情報セキュリティ

方針

当社グループでは、情報セキュリティを重点対策リスクのひとつに特定しています。情報セキュリティを含む情報の取り扱いについては「グループ情報管理規則」、その情報を保存・利用するための情報システムの取り扱いについては「グループ情報システム管理規則」にそれぞれ規定し、重要な経営資源としての情報の保護と活用を通じて、組織の信頼性と企業価値の持続的向上に資する取組みを行っています。

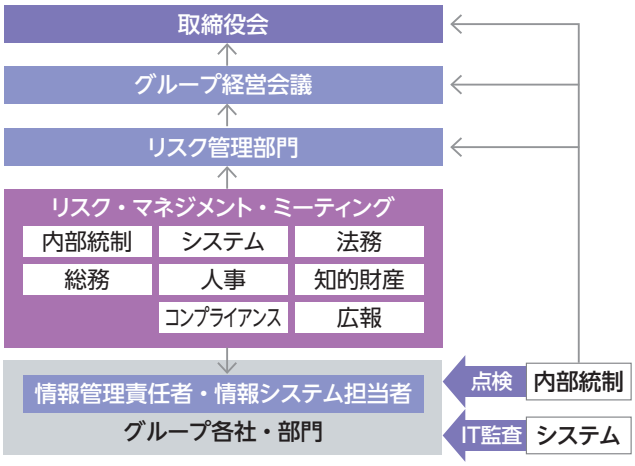
この方針および方針に基づく計画、取組みは、グループ経営会議で審議・決定し、当社取締役会へ報告します。当社取締役会は報告に対して必要な指示を行います。

体制

情報セキュリティリスクの総合的管理はシステム部門と内部統制部門によって行っています。情報管理のルールや体制整備などのソフト面での管理は内部統制部門が担い、加えて法務、知的財産、総務、人事の各リスク管理部門が連携して対応しています。情報・通信システム機器の整備・保全などのハード面の管理はシステム部門が担っています。情報セキュリティ、情報保全、情報利活用などの複合的課題を協議・解決するために内部統制、システム、法務、知的財産、総務、人事、コンプライアンス、広報の部門によるリスク・マネジメント・ミーティング（RMM）を隔月で開催し、課題への対処を検討しています。

RMMで決定した事項は、グループ各社・部門で任命している「情報管理責任者」および「情報システム担当者」などを通じてグループ各社・部門へ展開します。実行状況のモニターのため、すべてのグループ会社・部門を対象とした、内部統制部門による情報管理体制・運用状況の点検やシステム部門によるIT監査を年1回実施します。情報セキュリティに係る課題や点検結果などは、半期ごとに当社グループ経営会議および取締役会へ報告しています。

情報セキュリティ体制図



2022年度の取組み

1. システムの管理統制強化（IT全般統制）

施策	内容
システム変更手続きの統一	システム変更は、一貫性と透明性を確保するために、統一された変更手続きに基づいて実施します。 システムの起案承認～導入承認に関する手順と責任が明確化され、変更のリスクを最小限に抑えながら効果的な変更管理を実現します。
利用者の管理	システム利用者に関しては、アカウントの作成・削除、アクセス権限の付与・剥奪などを包括的に管理しました。役職や業務に基づいた適切なアクセス権限の付与、アカウントの不正使用の監視、退職者や転勤者のアカウントの適切な処理などを実施し、情報資産への不正アクセスのリスクを低減します。
システムの脆弱性管理	定期的な脆弱性評価と監視を実施し、システムの脆弱性を特定し、修正することにより、悪意のある攻撃やシステムの不正利用を防止します。また、セキュリティパッチの適用と脆弱性情報の共有により、迅速な対応が行われているかの管理を実現します。
BCP（事業継続計画）対策	災害や緊急事態に備えて、BCP対策を強化しました。適切なデータバックアップとリカバリプロセスの確立、代替施設やクラウドサービスの活用、緊急時の連絡体制などを整備し、業務の継続性を確保します。

2. ユーザー認証強化

施策	内容
多要素認証の導入	従来のIDとパスワードに加え、多要素認証を導入することで、利用者の身元をより確実に認証し、不正アクセスのリスクを低減しました。多要素認証は、追加の認証要素を要求することで、セキュリティレベルを向上させています。
多要素認証の展開と啓発	多要素認証の導入に伴い、利用者に対して適切な啓発活動を実施しました。多要素認証の利点、使用方法、設定手順についての情報を提供し、利用者が適切に多要素認証を活用できるよう支援しました。
監視と改善	多要素認証の運用開始に合わせて、パスワードの強化についても改善活動を実施しました。パスワードの強度や変更サイクルも見直し、継続的な改善活動を行っています。