リスクマネジメント、情報セキュリティの取り組みに関する情報は以下のページをご参照ください
リスクマネジメントの取り組み（情報セキュリティ含む）
https://www.westjr.co.jp/company/action/risk_management/
JR西日本グループ情報セキュリティポリシー
https://www.westjr.co.jp/guide/security.html

リスクマネジメント

リスクマネジメントに関するJR西日本グループの考え方

社会環境が大きく変容する中にあっても、JR西日本グループとして社会からの信認に応え続ける姿を目指し、社長を委員長、業務執行取締役などを委員とする「リスクマネジメント委員会」において、当社グループの経営に重大な影響を与える可能性のあるリスクおよび危機的事象の洗い出しを行い、リスクマネジメントの仕組みや体制の点検、評価を行っています。

グループ各社においても、経営幹部の主体的な関与のもと、経営上重大な影響を与えるリスクの抽出・低減の取り組みを推進しています。

取り組みにあたっては、リスクマネジメントの国際的な標準規格であるISO31000も参照しながら、当社グループの事業活動全般において、適正なリスクマネジメントが行われる体制の整備に努めています。

推進責任者
代表取締役副社長兼執行役員
倉坂 昇治

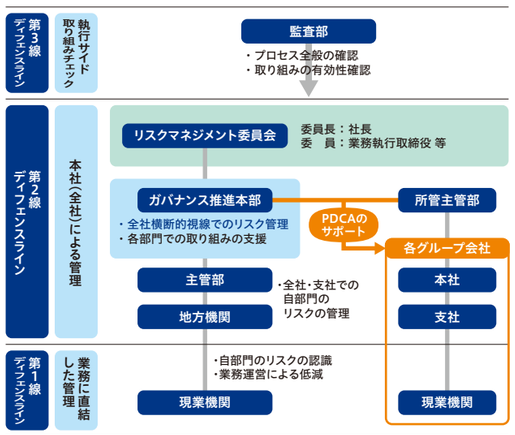
リスクマネジメントの取り組みの推進体制

当社では、「３つのディフェンスライン」によるＰＤＣＡサイクルでのリスクマネジメント体制を構築しています。

第１のディフェンスラインは、業務を遂行する現業機関での自律的なリスク管理であり、取り組みの基本となります。

第２のディフェンスラインは、現業機関を所管するスタッフ部門であり、現業機関の指導・支援などを通じてリスク管理の推進役の役割を果たしています。

第３のディフェンスラインは、内部監査部門であり、独立・客観の立場からプロセス全般を確認し、取り組みの有効性を確認しています。



コンプライアンスの取り組み

56ページを参照ください

危機管理の取り組み

- 自然災害、感染症、テロなどの多様化するハザードに対して、リスク事象発生時の迅速かつ適切な初動対応を構築すべく、体系化した規程・マニュアル類の整備、緊急時の情報連絡体制の構築、また定期的な訓練などを実施しています。
- 事業継続計画（BCP）を策定し、危機レベルに応じて柔軟に業務執行体制の構築が可能となるように危機発生時に備えています。

■大規模災害発生時の初動対応訓練の様子

情報セキュリティ

情報セキュリティに関するJR西日本グループの考え方

JR西日本グループは、情報資産を様々な脅威から守るために「JR西日本グループ情報セキュリティポリシー」を定めてこれを遵守し、グループ会社間の情報共有と相互連携により、グループ全体で情報セキュリティ対策を継続的に行っていくことを宣言しています。

近年、政府も国家戦略としてサイバーセキュリティの強化を要請しています。重要インフラを担う立場として、テレワーク拡大やDX進展に伴う脆弱性の拡大と、攻撃の巧妙化、脅威の増大に対し、経営課題として情報セキュリティに取り組んでいます。

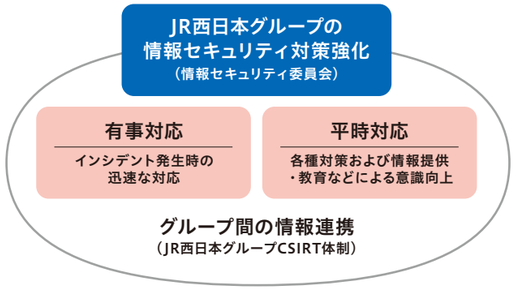
推進責任者
取締役兼執行役員
デジタルソリューション本部長
奥田 英雄

情報セキュリティの取り組みの推進体制

当社では、「情報セキュリティ委員会」を設置し、経営層と組織全体のリスクを共有し、セキュリティ対策の方向性を議論するとともに、グループ会社経営層とその実現に向けた認識共有を図っています。

また、セキュリティインシデントの未然防止や、発生時の被害拡大防止を目的としたグループ横断組織「JR西日本グループCSIRT※」を構築しています。

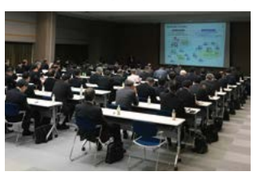
※シーサート（CSIRT）：Computer Security Incident Response Teamの略。コンピュータセキュリティに係るインシデントに対処するための組織の総称。



危機対応能力の向上

- 定期的な教育として、全社員向け情報セキュリティ教育および経営層向けトップ研修を実施しています。また、所定の研修を修了した参加者を社内独自資格である情報セキュリティリーダとして認定しています。
- 有事の際の訓練として、CSIRTメンバを対象としたインシデント対応訓練を実施するとともに、グループ会社も含めた全社員を対象とした標的型攻撃メール訓練を実施しています。

- 行政機関とも連携を深め、IPA（産業サイバーセキュリティセンター）への人財派遣や、内閣サイバーセキュリティセンターと連携した重要インフラ向け訓練にも参画しています。



PDCAサイクルの定着

必ず守るべき具体的なセキュリティ基準を定めたガイドラインを整備し、技術動向や過去のインシデントを踏まえて改善しています。これに基づき、毎年、当社およびグループ各社でIT環境の自主点検を実施し、継続的にセキュリティ対策を強化しています。