JR 九州グループ情報セキュリティ基本方針

JR 九州グループは、日々進化するサイバー攻撃から情報資産を守り、「安全を最優先し、お客さま視点で考え、安心で快適な毎日と”わくわく”するときをつくる」という使命を果たすため、グループ全体で組織的かつ継続的に情報セキュリティ対策に取り組みます。

① 経営層の関与

経営層は情報セキュリティの確保を「重要な経営課題」と認識し、情報セキュリティの向上を持続的かつ積極的に実行します。

② 法令等の遵守

情報セキュリティに関する国内外の法令、国が定める指針、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 情報セキュリティ推進体制の整備

情報セキュリティに関する役割・責任を明確にし、対策を実施するための体制を整備します。

④ 関係規程類の整備・遵守

情報セキュリティ基本方針に基づく規程類及びガイドライン等を整備し、これを遵守します。

⑤ 情報資産の保護

多様なサイバーリスクから情報資産を保護するために、情報技術による対策、運用と管理による対策、手順やルールによる対策、物理的な対策等を行います。

⑥ 情報システムのセキュリティ対策

情報システムの特性に応じたセキュリティ対策を実施し、不正行為から情報システムを保護します。

⑦ 情報セキュリティインシデント対応

情報セキュリティインシデントが発生した場合には、CSIRT を中心に応急処置、原因究明、対策を迅速に実施し、再発防止に努めます。

⑧ 委託先の管理

情報資産を取り扱う業務を外部に委託する際には、情報が外部に流出することを防ぐために、委託先の適格性を確認し、秘密保持等必要な契約を締結します。

⑨ 教育・啓発活動の実施

情報セキュリティインシデントを未然に防ぐために、社員等に対する教育・啓発活動を継続的に実施します。

⑩ 積極的なコミュニケーション

情報セキュリティに関して組織内外のステークホルダーと積極的なコミュニケーションを図ります。

⑪ 継続的な改善

法令改正や社会情勢の変化、最新の脅威などに的確に対応するために、情報セキュリティ対策の運用状況を定期的に確認し、継続的な改善に取り組みます。

2025年 4 月 21 日