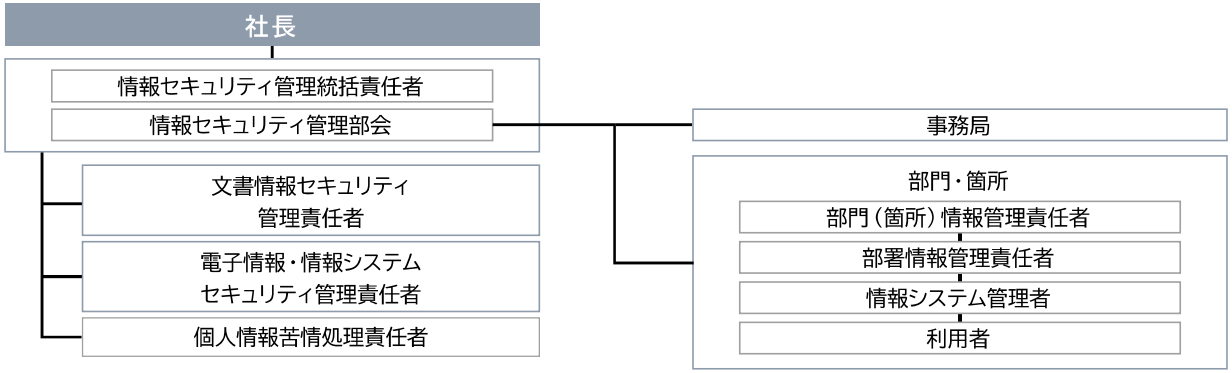
マイナスのインパクトの是正プロセス | リスクマネジメント

GRI 2-12,16,25/403-2,4

日油の情報セキュリティ管理体制図



情報セキュリティにおけるリスクと機会、およびリスクに対する施策

リスクまたは機会	内容	施策
リスク	● サイバー攻撃（不正アクセス、マルウェア感染）による生産活動・販売活動・研究開発活動の長期間の停止、および企業信頼の失墜 ● 機密情報・個人情報の漏洩による企業信頼の失墜、技術競争力の低下	● 自己点検の実施と改善計画策定、および改善計画実施 ● 国内グループ会社IT担当者会議による情報共有（1回／年） ● 不審メール対応訓練の実施（1回／年） ● 社外持出PCのHDD暗号化、私用記憶媒体の利用制限による対応 ● 社員向け、情報セキュリティ関連の教育実施（1回/年）
機会	● サイバーセキュリティ対策により、企業の競争力の向上 ● 情報資産管理の強化により、顧客からの信頼の獲得、および企業のブランド価値の向上 ● 情報セキュリティ強化により、社員の意識向上	−

事業継続計画（BCP※）の推進

日油は地震・津波などの自然災害や新型コロナウイルス感染症の流行のような非常事態が発生した場合においても、事業資産の損害を最小限にとどめつつ、中核となる事業の継続あるいは早期回復を可能とするため、BCPを策定しています。平常時と非常時における対応を決めたマニュアルを中心に、設備想定被害、復旧時に必要となる行政・インフラやサプライチェーン関係などの情報を整備し、毎年更新を行っています。また、年次で内部監査および訓練を実施し、BCPの定着と実効性の向上を図っています。

2023年度は、情報セキュリティにおけるリスクへの対応として、サイバー攻撃が発生した事態を想定したBCP訓練を実施し、インシデント発生時の初期対応手順や事業継続に向けた各部門・箇所の役割を確認することで、サイバー攻撃時の被害の最小化や迅速性など対応力の向上を図りました。

※ Business Continuity Planの略。大地震等の自然災害、感染症のまん延、テロ等の事件、大事故、サプライチェーン（供給網）の途絶、突発的な経営環境の変化など不測の事態が発生しても、重要な事業を中断させない、または中断しても可能な限り短い期間で復旧させるための方針、体制、手順等を示した計画のこと。