

情報セキュリティ

方針

当社グループでは、従業員への情報セキュリティ教育・啓発を継続的に実施するとともに、生成AIをはじめとする先端技術の業務活用を積極的に推進しています。その一環として、2025年6月には「生成AIツールの業務利用に関するガイドライン」を制定し、AI活用に伴うリスクへの対応体制を整備しました。このガイドラインでは、業務での生成AI利用における著作権・倫理的懸念などのリスクを明確化し、適切な利用範囲や手順を定めています。これにより、技術革新の恩恵を最大限に活かしつつ、組織としての信頼性を確保し、企業価値の持続的な向上を目指しています。

体制

当社グループにおける情報セキュリティリスクの総合的な管理は、情報システム部門が中心となって推進しています。ITガバナンスの強化およびセキュリティインシデントへの的確な対応を目的として、以下の取組みを継続的に実施しています。

1. ITガバナンスの確立に向けた監査活動

グループ各社および各部門に対して、年1回の情報システム監査を実施しています。監査では以下の項目を中心に運用状況を確認し、改善点の抽出と是正対応のフォローアップを行っています。

- アクセス権管理の適正性
- バックアップおよび障害対応体制
- システムの脆弱性対策状況

これらの監査結果は、グループ全体のIT施策にフィードバックし、リスク低減に資する改善活動へとつなげています。

2. セキュリティインシデント対応体制の構築と運用

2020年10月に、セキュリティインシデント対策チーム「NLM-CSIRT」を設立し、以下の活動を通じてインシデント対応力の強化を図っています。

- インシデント予防および発生時対応手順の整備(防御・監視・検知)
- 全従業員を対象としたセキュリティ教育(LMSによるeラーニング)
- 標的型メール訓練やインシデント対応訓練の定期的な実施

これらの活動を通じて、従業員のセキュリティ意識の向上と、インシデント発生時の迅速な対応体制の確立を目指しています。

2024年度取組み

前年度より引き続きグループ全体の業務システムに関して、システムの管理統制強化と併行してセキュリティ強化対策を実施しました。

システムの現状把握、情報漏えい・セキュリティ対策		
施策	計画・実績	評価
IT診断の全実施	計画：38カ所 実績：38カ所	○
ペネトレーションテストの全実施	計画：162サーバー 実績：上期58+下期104サーバー	○
標的型メール訓練システムの実施	計画：年2回実施 実績：8月、3月に実施	○
国内外との情報連絡会の実施	計画：国内年2回、海外年2回 実績：国内5月、11月実施 海外9月(東南アジア)、10月(中国)実施	○
CSIRT強化	計画：年2回インシデント訓練の実施 実績：12月に実施	△※1
セキュリティ外部監視サービスの導入	サービス選定が完了し2025年度運用開始	○
セキュリティeラーニングの実施	計画：全従業員の実施 実績：実施完了	○

バックアップ・リストア、災害復旧対策の実行継続		
施策	計画・実績	評価
重要システムの復旧テストの実施	計画：10サーバー 実績：10サーバー	○
災害発生時の情報ツール見直し	情報ツール調査中	△※2

管理規則見直し継続、IT全般統制(ITGC)の準拠対応		
施策	計画・実績	評価
グループ情報システム管理規則見直し	パスワードポリシーの見直し(10月) 生成AIの業務利用に関するガイドライン策定	○
全システムのIT全般統制の準拠対応	2024年度評価より全システムの本運用開始	○

○：計画値、計画回数を達成 △：計画値や予定に対して未達
※1 2024年12月ですべての関係部門の訓練が一巡し、2025年度に向けた訓練内容の再検討を開始 ※2 2025年度中にシステム選定完了の予定