

情報セキュリティ

基本的な考え方

川崎重工グループは、事業者や官公庁、一般消費者向け、防衛関連など幅広い分野で製品・サービスを提供しています。情報漏洩などが発生した場合、信用やブランド価値に影響を及ぼし、経営の根底をゆるがしかねないため、情報セキュリティの確保を重要な経営課題と捉えています。

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「川崎重工グループ情報セキュリティ方針」を定めています（2025年7月改定）。

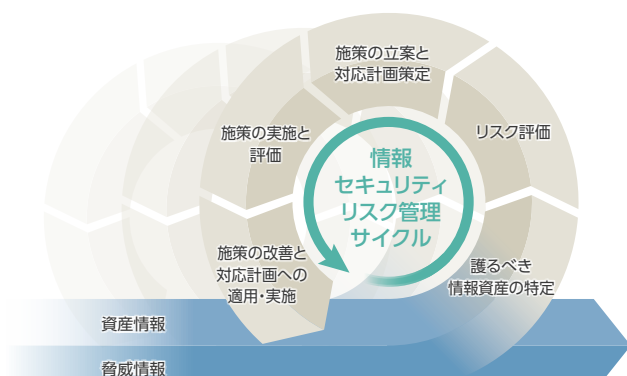
WEB 川崎重工グループ情報セキュリティ方針
https://www.khi.co.jp/sustainability/pdf/bcg_gr_info_seq_policy.pdf

情報セキュリティリスクの管理

情報セキュリティリスクを低減するため、守るべき情報資産を特定するとともに、高度化するサイバー脅威を的確に捉える目的で、独立行政法人情報処理推進機構（IPA）や一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）などの専門機関、セキュリティベンダー、アナリストから日々情報を収集しています。収集した情報から攻撃手法やシナリオを分析して脆弱性を特定し、情報資産が適切に保護されているかを定期的にアセスメントし、リスクを評価します。

また、内部監査等を通じて、リスク対策の実施状況や、方針・規程類に基づく管理・運用状況を定期的に点検・評価します。

情報セキュリティリスクの管理サイクル



NIST(米国立標準技術研究所)のサイバーセキュリティフレームワークを参考にリスク管理を実施

サプライチェーンの情報セキュリティ対策

サプライチェーンリスクに対応するため、リスクの識別、分析、優先順位付けおよび評価に関するプロセスを整備しています。

具体的には、「川崎重工グループお取引先様情報セキュリティガイドライン」（2022年度制定、2026年度改定）でお取引先に対して情報セキュリティ対策を促し、それぞれの特性に応じた対策を進められるよう取り組んでいます。また、サプライチェーンマネジメントの一環として国内外のお取引先を対象に実施しているアンケート調査において、2024年度より情報セキュリティに関する設問を設けました。

この調査等を通じて対策状況を確認し、リスクが高いと判断したお取引先にはさらなるセキュリティ対策の実装を要請するなど、調達関連部門とも連携してサプライチェーン全体におけるリスク低減に努めています。

WEB サプライチェーンのリスク評価
<https://www.khi.co.jp/sustainability/society/collabo.html#sr>

情報セキュリティ教育・訓練

当社グループは、情報セキュリティに関する法律やマナー、会社のルール、事故事例などについて、新入社員、一般従業員、幹部職員のそれぞれの立場に応じた教育を実施しています。また、定期的に標的型疑似攻撃メールによる訓練演習を実施しています。

2025年度は、情報セキュリティ教育を26,396名が受講したほか、標的型疑似攻撃メールによる訓練を16回、計8,157名に対して実施しました。

当社グループの取り組みの詳細は、「情報セキュリティ報告書」をご覧ください。

WEB 情報セキュリティ報告書
https://www.khi.co.jp/sustainability/library/infosec_report/2026/infosec_report_2026.pdf

