危機管理

事業基盤の強化

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するとともに、定期的に、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。

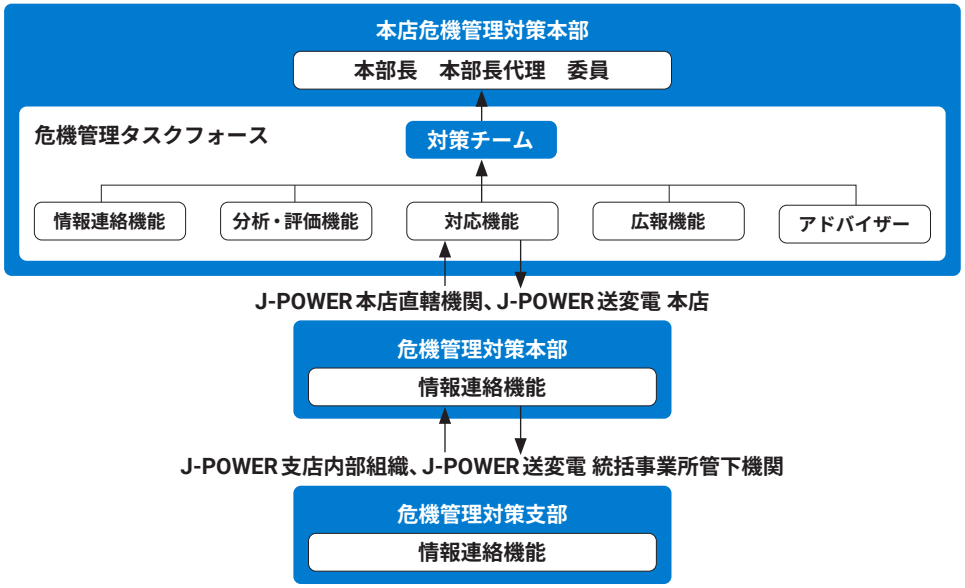
① 地震・台風・落雷・津波などの自然災害に対する適切な設備対応と非常時の復旧体制の整備
② 悪戯や暴力行為などに対する警備強化
③ 重大な供給支障防止に備えた日常の設備点検の強化、老朽化・機能低下・損傷設備に対する適切な修繕または更新
④ パンデミックなど、事業運営に重大な影響を及ぼす事象に対する行動計画等の作成

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、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。

危機管理対策本部の連絡体制



本店危機管理対策本部の構成

組織	構成
本部長	社長
本部長代理	副社長
委員	総務部担当役員および関係役員 総務部長、広報部長および関係部長
危機管理タスクフォース	危機管理対策チームおよび関係部

(タスクフォースの構成)	(分掌事項)
情報連絡機能	情報連絡、情報収集、情報管理
分析・評価機能	分析、評価、対策立案
対応機能	復旧対応、渉外、被害者対応、消費者対応、IRに関する情報
広報機能	メディア対応
アドバイザー	分析、評価、対策立案等に関する助言

危機管理

事業基盤の強化

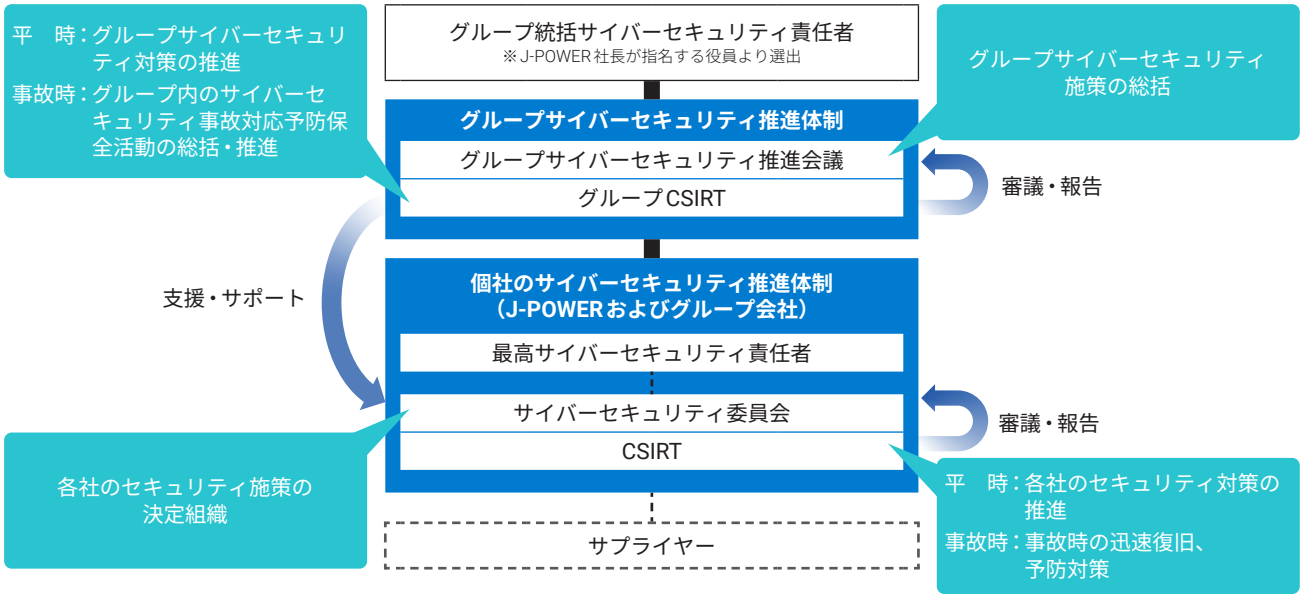
サイバーセキュリティ

情報漏えいやランサムウェア*1による業務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」に定める重要社会基盤事業者として、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のため、「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。

これらの施策と並行して、サイバー攻撃による万が一の被害発生時においても迅速に対処し、復旧できるようサイバーセキュリティに関する危機管理体制である「J-POWER CSIRT*2」を設置しており、サイバーセキュリティ事故の未然防止と被害最小化に取り組んでいます。

更に、当社は2022年6月17日に内閣サイバーセキュリティセンターより発表された「重要インフラのサイバーセキュリティに係る行動計画」に基づき、重要社会基盤事業者としてサイバーセキュリティ対策に万全を期す体制を整備し、更なる対策強化を進めています。また、2023年3月にグループが一丸となりサイバーセキュリティを推進するため、「J-POWERグループサイバーセキュリティ基本方針」並びに情報系と制御系を包含する「サイバーセキュリティ規程」を制定し、サプライチェーン全体での対応力を強化しています。

＊1 ランサムウェア：ファイルを暗号化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推進・対応チーム［注：本来CはComputerの頭文字であるが当社ではCyberとしている］



J-POWERグループサイバーセキュリティ基本方針

私たちJ-POWERグループの役員・従業員は、重要インフラを有し国民生活に多大な影響を与えうる企業として、サイバーセキュリティの確保に関する基本方針を以下のとおり定める。

1. 経営課題としての認識

経営者自らがサイバーセキュリティリスクと向き合い、サプライチェーン全体を俯瞰したサイバーセキュリティの強化を経営の重要課題として認識し、リーダーシップを発揮しつつ、自らの責任で対策に取り組む。

2. 法令及び契約上の要求事項の遵守

サイバーセキュリティに関わる法令、規制、規範、契約上の義務とともに、その他の社会的規範を遵守する。

3. 適切なサイバーセキュリティ対策の実施

サイバーセキュリティの維持及び改善のために推進体制・組織を設置し、人的・技術的・物理的対策を講じるとともに、新たな脅威の動向を把握し、速やかな対処を図る。また、取引先や委託先、海外も含めたサプライチェーン対策に努める。

4. 教育・訓練の取り組み

サイバーセキュリティに必要な知識、技術を習得し、教育・訓練に参加することでサイバーセキュリティへの取り組みを推進する。

5. 違反及び事故への対応

サイバーセキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処し、再発防止に努める。

6. 継続的な改善活動

以上の取り組みを定期的に評価、見直すことにより、継続的な改善活動を実施する。