川崎重工グループ　情報セキュリティ方針

1．基本的な考え方

川崎重工グループは、情報セキュリティの確保を企業の社会的責任であると認識するとともに、事業継続に関わる重要な経営課題と考えています。当社グループが取り扱う情報を重要な資産として管理、保護するために以下のとおり情報セキュリティ方針を定め、事業活動において適正な運営を行います。

2．情報セキュリティ方針

（１）目的および適用範囲

川崎重工グループの役員および従業員が事業活動における情報セキュリティの重要性を正しく認識し、適切に行動できることを目的とし、当社グループのすべての事業活動をその対象とします。

（２）法令および契約履行義務の遵守

川崎重工グループは、情報セキュリティに関連する法令、規則、その他の規範および顧客との契約を遵守します。

（３）情報セキュリティ管理体制

川崎重工グループは、情報セキュリティに関して組織的かつ継続的な運用を実現するための管理体制を整備し、情報セキュリティの確保に努めます。

サイバーセキュリティ担当役員を最高責任者とする統括主幹部門（以下、「サイバーセキュリティ統括部門」）を本社内に設置し、カンパニーの主管部門と連携して情報セキュリティを強化していきます。また、本社リスク管理部門と連携し、情報セキュリティ施策の執行状況を経営会議で定期的に報告します。

（４）問題発生時の対応

川崎重工グループは、万一、情報セキュリティインシデントが発生した際には、迅速な対応により被害を最小限に抑え、その原因を究明し再発防止策を講じます。

サイバーセキュリティ統括部門には、当社グループに対するサイバー攻撃に対して検知、対応、復旧を担当するサイバーディフェンスセンターを置き、さらなる態勢強化に努めます。重大なセキュリティインシデントの発生時には、速やかにサイバーセキュリティ担当役員と共有します。

（５）教育・訓練の実施

川崎重工グループは、役員および従業員に対し、職務に応じて必要な情報セキュリティの教育・訓練を継続的に行い、情報セキュリティ意識の向上を図ります。

また、サイバーセキュリティ統括部門はカンパニー主管部門と連携し、社外からの擬似攻撃訓練を実施し、最新のサイバー脅威に対する検知・対処能力向上に努めます。

（６） 情報セキュリティ管理の継続的な改善

川崎重工グループは、サイバーセキュリティ戦略を策定し、計画的に施策展開するとともに、内部監査を実施することで管理・運用状況を定期的に点検評価し、継続的な改善を図ります。
また、専門機関のアセスメントを積極活用し、グローバル基準の達成と維持に努めます。
法務・コンプライアンス部門とも連携し、各国の情報管理に関する法規制に確実に対応し、グローバルビジネスの拡大に貢献する情報セキュリティ基盤を提供します。

以上