Kawasaki
Powering your potential

2026

川崎重工グループ
情報セキュリティ報告書

INFORMATION SECURITY REPORT 2026

川崎重工業株式会社

INDEX

「情報セキュリティ報告書2026」刊行にあたって

本報告書は経済産業省の「サイバーセキュリティ経営ガイドライン ver3.0」に基づき、ステークホルダーの皆様に当社グループの情報セキュリティに関する取り組みを適切に開示し、理解頂くことを目的に発行いたしました。

CISOメッセージ …… 2

当社グループの情報セキュリティ

情報セキュリティの管理体制 …… 3
- 情報セキュリティの基本方針 指示1
- 情報セキュリティの管理体制 指示2

情報セキュリティリスクの管理 …… 9
- 情報セキュリティリスクの認識 指示4 指示9
- 情報セキュリティリスクに対する取り組み 指示3 指示4 指示10

情報セキュリティの改善活動 指示6 …… 11

情報セキュリティにおけるインシデント対応体制と仕組み …… 12
- 情報セキュリティインシデント対応の体制 指示7
- 情報セキュリティインシデント対応の仕組み 指示5 指示7 指示8
- 認証取得 …… 15

情報セキュリティ啓蒙活動と教育・訓練 指示3 …… 16
- 啓蒙活動と教育・訓練
- 情報セキュリティ人財の育成
- 産学連携の取り組み

AI利活用の取り組み …… 18
- AI利活用の取り組み
- AI利活用の体制

当社製品に対する情報セキュリティ

製品セキュリティの管理体制 …… 20
- 製品セキュリティの基本方針 指示1
- 製品セキュリティの管理体制 指示2

製品セキュリティリスクの管理 …… 22
- 製品セキュリティリスクの認識 指示4
- 製品セキュリティリスクに対する取り組み 指示3 指示4 指示10

製品セキュリティにおける脆弱性対応 指示5 指示7 …… 22

■ 経済産業省「サイバーセキュリティ経営ガイドライン」Ver.3.0

【重要10項目】

- 指示1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定
- 指示2 サイバーセキュリティリスク管理体制の構築
- 指示3 サイバーセキュリティ対策のための資源（予算、人材等）確保
- 指示4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
- 指示5 サイバーセキュリティリスクに効果的に対応する仕組みの構築
- 指示6 PDCAサイクルによるサイバーセキュリティ対策の継続的改善
- 指示7 インシデント発生時の緊急対応体制の整備
- 指示8 インシデントによる被害に備えた事業継続・復旧体制の整備
- 指示9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策
- 指示10 サイバーセキュリティに関する情報の収集、共有及び開示の促進

■ 対象期間　2026年3月31日までの活動を報告対象としております。

Message from the CISO

CISOメッセージ

川崎重工グループは2026年に創業130周年を迎えました。創業以来、陸、海、空の輸送機器からエネルギー、プラント、産業機械といった幅広い分野において、ものづくりを通じて技術・知見を磨き、世界中のお客様の多様なニーズに応える製品・サービスを時代の変化に合わせて提供してきました。さらに2030年に目指す姿として「グループビジョン2030 『つぎの社会へ、信頼のこたえを～Trustworthy Solutions for the Future～』」を制定し、今後の社会課題に対して、その解決を実現する革新的なソリューションを提供し、グローバルに貢献することを宣言しています。そのために事業のスタイルとそれを支えるプロセスを大きく変革していくための活動「Kawasaki-DX(Digital Transformation)」を推進中です。業務プロセスのデジタル化やリモートワークなどの新たな働き方の導入をはじめ、クラウドの強力な計算能力の利用や驚くべき速度で進化する生成AIの活用にも積極的に取り組んでおり、社内の多様な業務における生産性向上に効果が得られはじめています。

その一方で業務のデジタル化の進展により、サイバー攻撃によるリスクが急激に増加しています。個人情報、営業秘密等の重要情報の漏えいや事業用システムの停止といった事態を未然に防ぐ活動がこれまで以上に重要になっています。さらに生成AIの進化は偽情報の拡散やなりすまし攻撃の高度化など新たなリスクを生んでおり、開発・利用の両面において対応策が求められています。

このような状況を踏まえ、当社グループではNIST（米国国立標準技術研究所）の「Cyber Security Framework Ver2.0」や経済産業省の「サイバーセキュリティ経営ガイドライン Ver3.0」などを参考に、グループ全体の情報セキュリティ態勢を強化するための仕組みを構築しています。情報セキュリティ活動を統括する専門組織を立ち上げ、サイバー攻撃に対する24時間×365日体制での監視に加え、仮に侵害が発生しても影響を最小化すべく迅速に対応できる体制を運用しています。さらに、全ての役職員に対する情報セキュリティ教育、訓練を実施し、セキュリティに関する知識と意識のレベルアップを継続的に進めていくと共に、当社事業を支えるサプライヤのサイバーセキュリティ対策支援にも取り組んでいきます。

デジタル化が進む製品領域においては、製品セキュリティ体制の確立にも力を入れて取り組んでいます。企画、設計段階からサイバーセキュリティリスクを考慮した脅威分析や攻撃対策を行い、安全で高品質な製品開発を実現すると共に、製品運用段階においても継続的な脆弱性対応を実施する体制構築を進めています。

当社グループは社会課題を解決する新たなソリューションを創出すると共に、安全・安心な社会の実現に向けた取り組みの一つとして情報セキュリティの強化を積極的に推進していきます。

なかたに ひろし
中谷 浩

川崎重工業株式会社
代表取締役副社長執行役員
社長補佐、技術・生産・品質保証・調達・DX戦略担当

Information security in the Kawasaki Group

当社グループの情報セキュリティ

情報セキュリティの管理体制

情報セキュリティの基本方針 指示1

当社グループは社会インフラ事業向けから一般消費者向けといった幅広い分野で製品・サービスを提供しており、情報漏洩などが発生した場合は信用やブランド価値にも影響を及ぼすなど経営の根底をゆるがしかねないことから、情報セキュリティの（機密性・完全性・可用性）確保が重要な経営課題であると認識しています。そうした経営リスクからビジネスを守るために、お客様やお取引先に関わる情報や会社の事業に関わる情報などの重要な情報資産を適切に管理、保護し、社会的責任として情報セキュリティを確保すると共に、その維持と向上に取り組んでいます。

情報セキュリティへの取り組みとしては、次の4つの観点から取り組むことを基本的な考えとしており、この基本的な考え方を基に「川崎重工グループ情報セキュリティ方針」を定めているほか、NIST CSF*などの世界標準のフレームワークに倣った情報セキュリティに関する各種方針及びルールを定めています。

① グループ全体の連携を強化する体制構築
② 重要な情報などの情報資産の把握と管理
③ サイバー攻撃に対する識別・防御・検知・対応・復旧を実現する適切な施策の計画と展開
④ 全役職員の情報セキュリティ知識の習得と意識の向上

※NIST CSF（Cybersecurity Framework）：米国国立標準技術研究所が発行する重要インフラのサイバーセキュリティを向上させるためのフレームワーク

川崎重工グループ 情報セキュリティ方針

■ 法令及び契約履行義務の遵守

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する。

■ 情報セキュリティ管理体制

複雑化する事業活動に対して、適切な情報セキュリティ対策を実施し、お客様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る。

■ 教育・訓練の実施

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する。また、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る。

■ 情報セキュリティ管理の継続的な改善

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う。また、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る。併せて、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する。

■ 問題発生時の対応

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、原因を究明し再発防止策を講じる。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設置し、体制強化に努める。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。同時に取引先、関係省庁及び関係機関への速やかな報告を行う。

■ サプライチェーン全体の情報セキュリティ確保

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する。

川崎重工グループ 情報セキュリティ方針体系

川崎重工グループ情報セキュリティ方針

管理方針群

情報セキュリティ統括方針	情報セキュリティに関する統括を行うための考え方/取り組みを示している。
情報セキュリティ管理方針	情報セキュリティを維持する活動に関する管理を行うための考え方/取り組みを示している。

個別方針群

システム開発ライフサイクルセキュリティ方針	情報システムのライフサイクルプロセスを定める考え方/取り組みを示している。
アクセス管理方針	情報セキュリティを確保するためのアクセス管理の考え方/取り組みを示している。
通信ネットワーク・情報インフラセキュリティ方針	情報セキュリティの確保にあたり、整備すべき環境や対策を行うための考え方/取り組みを示している。
クラウドセキュリティ方針	クラウドサービスを安全に利用し、万が一の時には被害、事業活動への影響を最小限に抑えるための考え方/取り組みを示している。
エンドポイントセキュリティ方針	エンドポイントの情報セキュリティを確保するための保守、保護、情報セキュリティインシデントの検知と対応の管理と運用に関する考え方/取り組みを示している。
データ保護方針	重要なデータを識別し、保護するための管理と運用に関する考え方/取り組みを示している。
生産システムセキュリティ方針	生産システムをサイバー脅威から保護し、人命・環境を守り、事業を継続するための仕組みの構築と管理・運用に関する考え方/取り組みを示している。
サイバーディフェンス統制方針	情報資産を保護し、サイバーセキュリティインシデント発生時に事業への影響を最小限にとどめるためのサイバーディフェンス統制の考え方/取り組みを示している。

上記方針に基づき川崎重工業/関係会社にて各事業活動に応じた社則を整備

全従業員参加のサイバーセキュリティ 7つの行動指針

「川崎重工グループ情報セキュリティ方針」に基づき、全従業員に向けてのサイバーセキュリティに関する道しるべとして7つの行動指針をまとめています。

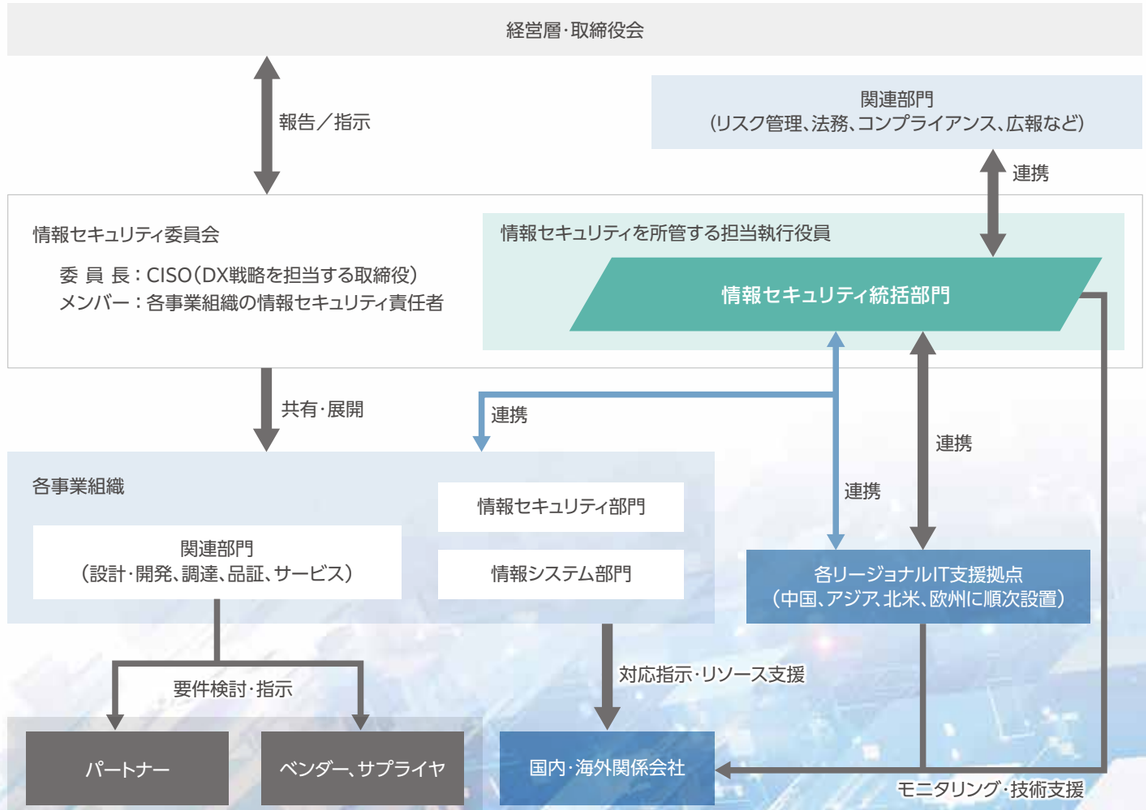
情報セキュリティの管理体制 指示2

DX戦略を担当する取締役がCISOとしての役割を担っており、CISOを委員長として各事業組織の情報セキュリティ責任者が参画する情報セキュリティ委員会を組織し、情報セキュリティに関する方針、計画、情報セキュリティリスクに対する各種施策などについて各事業部門、関係会社、関連組織に共有・展開をおこなっています。

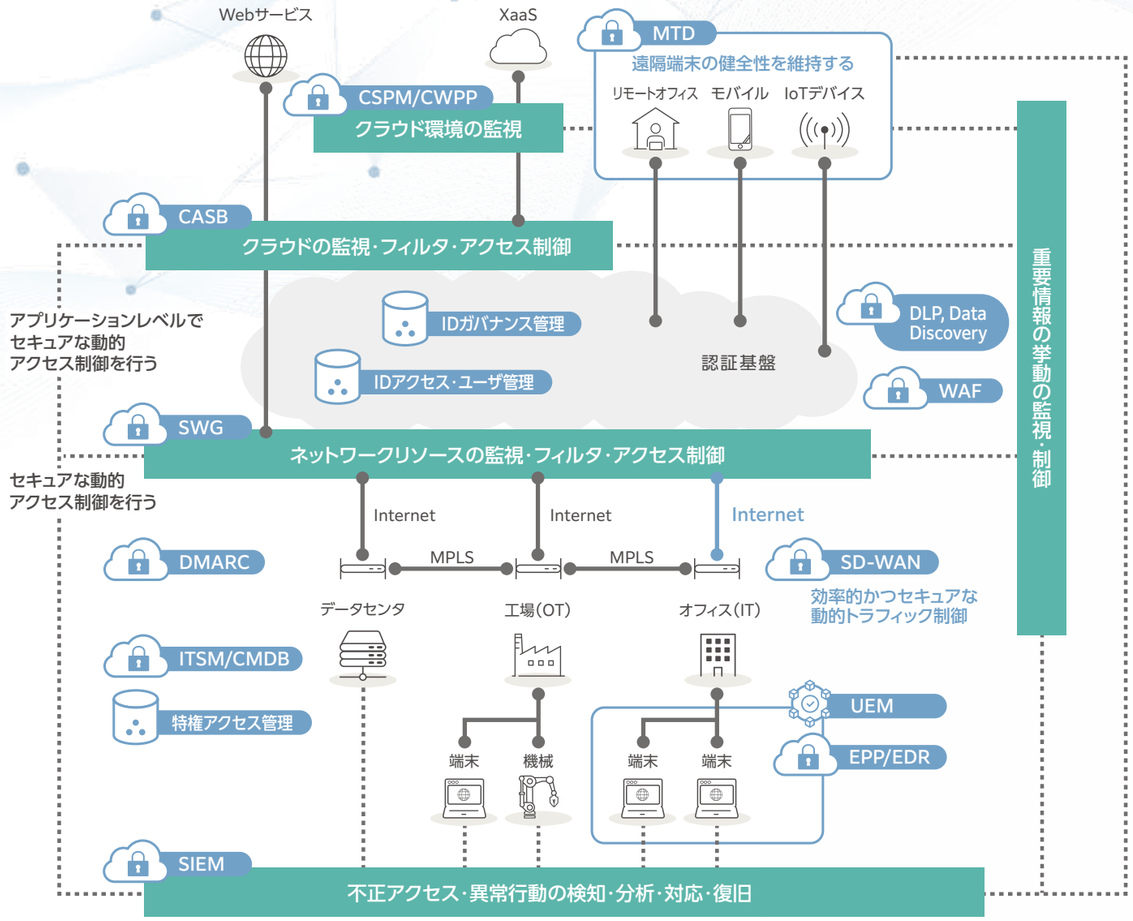
また、情報セキュリティを所管する担当執行役員のもとに、情報セキュリティに関する戦略の策定、情報セキュリティリスクの特定、施策の企画・立案・実施、監査、情報セキュリティインシデントの検知・対応・復旧を担う、情報セキュリティ統括部門を設置しています。

併せて、情報セキュリティ委員会からの指示に基づいて、情報セキュリティ統括部門を中心に各事業組織、関係会社、関連部門が互いに連携し、時々刻々と変化する情報セキュリティリスクに対して「技術対策」「教育・訓練」「ルール」の3つの視点から情報セキュリティの確保・維持・向上を体系的に整備し推進しています。

情報セキュリティの管理体制



情報セキュリティのテクノロジー全体像

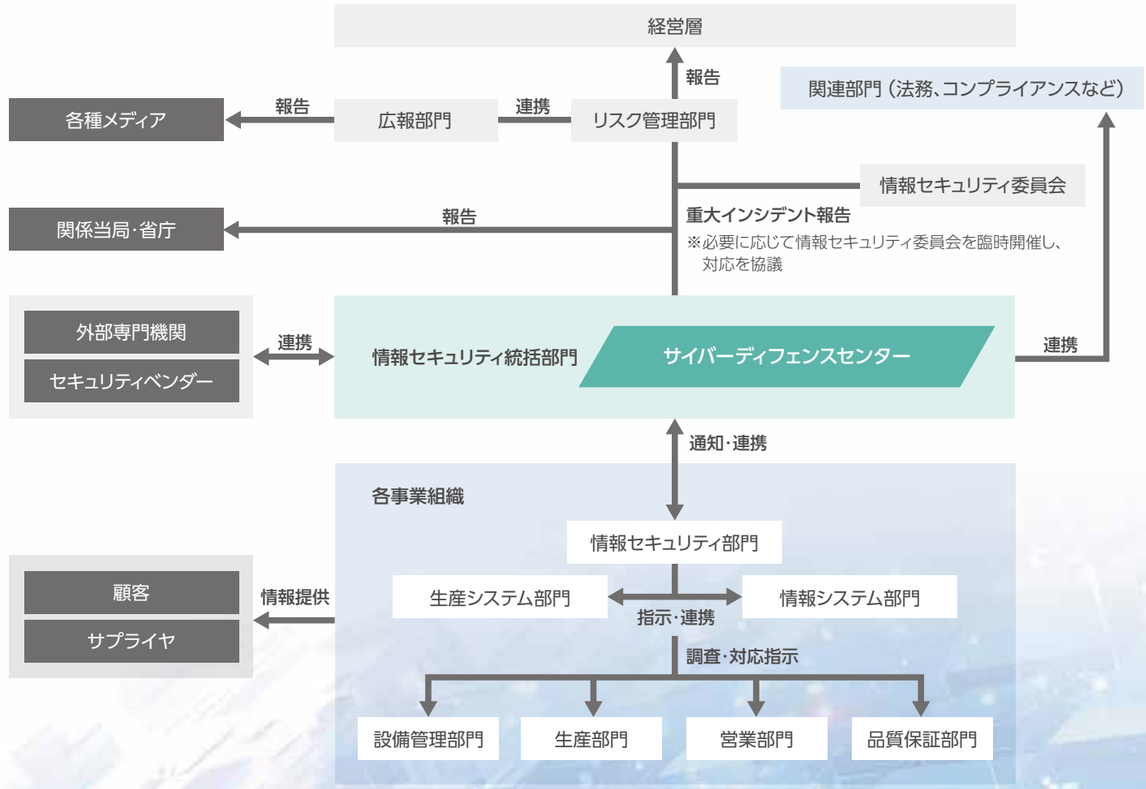


生産システムセキュリティの管理体制

近年、様々な業務システムと生産システムを通信ネットワークで接続し、生産性向上を目的としてデータの蓄積や活用を行う取り組みが進んでいます。これによりサプライチェーン上の一企業へのサイバー攻撃による侵害から連鎖的に影響が広がり、生産停止に追い込まれる事例が多発するなど、工場の生産システムに対するサイバー脅威が大きな社会課題となっています。

このような状況を鑑みて当社グループでは、各事業組織と情報セキュリティ統括部門が連携する体制を強化するなど管理体制を整備し、生産現場・設備の安全確保や環境への影響の最小化はもとより、生産活動の安定化を目的として工場の稼働を支える生産システムやインフラのセキュリティ強化に取り組んでいます。

生産システムセキュリティの管理体制



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の認識 指示4 指示9

当社グループの事業活動においては、お客様やお取引先の情報、ならびに当社グループの機密情報、知的財産、個人情報、事業を支える情報システム・生産システムを重要な情報資産として取り扱っています。そしてこれらの情報資産はサイバー攻撃をはじめとするあらゆる脅威に晒されています。このことから情報セキュリティに係るリスクは当社の事業活動を支える基盤における重要課題の一つと捉えており、日々高度化するサイバー脅威に対応し、事業活動への影響を最小限に抑えるために、情報セキュリティリスクを低減させる取り組みを当社グループ内に根付かせていくことが重要であると考えています。
また、サプライチェーンリスクに対応するにあたり、リスクの識別、分析、優先順位付け及び評価に関するプロセスを整備しています。

具体的には、2022年度に制定した「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」を2026年2月に改訂し、お取引先に対して情報セキュリティ対策への取り組みを促し、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。お取引先の情報セキュリティ対策を確認し、リスク状況を当社調達関連部門と共有した上で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、サプライチェーン全体におけるリスクの低減に取り組んでいます。

情報セキュリティリスクに対する取り組み 指示3 指示4 指示10

情報セキュリティリスクを低減させる取り組みとして、当社グループとして守るべき情報資産を特定すると共に、高度化するサイバー脅威を的確に捉えるため、情報処理推進機構（IPA）やJPCERT/CCなどの専門機関、セキュリティベンダー、セキュリティアナリストなどから発信された脅威情報を日々収集しています。収集した脅威情報を基に想定される攻撃者、攻撃手法、攻撃シナリオなどの分析、脆弱性の特定を行っています。その上で分析・特定した脅威や脆弱性から適切に情報資産が護られているかについて定期的にアセスメントを実施し、リスクの評価を行います。評価の結果に基づいて、必要となる情報セキュリティ施策を立案し、施策の実施に必要となる人財・予算など、資源の確保を含めたリスク対応計画を策定し実施します。情報セキュリティ施策の効果については、NIST CSFなどの各種フレームワークを参考に、情報セキュリティ管理の成熟度などを測定し、取り組みや運用管理の定着度合いを評価します。また万が一、当社グループの国内・海外拠点において情報セキュリティインシデントが発生した場合に備えてサイバー保険に加入し、そのサービスを活用することで業務への被害を最小限に食い止める対策を実施しています。

サイバー脅威インテリジェンス

専門機関やセキュリティベンダー、セキュリティアナリストなどから発信された脅威情報を継続的に収集・比較・分析し、最新のサイバー攻撃動向や技術トレンドの把握に努めています。これらの情報をもとに想定される攻撃者、攻撃手法、攻撃シナリオなどを分析すると共に、当社グループに影響を及ぼし得る脆弱性の把握を行うことで戦略・施策・運用それぞれの視点での活用を進めています。

戦略的な活用

当社各事業に対するサイバー攻撃の傾向やサイバーセキュリティリスクに基づいた情報を経営層に提供することにより、当社グループ全体の情報セキュリティ対策の意思決定を支えます。

施策に対する活用

攻撃者の具体的な手口、攻撃傾向の分析から当社及び関連会社に対するASM※やレッドチームテストの内容、情報報漏洩対策などの施策の策定と優先順位の決定に活用し、無駄のない効率的な施策適用を支えます。

運用的な活用

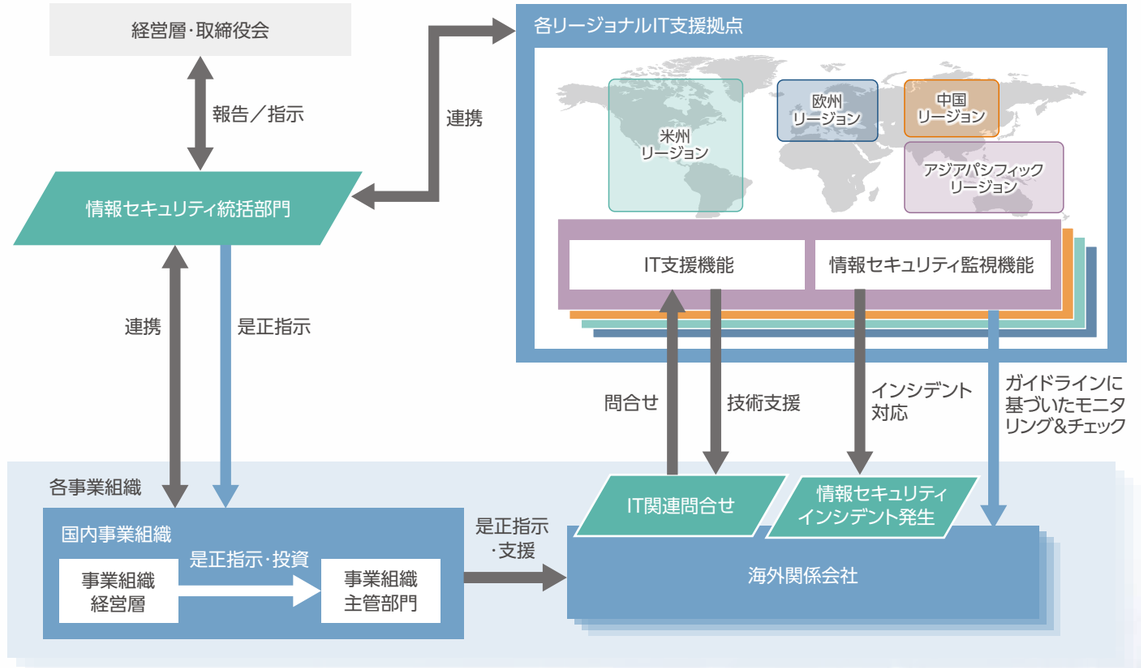
情報セキュリティインシデント発生時に「誰が・なぜ・どのように」当社を狙ったものかの特定に活用を行い、原因や影響範囲を迅速に見極め、取るべき対応や投資判断を誤らないための判断材料として活用し、被害の最小化と早期収束を支えます。

※ASM（Attack Surface Management）：企業が保有する全情報資産の内、外部からアクセス可能な情報資産を特定し、攻撃者の視点で継続的に調査・監視することにより脆弱性を評価・管理するサイバーセキュリティの概念。

関係会社に対する取り組み

国内外の関係会社に対して当社グループ統一のツールを導入することでサイバー攻撃を常時監視し、検知するための仕組みを整えています。加えて、国内の関係会社においては、機密情報やお客様の情報などの重要情報は適切に暗号化し、アクセス制御を厳格にする取り組みを進めています。また、海外の関係会社においては、地域固有の特性を考慮してリージョンごとの支援拠点を設置し、情報セキュリティ及びIT全般の支援体制を整備しています。これまでに、中国とアジアパシフィックリージョンにおいて支援拠点を設置しており、情報セキュリティガイドラインの整備と共に、これに基づいた定期的なセキュリティレベルのチェックを実施し、是正活動ならびにセキュリティ施策の展開に取り組んでいます。サイバー脅威が高度化する中、情報セキュリティを保つための取り組みを、当社グループ全体で進めています。

海外関係会社の情報セキュリティ強化体制



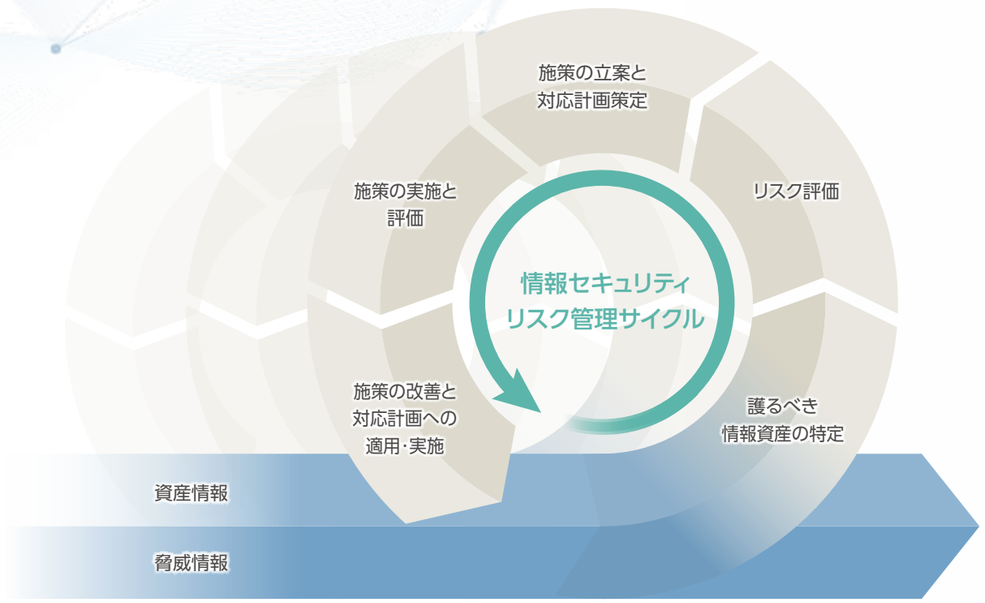
生産システムに対する取り組み

情報システムとは異なり、生産設備のライフサイクルは長いものが多く、また情報システムに適用するような施策の適用が難しいものも多いといった生産システムに関する特有の課題があるため、生産設備や工場内の通信ネットワーク、外部と通信するネットワークなどへのアクセスを必要最低限に制御し、生産システムにおける異常な通信の発生を検知するといった対応が必要になります。
当社グループでは、生産システムにおけるサイバー脅威を明確にするために定期的なリスク評価を実施し、その結果を踏まえて具備すべきセキュリティ機能について調査・検証・選定し、より安全な生産システムセキュリティ基盤の構築を進めるとともに、その基盤上の通信を監視し、異常な通信の発生を検知することで悪意のあるアクセスの発生やサイバー攻撃の予兆を監視する運用を行っています。
これに加えて、生産システム上の情報セキュリティリスクを低減する取り組みとして、年々高度化するサイバー脅威の動向を的確に捉える目的で専門機関などから発信されるサイバー脅威情報を収集・分析し、当社事業に影響のある情報セキュリティリスクを特定した上で、リスク評価にフィードバックしています。

情報セキュリティの改善活動 指示6

評価の結果に基づいて、サイバー脅威の監視強化、脆弱性の対策、管理運用ルールの改善、トレーニングと教育などをリスク対応計画に盛り込むなど、継続的にPDCAサイクルを回すことでリスクが顕在化する前に先手で抑え込むための改善活動を行います。

情報セキュリティリスクの管理サイクル



NIST（米国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

情報セキュリティにおけるインシデント対応体制と仕組み

情報セキュリティインシデント対応の体制 指示7

高度化、深刻化しているサイバー脅威からお客様やお取引先に関わる情報や当社グループの情報資産を守るため、サイバー脅威の状況を捉え、インシデントに対して迅速に対応するために必要とな る体制を整備しています。

情報セキュリティ統括部門内にサイバーディフェンスセンター(CSIRT※)を設置しており、右記の3つの機能から構成されています。

インシデントが発生した場合、迅速な対応が不可欠です。そのために、経営層、リスク管理部門や広報部門、各事業組織や役職員などの関係者と連携を図りながら、インシデントに対処するプロセスを整備し、定期的な訓練を行うことで、インシデントの発生に備えています。

■ インテリジェンス機能

サイバー脅威インテリジェンスの活用により、インシデント対応を支援します。

■ 検知・分析機能

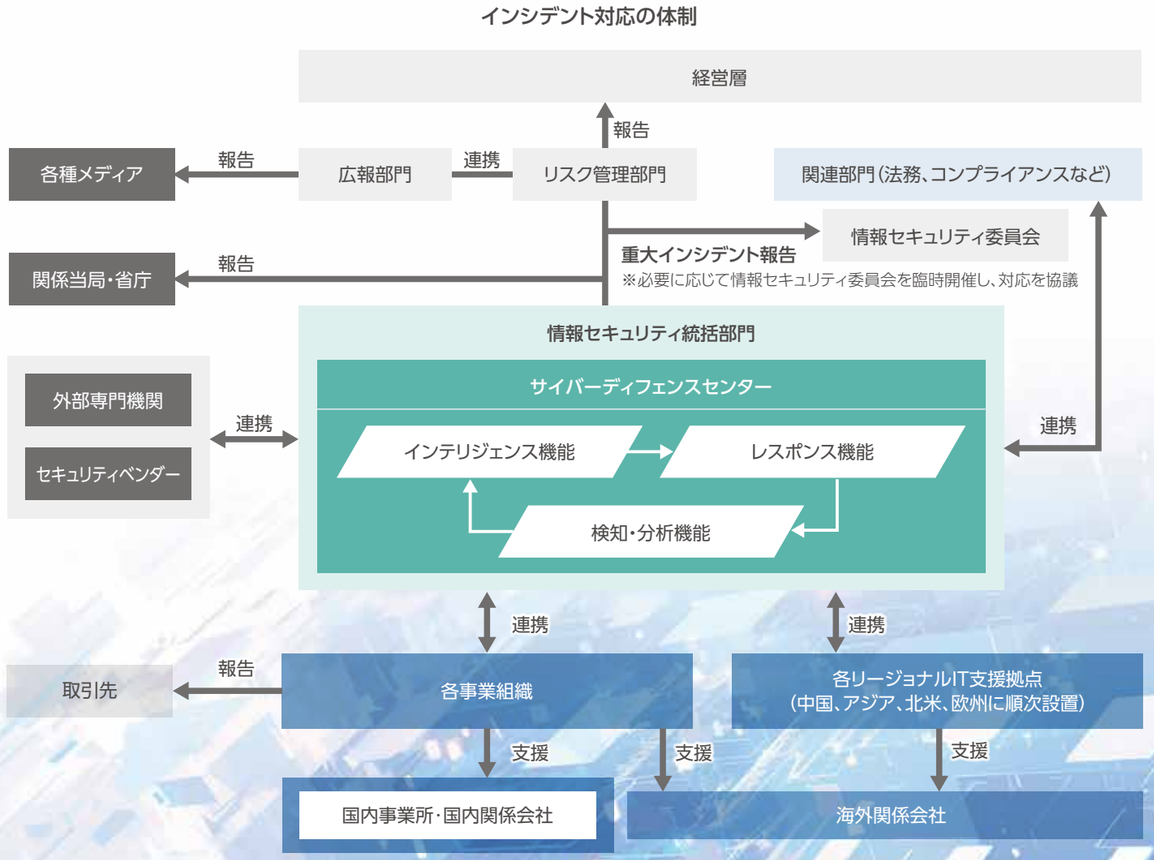
サイバー攻撃を常に監視し、異常を検知し、分析します。

■ レスポンス機能

攻撃を検知後、直ちに関係者と連携し迅速に対策を講じて被害を最小限に抑えます。

※CSIRT（Computer Security Incident Response Team）：企業の情報システムや通信ネットワークでウイルス感染や不正アクセス、サービス拒否攻撃（DoS攻撃）などセキュリティ上の脅威となる現象や行為（インシデント）が発生した際に、いち早く発生を検知し、組織内の対応窓口となって被害の拡大防止や関連情報の収集・告知、再発防止策の策定などの活動を行う。

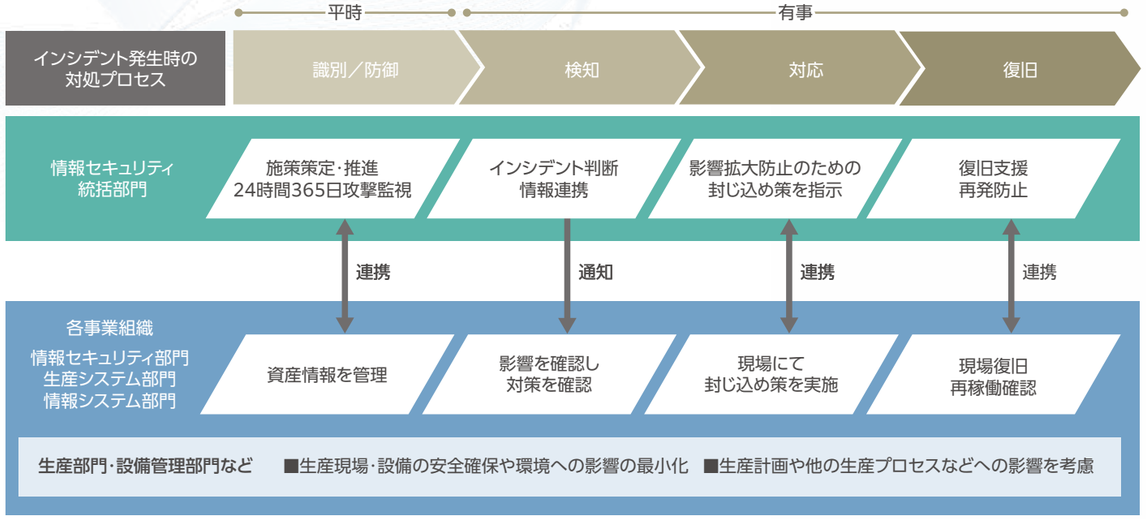
インシデント対応の体制



生産システムに対するインシデント対応の体制

生産システムは、仕組みや機能、規模などが異なる様々な設備やプロセスが連携して動作します。そのため情報セキュリティインシデントが発生した際には、生産関連部門と連携して対応することが重要です。当社グループでは、人命を最優先に生産現場・設備の安全確保や環境負荷の最小化はもとより、他の生産プロセスへの影響も考慮した対応を迅速に行う体制が必要となります。そのために各事業組織の生産部門や設備管理部門とも連携して適切に対応を行う体制とプロセスの整備を進めています。

生産システムに対するインシデント対応の体制とプロセス



情報セキュリティインシデント対応の仕組み

指示5 指示7 指示8

インシデント検知、分析

役職員が使用する情報システムや個人用の端末、生産システムなどにおいて不審な事態や不審なメールに気が付いた際には、速やかに定められた報告ルートに基づいてサイバーディフェンスセンターに状況について報告することとしています。加えてセキュリティアラートや各種ログを集中監視する基盤を確立すると共に、情報資産の構成情報を一元管理することで、侵害を受けた範囲を的確に把握します。この管理体制により、通信ネットワーク、情報機器、アプリケーション、データなどに対する不正アクセスや異常な活動を24時間365日の体制で監視しています。そこでインシデントが検知された場合は、詳細調査を行い、侵害を受けたシステムやデータを特定し、事業活動への影響を迅速かつ適切に評価しています。その上で、定められた報告・連携ルートに基づき、関係者と情報を共有・連携する仕組みを構築しています。

監視については、以下の4つの領域においてそれぞれ複数の監視システムで実施しています。

Endpoint
（PC、サーバ）

クラウド環境
（サーバ、ストレージ）

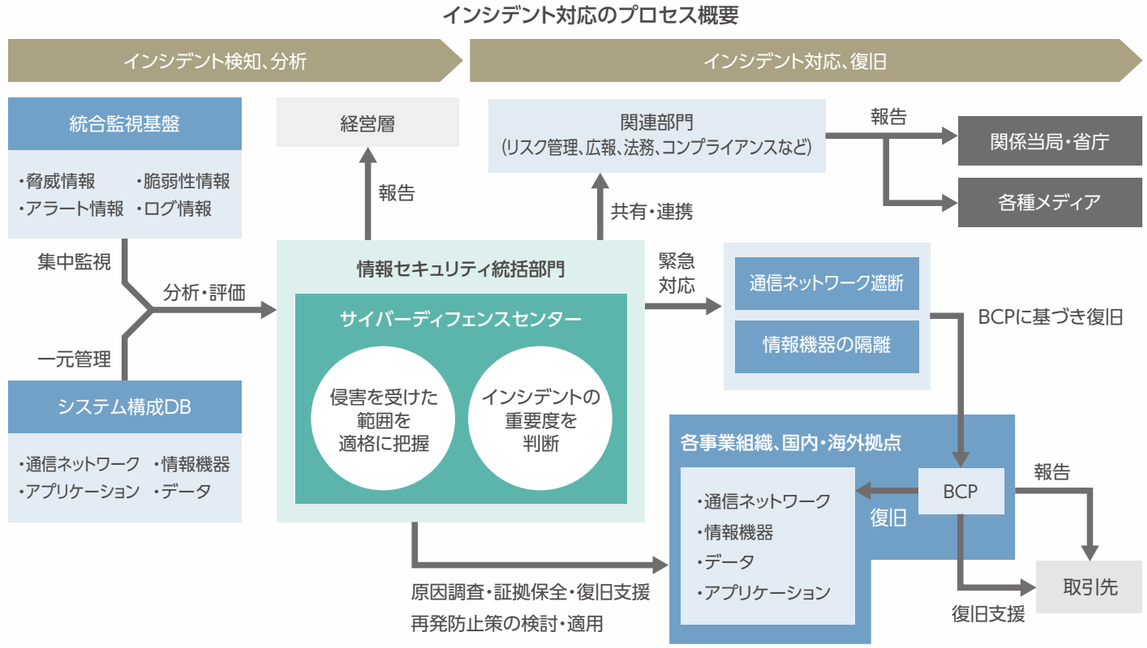
インターネット境界
（DMZ、Webアクセス、メール）

統合監視
（アラートとログの相関分析）

インシデント対応、復旧

分析した結果、侵害されていると判断されたインシデントに対しては、インシデントの重要度を判断し、更なる侵害を阻止するために必要となる対応として、通信ネットワークの遮断、情報機器の隔離などを実施します。また、事業活動への影響や侵害範囲などを踏まえて関係者と協力し、侵害を受けた原因の調査、証拠保全を実施すると共に、事業活動を平常稼働に戻すための復旧作業を実施します。重大なインシデントの発生時には、速やかに定められたルートに従い経営層に報告すると共に、関連部門で情報を共有・連携し、お取引先や関係省庁及び関係機関に速やかな報告を行います。

インシデント対応のプロセス概要



再発防止策の検討

発生したインシデントからは同じインシデントが再び発生しないよう、情報セキュリティに関わるルールの見直しやインシデント対応手順の改善、関係者間の連携方法の再確認、情報システム、通信ネットワークの設定変更など必要な強化策を実施し、関係者全体で学びを得ることで情報セキュリティに関する仕組みの改善に繋げています。

インシデント対応訓練

あらゆるサイバー攻撃や不正アクセスに備え、関連部門の担当者も含めて定期的な訓練を実施し、役割や対応プロセス、情報連携の方法を確認しています。具体的な訓練内容としては、机上での対応手順確認や実機上での実際の攻撃を模擬した侵入テスト（レッドチームテスト）を通じて、迅速な対応と連携強化を図っています。また、訓練を通して蓄積したノウハウはインシデント対応の手順書へ反映することで、インシデント検知・分析・対応・復旧へフィードバックしています。

生産システムに対する仕組み

生産システムセキュリティ基盤上の通信を監視し、悪意のあるアクセスや情報セキュリティインシデントが疑われる通信の発生を検知した場合には、情報セキュリティ統括部門と各事業組織が協力し、侵害の内容と範囲を迅速に把握します。稼働中の生産設備を急には止められないため、生産システム部門と連携して対応を行い、生産現場の安全を確保したうえで生産設備を停止します。その上で環境に配慮しつつ当社グループの事業に対する被害を最小限に抑え、速やかな業務の復旧に努めます。

認証取得

当社グループでは、情報セキュリティに関する第三者評価・認証取得を推進しており、情報セキュリティに関する認証を取得した組織は以下のとおりです。

ISMS(ISO/IEC27001)※1 認証取得組織

川崎重工業株式会社
　社長直轄プロジェクト本部　事業企画総括部　PNT推進部
ベニックソリューション株式会社
　デジタル基盤本部　基盤サービス設計部・運用サービス部

※1 ISMS(ISO27001)(Information Security Management System):
組織内での情報の取り扱いについて、機密性、完全性、可用性を一定の水準で確保するための仕組みのこと。組織の管理の一環として、取り扱う情報の種類などから確保すべきセキュリティの水準を定め、計画や規約を整備して情報システムの運用などに反映させる取り組みの総体を指す。

産業用サイバーセキュリティ国際標準規格(IEC62443-4-1※2)認証取得組織

川崎重工業株式会社
　精密機械・ロボットカンパニー ロボットディビジョン

※2 ISC62443-4-1:産業用オートメーション及び制御システム(IACS:
Industrial Automation and Control System)で使用されるセキュアな制御機器を開発するためのプロセス・組織要件をを規定したもの。

プライバシーマーク付与認定取得企業

ベニックソリューション株式会社
株式会社ケイキャリアパートナーズ

IACS統一規格「船上のシステム及び機器のサイバーレジリエンス」(IACS UR E27※3)認証取得製品

川崎重工業株式会社
SOPass船上システム(K24SP-US1)
　エネルギーソリューション&マリンカンパニー
　船舶海洋ディビジョン

※3 IACS UR E27:2022年4月にIACS (International Association of Classification Societies:国際船級協会連合)によりサイバーインシデントの発生を低減し影響を軽減する機能(サイバーレジリエンス)を最低限確保した船舶を実現することを目的に発行された、サイバーセキュリティに関する2つのUR(Unified Requirement:統一規則)の内の1つで、UR E27は、船上のシステム及び機器が対象として定められいる。

情報セキュリティ啓蒙活動と教育・訓練 指示3

啓蒙活動と教育・訓練

法律、会社のルール、事故事例などを踏まえた情報セキュリティに関する教育を、入社する社員、一般社員、幹部職員、経営層のそれぞれの立場に合わせて定期的に実施しています。併せて、日常の業務でサイバー攻撃やネット犯罪などの被害に合わないよう、疑似標的型攻撃メールによる訓練を実施しています。2025年度においては、情報セキュリティ教育を26,396名、疑似標的型攻撃メールによる訓練を8,157名に対して実施しています。

また、当社グループ報に情報セキュリティに関するコンテンツを掲載し、グループ全体としてのセキュリティ意識の向上に努めています。

職務別啓蒙活動の取り組み

対象者	啓蒙活動の目標	具体的な取り組み
経営層	社員全員に対する適切な危機意識の醸成、徹底した管理を推進できること	経営層のためのエグゼクティブ向け教育
幹部職員	自社の情報セキュリティリスクを正しく把握し、自ら改善の実行指導がはかれること	最新のセキュリティトレンドなどを踏まえた管理者向け教育
一般社員	日常業務で遭遇するリスクや脅威に対し、適切な行動、対応をとることができること	日常常務などの留意事項を踏まえた一般社員向け情報セキュリティ教育 標的型攻撃メールによる訓練演習
入社する社員	情報セキュリティ管理に対する基礎知識の習得すること	新たに受け入れた新卒採用者、中途採用者、派遣などへの新入社員研修

川崎重工グループ報「かわさき」掲載コンテンツ

情報セキュリティ人財の育成

サイバー脅威から当社グループのビジネスを護り、事業活動を継続していくためには、情報セキュリティに関する高い専門知識を持った人財が必要不可欠であると認識し、さまざまな活動に取り組んでいます。情報処理推進機構（IPA）や外部のセキュリティ専門企業に人財を派遣し、業界の最前線で経験を積むことや、各企業の専門家との交流を通じて、最新の動向や技術などを学んでいます。そのほか外部のセキュリティ専門企業による定期的な教育を実施しており、セキュリティリスクに対処する能力を高める取り組みを行っています。

また、セキュリティ人財の育成だけでなく、人財の中長期採用計画を策定し、それに基づき異動や新卒、中途採用を実施しています。新卒採用においては、インターンシップや次項の産学連携を通じて実際の現場を体験する機会を提供するなど、人財の確保に積極的に取り組んでいます。

産学連携の取り組み

情報セキュリティの確保は、事業活動において必須の要素であり、特に製品に関する企業機密や顧客・取引先の情報などの重要な情報を取扱う産業界においては企業インフラを形成する上で欠かせないものと言えますが、一方で情報セキュリティの中でもサイバーセキュリティ分野の人財確保が難しいという課題があります。
当社グループではこの課題に対する取り組みの一つとして、サイバーセキュリティ分野における学術機関や研究機関の活動やその成果が国内外にも高く評価されていることに着目し、産学連携という形で共同研究や出張講義などの交流を通じて最新の技術や知識を学ぶことで人財の育成を行っています。

また独立行政法人国立高等専門学校機構が実施しているサイバーセキュリティ人材育成事業の活動に参画し企業における情報セキュリティ対策に関する講義を行うなど、より実践的な当社グループのサイバーセキュリティ対応の現場や、取り組みに触れる機会を学生や研究者に提供することで、将来のサイバーセキュリティ専門家の育成にも貢献しています。
このように双方にメリットのある産学連携を通して、当社グループではより高度な情報セキュリティの確保と将来のサイバーセキュリティ分野の人財育成に取り組んでいます。

AI利活用の取り組み

AI利活用の取り組み

当社グループは、革新的なソリューションの開発やDXによる社内改革を実現するため、AI関連技術の研究開発に取り組んでいます。一方で、急速に高度化するAIの不適切な使用により、人権やプライバシーの侵害、差別の助長といった倫理上の課題や、自律化した工業製品に対する安全性への懸念が社会課題となっています。
これらの状況を踏まえて当社では、一連の取り組みを統括する組織を組成し、AI関連技術の開発及び利活用を拡大していく上で遵守すべき「川崎重工グループAI倫理方針」を定めるとともに、その内容を具体的な行動に落とし込んだガイドラインを策定し、定着を図っています。

川崎重工グループ AI倫理方針

■ 人間中心のAI活用

AIが人間と社会に奉仕し、人間の尊厳と自律性を尊重し、社会と地球環境の未来に貢献するため、適切に管理・監督できる形で機能するツールとして活用するように努める。

■ 安全性・堅牢性・セキュリティの確保

AIが利用者に身体的・精神的な危害を加えないよう安全性を確保するように努める。また、AIに著しく誤った判断をさせないように堅牢性を確保し、さらにサイバー攻撃によってAIの機能が停止したり、振る舞いに意図しない変更が生じたりすることのないようにセキュリティの確保に努める。

■ 法令などの遵守

コンプライアンスを重視し、関連する法令、社内規則に従い、プライバシー・個人情報や知的財産の保護に努めると共に、AI活用に関する監査などを通してガバナンスの強化に努める。

■ 透明性の追求

AIが判断した理由を追跡・説明可能にするように努めると共に、技術的かつ社会的合理性が認められる範囲でステークホルダーへ情報開示するように努める。

■ 多様性・公平性の尊重

AI活用において、常に公平性を意識すると共に不当な差別が発生しないように多様性を尊重し、差別的影響や不当なバイアスを回避するように努める。

■ イノベーションの促進と持続可能な社会の実現

AIの活用を通して、社会全体のイノベーションの促進に貢献し、持続可能な社会を実現するように努める。

■ AIに関する教育

AI活用に関する責任を果たすために、職務に応じて必要な教育を継続的に行い、AI倫理方針の定着及び意識の向上に努める。

AI利活用の体制

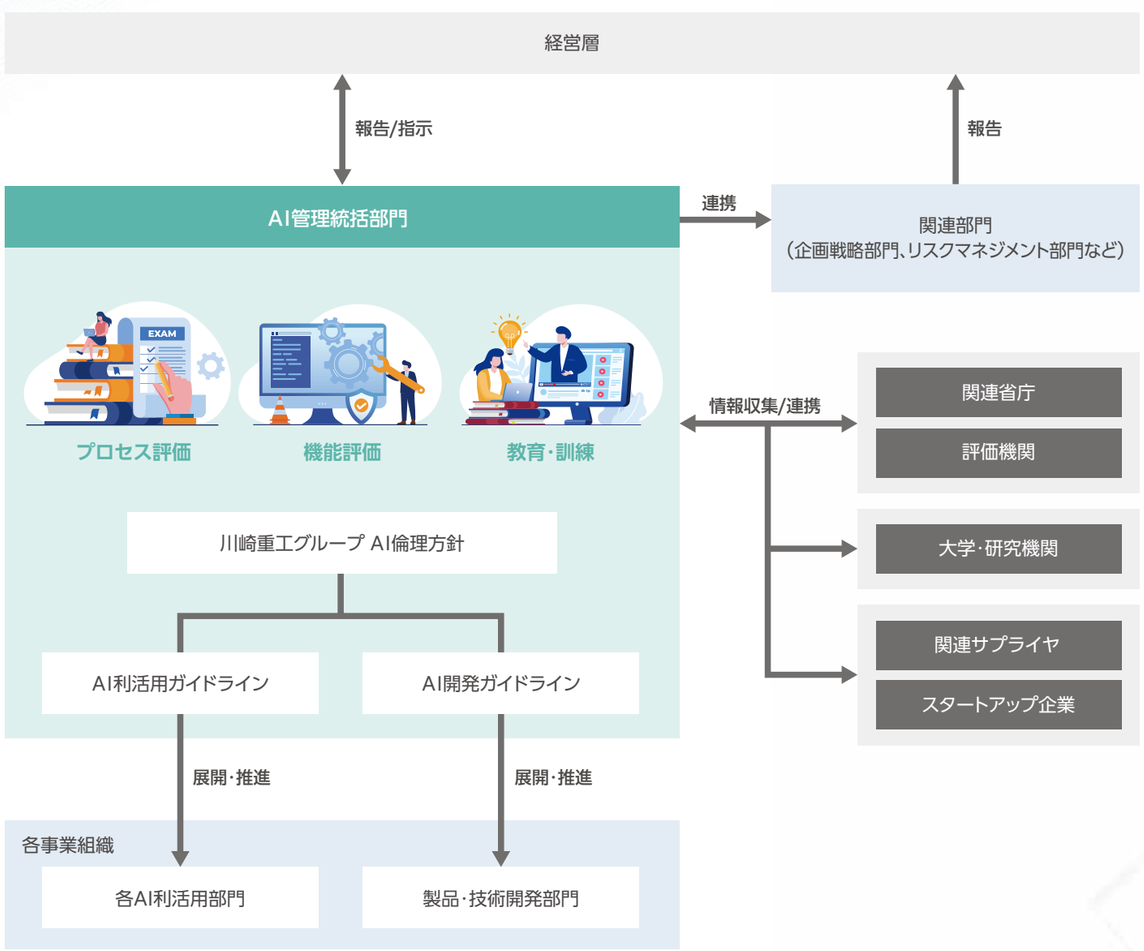
■ AI管理統括部門

関連省庁や評価機関、大学などの研究機関、サプライヤと連携し、技術はもちろん規制や社会受容性を含むAIを取り巻く動向について、幅広く情報を収集・分析します。
また、経営層からの指示に基づき、企画戦略部門やリスク管理部門とも連携し、必要な施策を検討して各事業組織に展開します。さらに、各事業組織における実施状況を確認し、必要に応じて改善を支援することにより、施策の実行を推進します。

■ 各事業組織

当社グループの方針及びガイドラインに則り、AIの利活用及び関連技術の開発を行うとともに、事業に固有の規制など各種要件について情報を収集・分析し、適切に対応します。

AI倫理・管理体制



Information security for the Kawasaki Group products

当社製品に対する情報セキュリティ

製品セキュリティの管理体制

製品セキュリティの基本方針 指示1

当社グループの製品はクラウドなどの通信ネットワークに接続し、より高度な機能やサービスを提供できるよう進化を続けています。一方でデジタル化の進展によりサイバー攻撃の標的となるなどのサイバー脅威にさらされるリスクも増えており、お客様やお客様の事業を守るための製品品質の一つとして製品セキュリティを位置付け、品質の維持と向上に取り組んでいます。

製品セキュリティに対する取り組みとしては、国内外の法令、規格及びお客様との契約の遵守に加え、サイバー攻撃による侵害を防ぐことで安全・安心な製品・サービスを提供するための「川崎重工グループ製品セキュリティ方針」を定めているほか、製品・サービスの企画、設計、製造からお客様における運用に至る製品ライフサイクル全般を対象として、適切なセキュリティを確保するための規定やガイドラインなどを整備しています。

川崎重工グループ 製品セキュリティ方針

■ 法令および契約履行義務の遵守

製品・サービスに対するサイバーセキュリティ確保にあたり、関連する法令、規則、その他の規範およびお客様との契約の遵守を徹底する。

■ 製品セキュリティ管理体制

製品・サービスのライフサイクル全体における製品セキュリティ確保に関して組織的かつ継続的な運用を実現するために管理体制の整備を行う。

■ 製品セキュリティに留意した製品開発の推進

製品・サービスの安全性などの守るべき資産やそれらに対するサイバー攻撃の可能性を、製品・サービスの企画・開発段階において検討し、脆弱性が含まれることのないように努める。

■ 製品セキュリティに留意した運用の推進

お客様に製品・サービスを安心してご利用いただくため、製品セキュリティに関する情報を継続的に収集して分析すると共に、製品・サービスに製品セキュリティ上の問題が発見された際には、関連部門が連携して迅速に対応することで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る。また、必要に応じて、関係省庁及び関係機関への速やかな報告を行う。

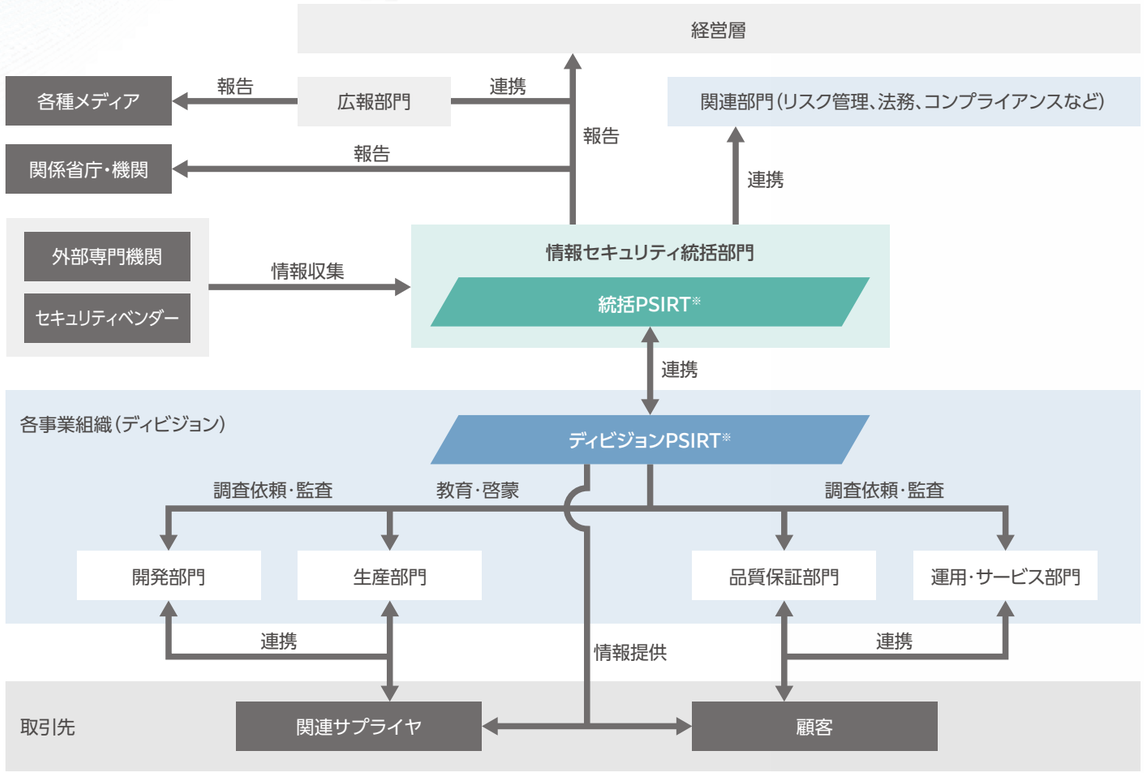
■ 継続的な情報収集とそれに基づく教育の実施

製品セキュリティに関する専門機関や団体との連携などを通して常に最新情報の収集を行い、関連部門間で共有するとともに、社内教育に活かすことで製品・サービスにおけるサイバーセキュリティ意識の向上を図る。

製品セキュリティの管理体制 指示2

お客様にご採用いただいた製品を、安全かつ安心してご利用いただくために、製品・サービスを提供する各事業組織（ディビジョン）に、製品・サービスの脆弱性やセキュリティに関するインシデントへの対応を主導するディビジョンPSIRT※を設置するとともに、各ディビジョンPSIRTと連携してPSIRT活動全般を統括し、経営層やリスク管理部門などの社内関係部門への報告・連携のほか、関係省庁・機関への報告や外部専門機関と連携する専門組織として統括PSIRTを情報セキュリティ統括部門内に設置することで、製品セキュリティの管理体制を構築しています。

製品セキュリティの管理体制



※ PSIRT（Product Security Incident Response Team）：製品に含まれる脆弱性の発見、問題の分析や深刻さ、影響などの調査、改修や修正版の提供、顧客や一般への案内や周知、情報提供、問い合わせ対応、外部からの通報の受付、協業先や関連機関との連絡調整などの活動を行う。

製品セキュリティリスクの管理

製品セキュリティリスクの認識 指示4

当社グループでは、日々高度化するサイバー攻撃による脅威がお客様に影響を及ぼさないように対策を講じることは、当社の事業活動における重要な課題の一つであると捉えています。そのために、製品やサービスに対するサイバーセキュリティリスクを低減する取り組みを当社グループ内に定着させることが重要であると考えています。

製品セキュリティリスクに対する取り組み 指示3 指示4 指示10

安全・安心な製品やサービスを設計・開発するためのセキュア開発プロセス（SDLC※1）を構築して運用し、そのプロセスにおいて構成分析（SCA※2）ツールを活用してソフトウェアの構成情報（SBOM※3）を出力します。出力されたSBOMと収集している脆弱性情報を組み合わせて分析し、製品やサービスに脆弱性が混入するリスクを軽減します。

また、高度化するサイバー脅威を的確に捉えるため、IPAやJPCERT/CCのほか、National Vulnerability Database（NVD）、EU Vulnerability Database（EUVD）などの専門機関などから発信されるサイバー脅威及び当社製品に影響を及ぼす可能性がある脆弱性の情報を継続的に収集し、製品やサービスの設計・開発や脆弱性対応に活用します。

これら一連の取り組みを支えるために、関連するセミナーや教育プログラムへの担当者の派遣、資格取得の奨励と費用の補助などを行うことで人財の育成を進めています。

※1 SDLC（Secure Development Life Cycle）：開発する製品がセキュアであることを担保することを目的とする開発ライフサイクルであり、プロセスの上流から全体においてセキュリティ対策を実施する。

※2 SCA（Software Composition Analysis）：ソフトウェアに含まれるオープンソースソフトウェアやサードパーティライブラリの種類やバージョンなどを特定・把握し、それらに含まれる既知の脆弱性やライセンスリスクを分析・管理することを可能にする技術。

※3 SBOM（Software Bill of Materials）：ソフトウェアに含まれるオープンソースソフトウェアやサードパーティコンポーネント、バージョン、ライセンス情報やそれらの依存関係の情報を含む機械処理可能な一覧リスト。

製品セキュリティにおける脆弱性対応 指示5 指示7

脆弱性の悪用やインシデントによる被害を最小限にとどめるために、社外からの情報提供を受け付ける窓口を当社ホームページ上に設置しています。情報提供やインシデント報告を受けた場合やディビジョンPSIRTにて脆弱性を発見した場合には、脆弱性の内容やインシデントの原因及びその影響範囲の分析、製品を利用されているお客様へのヒアリングのほか、対応方法の検討及び実装をディビジョンPSIRTにて主導し、各事業組織にて対応を行った上で、お客様に脆弱性への対応策など必要な情報を共有します。また、並行して統括PSIRTは、経営層やリスク管理部門など社内関係部門との報告・連携のほか、関係省庁・機関への報告や外部の専門機関と連携して迅速に対応を行います。

川崎重工業株式会社
https://www.khi.co.jp/

この「情報セキュリティ報告書」は当社Webサイトから
ダウンロードいただけます。

2026年9月発行