと個人情報保護のマネジメントシステムを一体的に運用してきました。これまで継続的にマネジメントシステムの運用の改善・強化を図ってきたことで、情報管理体制の強化と社員の情報保護・管理の意識の向上が図られ、その結果ISMS認証を継続することができました。また情報セキュリティおよび個人情報保護に関わる重大な事故は発生していません。

2023年には新たな認証であるISO27017（クラウドサービスセキュリティ）を取得しました。近年利用が増加しているクラウドサービスは、利便性・拡張性・コストメリットなどから非常に便利なツールと言えます。しかしながらその反面、情報漏洩・データ消失・サイバー攻撃・不正アクセスなどのさまざまなセキュリティリスクもクラウド環境のなかには点在しています。そのため社内でのクラウドサービスの安心・安全な利用が行えるよう、当社はISO27017の管理策を用いてクラウドサービスセキュリティへの堅実な取り組みを行っています。

また世界的に増加しているサイバー攻撃への対策として、技術的なセキュリティ対策はもちろんのこと、人的対策として社員へ定期的なメール訓練を実施し、不審なメールを見分けるスキルの向上や情報セキュリティ／サイバーセキュリティ情報の発信によりリテラシーの向上を図っています。加えて、高度化するサイバーセキュリティへの脅威に対応すべく、CSIRT（Computer Security Incident ResponseTeam）の強化など、有事の対応力の強化に向けた取り組みを実施していきます。

これらの取り組みは当社のみならず当社グループ会社においても重要な事項であると認識し、情報セキュリティ活動の横展開を開始しました。

今後も法令や当社情報セキュリティ基本方針および個人情報保護方針にのっとった活動を推進することで、ステークホルダーの皆様から常に信頼を得られるよう、情報セキュリティの強化に継続的に取り組みます。