危機管理

危機管理体制

J-POWER本店に危機管理対策チームを常設しているほか、危機の予見・発生時に緊急対策の必要がある場合に危機管理対策本(支)部を組織します。

危機管理対策チームでは、危機の予見、発生時の迅速な初期対応および危機管理対応業務の総括を行っており、有事の際は、各地区の危機管理対策本(支)部と連携し、災害や設備事故などの危機事象に対する的確な予見・防止、および顕在化した場合の迅速かつ適切な対応・管理を行っています。

また、毎年本店および対象地区の対策本(支)部と連携して総合防災訓練を実施し、当社社員およびグループ会社社員の安否報告訓練を実施しています。

危機管理に係る取り組み

国民生活に不可欠な電力の安定供給は電気事業者としての責務であり、電力を生産・流通する設備への障害を未然に防ぐとともに、障害が発生した場合は速やかに復旧する必要があります。このため、J-POWERグループでは以下の取り組みを行っています。

①地震・台風・落雷・津波などの自然災害に対する適切な設備対応と非常時の復旧体制の整備
②悪戯や暴力行為などに対する警備強化
③重大な供給支障防止に備えた日常の設備点検の強化、老朽化・機能低下・損傷設備に対する適切な修繕または更新
④パンデミックなど、事業運営に重大な影響を及ぼす事象に対する行動計画等の作成

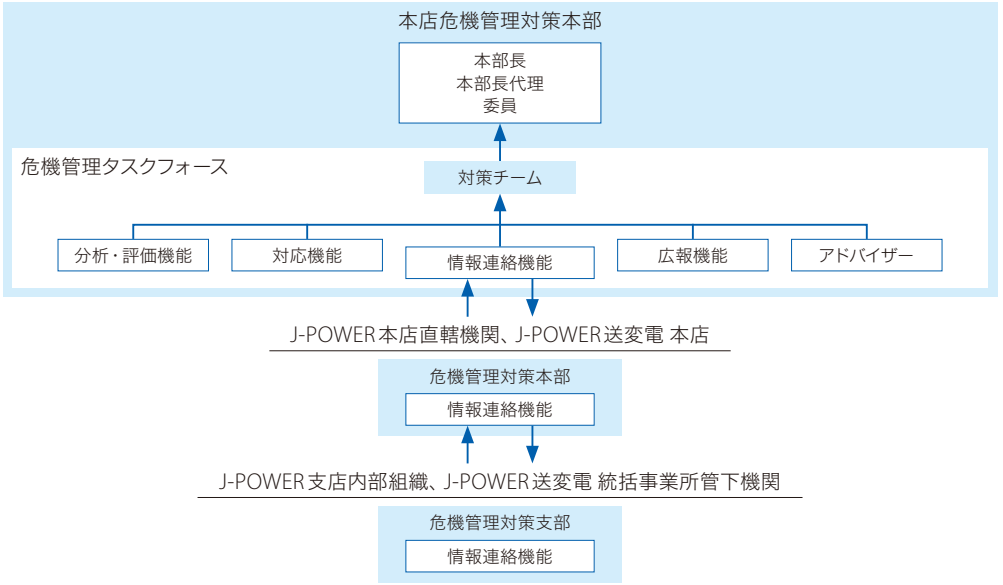
防災・事業継続への取り組み

当社は、基幹ライフラインを担う電気事業者として、災害対策基本法等に基づき指定公共機関に指定されています。

このため、大規模な自然災害も想定したハード対策とともに、災害発生等における規程類を整備し、本店から現地各機関までの体系的な防災体制などのソフト対策を積極的に進めることで、想定を超える災害被害に際しても事業を継続できるよう、防災体制の一層の強化を図っています。

なお、新型コロナウイルス感染症が拡大して以降においては、フルリモートの防災訓練を実施することで、社員の出社状況に拠らない防災体制も構築しています。

対策本部の連絡体制



サイバーセキュリティ

情報漏えいやランサムウェア*1による操業停止が社会問題になるなど、近年、サイバー攻撃は増加するばかりでなく高度化、巧妙化しています。当社は「サイバーセキュリティ基本法」の重要社会基盤事業者として、内閣サイバーセキュリティセンターの「重要インフラの情報セキュリティ対策に係る行動計画」に基づき、コンピュータウイルス対策や不正アクセス、情報漏えい対策など最新の知見を踏まえた技術的対策を実施しています。また、電力の安定供給のため電力制御システムなどのセキュリティ確保として、「電力制御システムセキュリティガイドライン」を遵守しています。

サイバー攻撃に対応し、万が一の被害発生時に迅速に回復できるよう、「情報セキュリティ基本方針」を制定するとともに、サイバーセキュリティに関する危機管理体制として「J-POWER CSIRT*2」を設置し、サイバーセキュリティ事故の未然防止と事故発生時の被害最小化に取り組んでいます。

*1 ランサムウェア：ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求するコンピュータウイルスの一種
*2 CSIRT (Cyber Security Incident Response Team)：サイバーセキュリティインシデントレスポンスチーム[注：本来CはComputerの頭文字であるが当社ではCyberとしている]