リスクマネジメント

基本的な考え方

当社グループは、事業活動によって発生するさまざまなビジネスリスクを認識しており、リスク発生を回避し、リスクが発生した場合は早期対応に努め、影響を最小限に抑えることを方針としています。適切なリスク管理を行い、持続的な成長を目指します。

リスク管理体制

当社グループは、リスクの発生を未然に防ぐため、内部監査を通じてリスクを網羅的に特定しています。グループ会社に対しては、代表取締役社長の諮問機関である業務監理委員会が、法令遵守やリスク管理の適切な運用を支援・指導するとともに、業務執行上のリスクをモニタリングしています。また、内部監査で抽出された課題は、管理本部・管理部などを中心とするプロジェクトチームが週次で進捗を管理し、継続的な改善を通じて経営の透明性と質の向上を図っています。

危機対応体制の整備

当社グループは、BCP（事業継続計画）の一環として、地震・火災・風水害などの自然災害や、有害物質の漏出、不慮の事故、経営危機など、さまざまな危機を想定した「危機管理マニュアル」を策定しています。同マニュアルでは、危機管理体制への移行条件や、各拠点・各本部における具体的な対応を定めています。危機発生時には、管理本部内に「経営危機管理対策本部」を設置し、平常体制に移行するまで対応を指揮します。各拠点で危機が発生した場合は、速やかに本社へ報告するとともに、安否確認システムを活用し、従業員やその家族の安否、人的・物的被害の状況を迅速に把握します。また、収集した情報をもとに外部への情報開示の必要性を判断し、必要に応じて当社ホームページで開示しています。

さらに、危機管理マニュアルに基づく緊急連絡訓練を定期的に実施し、取締役も参加して危機対応体制の実効性を検証しています。各拠点・工場においても毎年防災訓練を実施するなど、継続的な危機対応力の向上に努めています。

情報セキュリティ

情報セキュリティ基本方針・体制

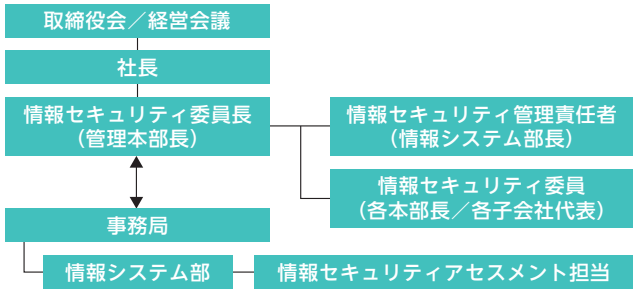
当社グループは、システムの安定稼働とデータの安全確保を重要な経営課題と認識し、「情報セキュリティ基本方針」を定め、グループの情報資産を保護する指針としています。また、デジタル化の進展やサイバーリスクの高度化を踏まえ、グループ全体の情報セキュリティ体制の強化に継続的に取り組んでいます。

2025年12月には「情報セキュリティ委員会規程」を策定し、海外拠点を含むグループ全体のガバナンスを強化しました。同規程に基づく情報セキュリティ委員会は、情報システム部を事務局とし、各本部長・部長などの業務責任者が参画しています。原則月1回開催し、法令遵守やリスク管理、情報管理業務のモニタリング、インシデント発生時の対応、役員・従業員への教育・啓発など、情報セキュリティに関する重要事項を継続的に協議しています。

さらに、2026年1月には「情報セキュリティ基本方針」に、情報セキュリティ、情報リスクアセスメント、セキュリティインシデントへの対応、デバイス利用、生成AI活用などに関するガイドラインを追加し、情報資産の保護と事業継続性の確保に向けた対策の実効性向上に取り組んでいます。

情報セキュリティ基本方針

情報セキュリティ委員会体制図



＜2025年度　情報セキュリティ委員会　主なテーマ＞

- AIによるサイバー攻撃の脅威とその対応
- 経産省サプライチェーン評価制度について
- IT BCPドラフトについて
- 米国NIST（National Institute of Standards and Technology）のサイバーセキュリティ フレームワーク2.0について　ほか

サイバーセキュリティ対策

大規模な災害発生やフィッシングメールなどの悪意のある攻撃から、システムを構成するハードやソフトを守るため、徹底したセキュリティ対策を実施しています。2026年1月には、EDR※1およびSOC※2を導入することで、24時間365日の監視体制を構築しました。

また、社内イントラネットでの注意喚起に加え、取締役およびグループ会社の出席者を含む経営会議の場においても、継続的に注意喚起を行っています。2025年度には、国内外の各グループ会社計10名を対象に、情報セキュリティ研修を実施し、情報セキュリティに関する理解度の向上を図りました。

※1 Endpoint Detection and Response
※2 Security Operation Center

サプライヤーを対象としたセキュリティ調査の実施計画

サプライチェーン全体のリスク低減を目的に、今後、サプライヤーを対象とした、セキュリティ水準ならびにセキュリティ強化に向けた取り組み状況に関する調査実施を計画しています。