

→ 情報セキュリティ

企業リスク一覧

以下は14の「企業リスク」が当社グループに与える影響や対応策をまとめた一覧です。対応策は「中期経営計画」と連動しており、定期的に進捗管理も行っています。

分類	項目	影響度	次年度の見通し	マイナス面	プラス面	対応策
戦略リスク	既存の事業モデルの衰退	非常に大	↑	●中核事業の業績低迷によるグループ全体の活力低下	●中核事業の事業モデルの抜本的な変革による再成長	●コンテンツの魅力向上、デジタルとの融合、環境価値の向上による店舗の魅力強化および都心の大型店舗の資産価値向上
	サステナビリティ経営の高度化	非常に大	↑	●対応の遅れによる投資家・株主の離反、格付けの低下	●着実な対応による持続的な成長	●「脱炭素社会の実現」をはじめとする7つのマテリアリティ(重要課題)の推進による「Well-Being Life」の実現
	加速度を増すデジタル化への対応	非常に大	↑	●グループ全体の成長の停滞 ●競争力の低下	●既存事業のビジネスモデルの変革 ●リアルな人とのつながりの再認識	●「OMO(オンラインとオフラインの融合)」によるビジネスモデルの変革 ●リアルとデジタル両輪でのコミュニケーションの高度化 ●デジタル化による業務の変革
	都市の分散化(都市と地方のリバランス)	大	↔	●都心立地の従来型商業施設の集客力低下	●都市の分散化に対応した事業展開	●都心店舗での防疫、非接触サービスの強化 ●都心や準都心での商業だけでなく多様な用途での不動産開発
	ポストコロナにおける消費行動の変化	大	↔	●消費ニーズとのアンマッチによる業績の低迷	●新規マーケットの開拓	●コモディティ(汎用)商品の適正規模への見直し ●「OMO(オンラインとオフラインの融合)」による顧客満足向上 ●アート・カルチャー・エシカル商品の強化
	業際を超えた再編、M&Aの加速	大	↔	●当社グループの敵対的買収	●事業ポートフォリオの見直し ●M&Aの活用による企業成長	●事業ポートフォリオのレジリエンス(強靱性)向上 ●他企業のM&A、他企業との業務提携による新規事業創出
	ニューノーマル時代の働き方、人財・組織改革の進展	大	↔	●優秀人材の流出 ●人材獲得競争での劣後	●企業文化の変革によるイノベーションの創出	●中途採用の強化 ●働き方の柔軟性の向上 ●サステナビリティ(持続可能性)のある組織への変革
	加速する所得の二極化	大	↔	●ボリュームマーケットの縮小による業績低迷	●新たな富裕層マーケットの出現	●ボリューム価格帯の商品・サービスの適正規模への見直し ●多様なアプローチによる富裕層マーケットの深耕
	顧客の変化、特に少子高齢化・長寿化	大	↔	●国内市場の縮小	●シニアマーケットの拡大	●上質な子どもマーケットの深耕 ●安全・安心な店舗環境の整備 ●アート・カルチャー・ウェルネスの強化
外国人マーケットの不透明さ	大	↔	●インバウンド売上大幅減少の長期化	●新たなアプローチによる外需の獲得	●インバウンド戦略の見直し ●越境ECやライブコマースの強化	
ファイナンスリスク	資金調達マネジメントの重要性の向上	大	↔	●資金不足による経営破綻 ●不利な条件での資金調達による成長の停滞	●成長分野への投資資金確保による事業育成	●グループ資金調達の一元化と資金効率化 ●資金調達手段の多様化
	環境変化に対応できるコスト構造の必要性	非常に大	↔	●事業存続の危機 ●業績回復の遅れ	●事業ポートフォリオの組み替え ●成長事業への投資	●ビジネスモデル改革によるコスト削減 ●事業基盤の絞り込み
ハザードリスク	頻発する自然災害・疫病	非常に大	↔	●顧客・従業員の人命損傷 ●事業継続の危機	●地域社会の安全・安心確保への貢献	●「事業継続」[感染症対応]マニュアルの整備 ●BCP訓練の継続的な実施
	情報セキュリティの重要性向上	大	↔	●重要情報流出による社会的信用失墜・営業損失 ●業務の遅延・停滞	●円滑なDX(デジタルトランスフォーメーション)の推進	●「情報セキュリティポリシー」[ITガバナンス方針]の整備 ●システムのクラウド移行の推進 ●教育・訓練による情報リテラシーの向上

情報セキュリティ

サイバー攻撃の手法が高度化・巧妙化している中、JFRグループでは、「侵入を完全に防ぐのは不可能であり、攻撃を受ける前提でいかに早く復旧させるか」という考え方のもと、NIST※1のサイバーセキュリティフレームワークに基づいたセキュリティ対策を推進しています。

当社内にCSIRT※2(シーサート)を設置し、当社とグループ各社の情報セキュリティ管理責任者が連携し、インシデント発生時に備えたマニュアルの整備や対応訓練を実施し、グループ全体の情報セキュリティ管理体制の強化を進めています。

また、2020年に制定した「ITガバナンス方針・規程」では情報セキュリティポリシーの遵守を重点施策の一つとしています。その取り組みとして、全従業員を対象としたeラーニング、標的型攻撃メール訓練を継続的に実施し、従業員の情報セキュリティの遵守と意識の向上を図っています。

加えて、テレワークの浸透やクラウドサービスの拡大などの環境変化を踏まえ、インシデント発生時の業務端末の隔離と復旧、未許可のクラウドサービスを可視化・制御するシステムの導入を進めています。安全かつ働く場所にとらわれない情報セキュリティへの対策を行うとともに、サイバー攻撃に対して素早く分析・対応を行う体制を整備し、対策に抜け漏れがないよう常にアップデートを行っています。

※1 National Institute of Standards and Technology (米国国立標準研究所)
 ※2 Computer Security Incident Response Team (コンピュータセキュリティインシデント対応チーム)