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、お客様をはじめとした取引先の情報や当社グループのブランド価値の保護、各々の事業活動に影響を与えない等の情報セキュリティ（機密性・完全性・可用性）の確保を企業の社会的責任であると認識すると共に、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の方針を定め、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） 目的及び適用範囲

川崎重工グループのすべての役員及び従業員が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） 法令及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、その他の規範及び取引先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、グローバル規模で複雑化する事業活動に対して、より一層適切な情報セキュリティ対策を実施し、当社グループ顧客はもとより社会に対する信頼、安全及び安心を守るため、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。

情報セキュリティを統括する担当役員を最高責任者とする統括部門を本社組織として設置し、各カンパニー、関連企業などの事業組織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、情報セキュリティ施策の執行状況を情報セキュリティ委員会を通して経営層に報告します。

（４） 教育・訓練の実施

川崎重工グループは、すべての役員及び従業員に対し、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、情報セキュリティに対する方針の定着や意識向上を推進します。また、統括部門は各カンパニー、関連企業などの事業組織の主管部門と連携し、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・対応・復旧能力の向上に努めます。

（５） 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、情報セキュリティ戦略を策定し、計画的に施策展開すると共に、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、必要な経営資源を確保・投入することで継続的な改善を行います。また、専門機関のアセスメントを積極活用すると共に、当社

事業に対する脅威情報を収集・評価・分析し、常に最適な対策を実施することで、情報セキュリティ管理の維持に努めます。
統括部門は、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体制を構築します。

（６） 問題発生時の対応

川崎重工グループは、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。
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・復旧を担当する専任部門を置き、さらなる体制強化に努めます。重大な情報セキュリティインシデントの発生時には、速やかに担当役員と情報を共有すると共に、取引先、関係省庁及び関係機関への速やかな報告を行います。

（７） サプライチェーン全体の情報セキュリティ確保

川崎重工グループは、社外のステークホルダー（顧客・パートナー・ベンダー・サプライヤ等）などを含めたサプライチェーン全体の情報セキュリティ対策状況の把握に努めるとともに、情報セキュリティリスクの低減のための適切な情報セキュリティ管理・対策を社外のステークホルダーと共に推進します。

制定　2021 年 9 月
改定　2021 年 11 月
改定　2022 年 8 月
改定　2025 年 7 月

以 上