情報セキュリティ基本方針

株式会社リケンおよびグループ会社（以下、「当社グループ」という。）は、お客様や取引先をはじめとしたステークホルダーの皆様から預かった大切な情報をもとに事業を行っており、そうした情報を外部からの不正アクセスやサイバー攻撃、内部不正による情報流出などから確実に保護し、信頼に応えることが、経営の重要課題であると認識しています。

当社グループは、２０２２年７月１７日に発生した情報セキュリティインシデントによってステークホルダーの皆様に多大なご迷惑とご負担をお掛けしたことへの深い反省に基づき、改めて「情報セキュリティ基本方針」を見直すとともに、確かな情報セキュリティ管理体制を再構築し、情報セキュリティを継続的に向上していきます。

１．経営者の責任

当社グループは、情報セキュリティの確保を経営上の重要課題とし、情報セキュリティ管理に関する全ての事項の決定権限と責任を持つ「最高情報セキュリティ責任者（ＣＩＳＯ）」のもと、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に取り組みます。

２．コンプライアンス

当社グループは、情報セキュリティ関連の法令や規則、お客様・取引先との秘密保持契約をはじめとした契約上の義務、およびその他の社会的規範を遵守します。

３．情報セキュリティ管理体制

当社グループは、「ＤＸ・サイバーセキュリティ推進部」を主管部門として、サイバーインシデントを防ぐためのリスクアセスメント、IT システムや機器の脆弱性診断、不正アクセス・操作等の監視などの情報セキュリティ対策を確実に実施します。

また、当社グループは自動車産業の一員として「自動車産業サイバーセキュリティガイドライン」を指針とした情報セキュリティ強化の取り組みを推進し、継続的なレベルアップを図っていきます。

（次頁に続く）

４．情報資産の適切な取り扱い
当社グループは、情報セキュリティ関連諸規定に基づき、保有する情報資産を分類・整理し、機密レベルに応じた施錠保管やシステム的なアクセス制御、入退室管理などの適切な情報管理を行います。また、当社グループの役員および従業員等は、業務上の目的以外に、当社グループの情報資産を利用しません。さらに、外部の専門機関によるシステム監査等を継続的に受審し、適切性や信頼性を担保します。

５．情報セキュリティ教育
本方針を徹底するため、当社グループは、情報資産を取り扱うすべての役員および従業員等に対して、情報セキュリティに必要な知識（リテラシー）や、重要性やリスクの認識、利用者・管理者における責任と義務など、情報セキュリティを確保していくために必要な教育・訓練を継続的に実施します。また、情報セキュリティの関連部署や管理に携わる役員および従業員等には、役割に応じた階層別教育を行います。

６．情報セキュリティインシデントへの対応
当社グループは、情報セキュリティ管理体制のもと、ＩＰＡやＪＰＣＥＲＴ／ＣＣ等の外部組織から発信されるセキュリティ関連情報を適時に収集・確認し、継続的なセキュリティ監視および自社のＩＴシステム・機器のセルフチェックを行い、サイバーインシデントの発生予防に努めます。
また、インシデント発生に備え、効果的に対応するための体制・手順を平時から整備するとともに、万一の有事の際には、迅速に対応して被害の最小化に努めます。

２０２３年６月２３日
株式会社リケン
取締役常務執行役員　兼　最高情報セキュリティ責任者
坂場　秀博