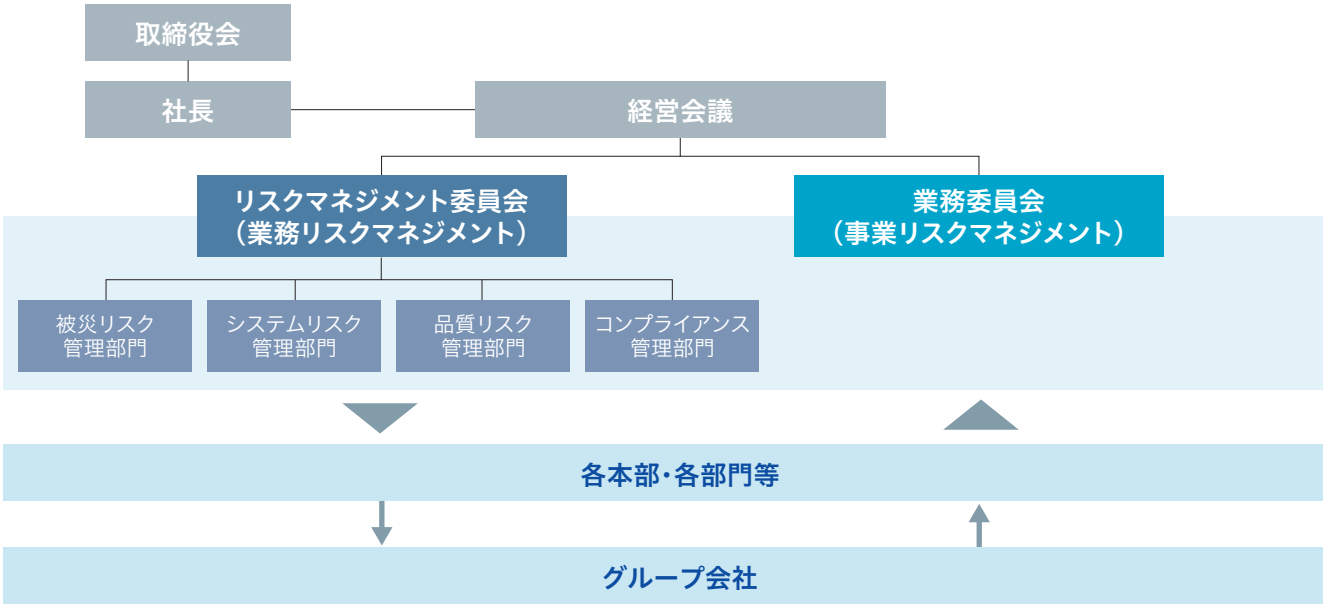
リスクマネジメント

リスクマネジメント体制

「経営会議」が当社グループのリスクマネジメント全体を統括し、その議長である社長執行役員がリスクマネジメントを統括しています。そのもとで「業務委員会」が事業リスクを、「リスクマネジメント委員会」が業務リスクを、それぞれマネジメントしており、これらのリスクマネジメント体制を取締役会が監督しています。「リスクマネジメント委員会」は原則毎月1回開催し、業務リスクの抽出、対応策や再発防止策の検討・立案などのほか、必要に応じて全社やグループ会社への情報共有などを実施しています。

■ リスクマネジメント体制図



業務委員会

事業リスクを管理することを目的として、「業務委員会」を設置し、経営計画および特定の経営課題の審議ならびに遂行管理等を行っています。「業務委員会」が全社および当社グループにおいて果たす役割は以下のとおりです。

1. グループ戦略の立案、審議
2. 中長期経営計画および単年度計画の企画立案、事前審議、調整
3. 特定の経営課題に関する対応方針の審議およびその対応の進捗管理
4. 組織体制、要員計画等の企画・立案、審議
5. 全社および当社グループの事業リスクの統括管理
6. その他重要事項の審議

リスクマネジメント委員会

業務リスクを管理することを目的として、「リスクマネジメント委員会」を設置し、リスクマネジメント方針・計画の策定およびリスク課題の把握・評価、対応策の策定ならびに指示などをしています。

「リスクマネジメント委員会」では、リスクマネジメントに関する国際標準規格ISO31000などを参照し、業務リスクを統括的にマネジメントするとともにPDCAサイクルを確立し、クライシス対応や予防的リスク管理をより的確に実施できる体制としています。コンプライアンス違反と判断された場合は、リスクマネジメント委員会が調査と対処を指示し、モニタリングを行います。「リスクマネジメント委員会」が全社および当社グループにおいて果たす役割は以下のとおりです。

1. リスクマネジメント方針・計画の策定
2. リスクマネジメントに関する組織整備ならびに責任・役割の明確化
3. 管理すべきリスク課題の把握・評価、対応策の策定ならびに指示
4. リスクマネジメント状況の把握・評価、改善策の策定ならびに指示
5. 緊急性の高い事件事故等の業務リスクが発生した場合の対応策の審議ならびに指示

主要なリスク

主要なリスクの詳細は有価証券報告書をご参照ください。

https://www.mitsuifudosan.co.jp/corporate/ir/library/fs/pdf/YUHO_2503.pdf

サイバーセキュリティ

企業を標的としたサイバー攻撃は高度化・巧妙化し、事業継続における重大なリスク要因となっています。三井不動産グループでは、すべての事業領域においてDXを推進するなか、サイバーセキュリティ対策が経営の重要課題の一つであると認識しています。
当社グループでは5つのサイバーセキュリティの基本方針を策定し、包括的なサイバーセキュリティ対策の強化に取り組んでおります。また、サイバーセキュリティの状況を経営層に定期的に報告する体制を整え、経営レベルでの監視・意思決定を行っています。

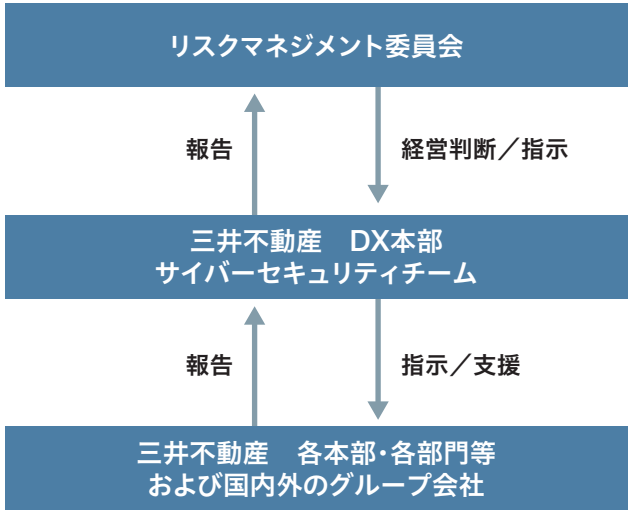
■ サイバーセキュリティの基本方針

- 基本的対策の徹底
- 侵入がありうる前提での検知力／即応力強化
- 可視化・モニタリング
- 建物のセキュリティ強化
- グループセキュリティシステムの総合進化

経営層へのサイバーセキュリティレポート

当社は、サイバーセキュリティを重要な経営課題として位置付け、経営層への適切な状況報告体制を確立しています。社長執行役員を筆頭とした経営陣によって構成されるリスクマネジメント委員会において四半期ごとに実施されるセキュリティレポートでは、グループ内で発生したセキュリティインシデントの詳細と対応状況、世のなかで確認された重大なセキュリティ事案の分析と教訓、そして各セキュリティシステムの検知状況と傾向の分析内容が報告されています。
これにより経営陣は、潜在的なリスクと実施中の対策効果を定量的・定性的に把握し、サイバーセキュリティに対する経営判断に活用しています。また、三井不動産DX本部に設置しているサイバーセキュリティチームでは、グループ会社から報告を受けたセキュリティインシデントへの対応指示・支援も行っています。

■ サイバーセキュリティ状況のレポーティングライン



先進的なサイバーセキュリティの取り組み

当社では先進的なセキュリティの取り組みとして「最新脅威情報の継続的な分析による迅速な脆弱性対応」を推進しています。年間数万件発表される世界中のソフトウェアの脆弱性を数百種類のセキュリティ情報源から毎日、情報を収集・分析し、社内外のセキュリティ専門家で検討した基準に基づき脆弱性の緊急性を判断しています。緊急性が高いと判断した脆弱性については、攻撃手法の詳細調査を行い、当社アセットに影響を及ぼすかを評価し、必要に応じて即時対応しています。実際に当社が即時対応を決定した脆弱性のなかには、国内外のサイバーセキュリティ関連機関の情報発信よりも早く対応を開始したものや、別組織において攻撃被害が発生したと発表されたものも含み、本対応により重大インシデントを未然に防止しています。この選択と集中による脆弱性対応の仕組みにより、実際に攻撃を受ける可能性の高い脆弱性へのリソース投入を最適化し、顧客データの保護と事業継続性をサイバー攻撃の脅威から守っています。

■ 2024年度実績