危機管理

社会の一員としての責任

●重要な生活・社会インフラを担う企業グループとして、危機対応能力を向上

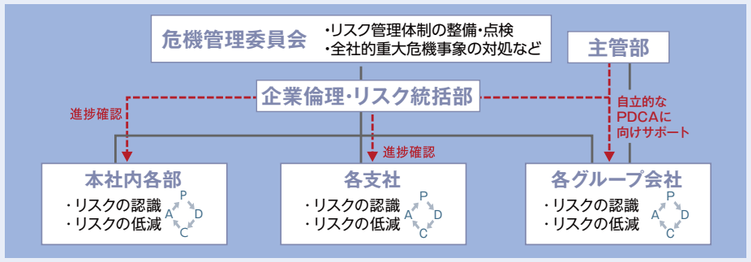
基本的な考え方

企業集団における内部統制システムの構築・運用が重要視される中、JR西日本グループでは、グループ全体の事業活動全般に関する適正なリスク管理体制の整備に努めています。万が一、不測の危機事象が発生した際に、ダメージの最小化に努めるだけでなく、平時から各種リスクの発生可能性や被害規模を極小化させるべく、リスクを予測し予防・準備を行うことが危機管理の要諦です。危機管理の取り組みの柱は、平時の取り組みとしての「リスクマネジメントの推進」、危機事象が発生した場合の被害規模を最小化させるための「有事初動対応力の向上」です。

推進責任者
企業倫理・
リスク統括部長
沖永 英治

JR西日本グループでのリスクマネジメント推進

内部監査
・プロセス全般の確認
・取り組みの有効性確認



Plan グループ一体となりリスクマネジメントを推進

Do 持続的な取り組みとなりグループに浸透

JR西日本グループでは、社会情勢の変化を意識しながら、各部門やグループ各社が自らを取り巻くリスクを洗い出し、それらの評価を行った上で、重要なリスクに対しては低減策を立案・実行しています。あわせて、点検や監査を通じて継続的改善を図るという「リスクマネジメント」PDCAサイクルの取り組みの一層の定着を進めています。

Plan 重要リスクの低減

Do 伊勢志摩サミット・関係閣僚会合での警戒警備体制を構築

リスクマネジメントで抽出した「重要リスク」については、その低減に向けての着実な取り組みが必要となります。

重要リスクの一例として、2016年4～5月、9月開催の「伊勢志摩サミット・関係閣僚会合」に関連したテロの発生があげられました。鉄道テロ対策、ソフトターゲット※1対策、サイバーセキュリティ対策を柱に、国土交通省、警察をはじめとした諸機関と連携しながらJR西日本グループ一体となり、警戒警備体制を構築しました。

社外からの一言

伊勢志摩サミット、オバマ大統領広島訪問での警備を終えて

伊勢志摩サミットに関連する外務大臣会合が2016年4月に広島市で開催され、また5月には、アメリカのオバマ大統領が広島市を訪問しました。

最近のテロ事件では、ソフトターゲットが狙われていることから、広島県警はJR西日本グループと連携して警戒を行い、またゴミ箱の撤去やコインロッカーの使用禁止などの措置を講じました。

警護警備に際し積極的に協力いただいたおかげで、無事一連の警備を終えることができました。今後ともJR西日本グループはもとより、一般の方々や事業者の方々の協力もいただきながら、テロ事案の未然防止に努めていきます。

広島県 世羅警察署長
（当時 広島県警察本部
警備部 サミット対策課長）
圖石 貞祐 様

伊勢志摩サミット・関係閣僚会合対策本部ミーティング

※1 ソフトターゲット：一般的に「警備や監視が手薄で攻撃されやすい標的」を指す、ホテルやレストラン、ショッピングセンター、スタジアム、博物館などの大規模集客施設

Plan グループ全体の有事対応能力の向上

Do 実践型訓練の実施

不測の重大事象が発生した有事（緊急時）に、被害の最小化と拡大の防止、新たな危機の連鎖発生防止のための緊急事態対処に万全を期すことが求められます。一例として、「大規模災害の発生」をテーマに当社・グループ会社の危機管理担当者に実践型の初動対応訓練を実施するなどして対応力の向上に努めています。

有事の初動対応をディスカッション

CHECK&ACTION

CHECK

継続的な取り組みとなっています

JR西日本グループのリスクマネジメントについては、各部門、各グループ会社ともに継続的な取り組みとなっています。今後は、リスクマネジメントPDCAサイクルの「C（点検・監査）」の充実を図り、リスクマネジメントの精度を向上させる必要があります。

ACTION

事業継続計画（BCP）※2をブラッシュアップします

更に、リスクマネジメントの「C」の充実の中で、企業共通の長期的な重要リスクである「事業継続計画（BCP）」についても、これまでの取り組みを検証した上で、大災害発災時にBCPが迅速かつ適切に発動できるようブラッシュアップします。

情報セキュリティ

Plan 情報セキュリティ施策の推進

Do 継続的な教育・訓練の実施とBCP対策強化

当社では、情報セキュリティを危機管理の必須項目と位置付け、高度化するサイバー攻撃やウイルスなどへの対策として、システム面でのセキュリティ強化を進めてきました。また、職場単位で情報セキュリティ推進者を配置し、定期的に個人情報や情報機器の適切な取り扱いを点検するとともに、全社員への教育や標的型メール訓練、グループ会社を含めた講習会を継続的に実施しています。

またBCP対策の強化に取り組み、2015年度は被災リスクの低い場所に堅牢なデータセンターを新たに建設し、システム基盤の運用を開始しました。

新データセンター及びシステム基盤が稼動

CHECK&ACTION

CHECK

情報セキュリティに関する重大な事故被害はゼロ

2015年度は情報セキュリティに関する重大な事故や被害は発生していません。しかしながら、不注意による個人情報の紛失や標的型メールが社内で確認されるなどのリスク事象が発生していることから、グループ全体で情報セキュリティ対策の継続的な取り組みが必要です。

ACTION

グループ全体の情報セキュリティ対策を推進

グループ会社共通のセキュリティルールや会社間の情報連携体制を整備するとともに、インシデント発生時に被害の拡大防止といった初動対応をサポートするシーサート（CSIRT）※3を構築します。また、重要インフラシステムのセキュリティ点検などを実施し、巧妙化するサイバー攻撃への対応を強化していきます。

※2 事業継続計画（BCP）：Business Continuity Planの略。企業が自然災害、事故、テロなどの予期せぬ緊急事態に遭遇した場合に、重要業務に対する被害を最小限にとどめ、最低限の事業活動の継続、早期復旧を行うために事前に策定する行動計画
※3 シーサート（CSIRT）：Computer Security Incident Response Teamの略。コンピューターセキュリティにかかるインシデントに対処するための組織の総称