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

情報セキュリティ管理

（1）営業秘密管理および個人情報保護

日油では、顧客や取引先からお預かりした、または保有する企業秘密・個人情報などの情報、およびそれらを利活用するためのシステム等の情報資産が企業活動において重要な経営資源であり、情報資産に対する堅牢な情報セキュリティの確立が安定した経営を実現するために不可欠であるとの認識に基づき、情報資産の活用と保護を推進するための基本方針として情報セキュリティポリシーを制定しています。同時に、日油では、個人情報を保護することが当然の社会的責務であるとの認識に基づき、プライバシーポリシーを制定し、公表しています。

上記のポリシーに基づき、情報の機密性、完全性、可用性のレベルを高めるための具体的施策および個人情報の具体的取り扱い方法を、情報セキュリティ管理規則、個人情報保護規則、情報システム関連諸規定等の社内規定ならびに機密情報取扱マニュアルおよび情報機器取扱マニュアルに定め、周知徹底を図っています。

（2）管理体制

社内組織としては、情報セキュリティに係る重要事項を審議、決定する機関として、情報セキュリティ管理部会を設置し、部会長である情報セキュリティ管理統括責任者のもと、文書情報セキュリティ管理責任者、電子情報・情報システムセキュリティ管理責任者、個人情報苦情処理責任者および部門、箇所、部署ごとに管理責任者を置き、具体的施策の運用を管理しています。また、外部からの不正アクセス、または漏洩、改ざん、破壊等の脅威に対して、適切かつ合理的なレベルの安全対策を実施しています。加えて日油では、内部監査を通じて、情報セキュリティ管理および個人情報保護に係る体制および施策を継続的に見直し、その改善に努めています。

日油グループ情報セキュリティポリシー

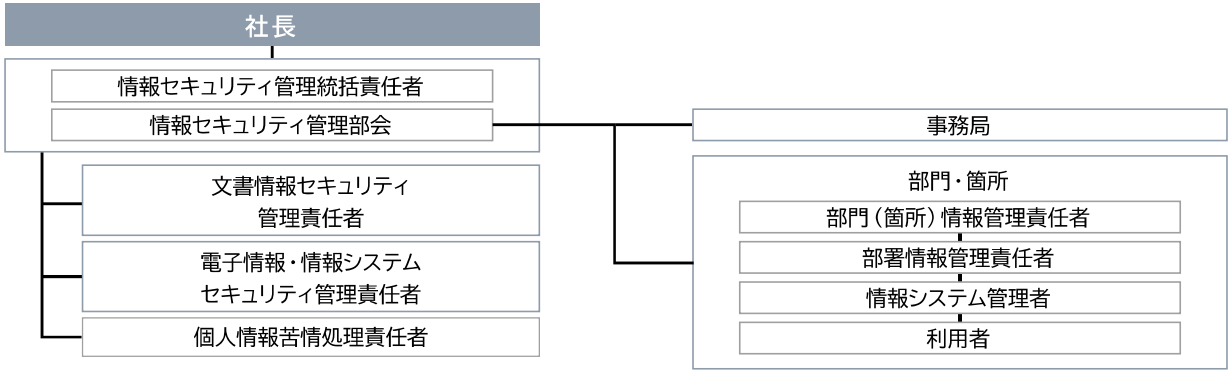
日油グループは、顧客や取引先からお預かりした、または日油グループが保有する企業秘密・個人情報などの情報、およびそれらを利活用するためのシステム等（以下「情報資産」という。）が企業活動において重要な経営資源であり、情報資産に対する堅牢な情報セキュリティの確立が、安定した経営を実現するために不可欠であるとの認識に基づき、以下の方針を定め、これを遵守します。

（1）情報資産の管理機能を一層強化するため、体制を整備します。
（2）保有するあらゆる情報資産を、漏洩、改ざん、破壊等から保護するために、適切な教育、規程類の整備や技術的な対策を行います。
（3）情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守します。
（4）情報セキュリティに関わる事故が発生した場合には、事象ごとに適切かつ迅速に対処するとともに、再発防止に努めます。
（5）本ポリシーの取り組みについて、継続的な維持および改善に努めます。

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。