Kawasaki
Powering your potential

川崎重工グループ

情報セキュリティ報告書

2023

川崎重工業株式会社

「情報セキュリティ報告書2023」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

INDEX

○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

2023年12月31日までの活動を報告対象としております。

デジタル時代の到来は、人々の暮らしに急速な変化をもたらしています。あらゆるものがネットワークでつながることで我々は場所を問わずに膨大な情報にアクセスでき、クラウドの強力な計算能力を利用した様々なサービスを受けることができます。このような進化が社会の利便性を高めていく一方で、社会インフラの安定性や個人のプライバシーを脅かすサイバー攻撃が大きな社会問題になっています。また、世界は地政学的な不安定さを増しており、安全保障上の課題としてもサイバーセキュリティが多く語られている状況です。サイバー脅威にどう立ち向かうのか、国や社会全体が一体となって連携すべき新たな課題と感じています。

川崎重工グループは120年以上にわたり、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」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。

その一方でDXによる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、営業情報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。
このような状況を踏まえ、当社グループで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24h/365d体制での監視に加え、仮に攻撃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、全ての従業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み始めています。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ともに、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に取り組んでいます。

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、安心・安全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・調達・TQM・総務・DX戦略担当、全社北米事業タスクフォース担当、技術開発本部長

情報セキュリティの方針

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、お客様やお取引先様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ともに、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、以下の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およ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体系

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

川崎重工グループ情報セキュリティ方針

〇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。

〇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。

〇教育・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。

〇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、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。

〇問題発生時の対応
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。

情報セキュリティの方針

情報セキュリティの管理体制

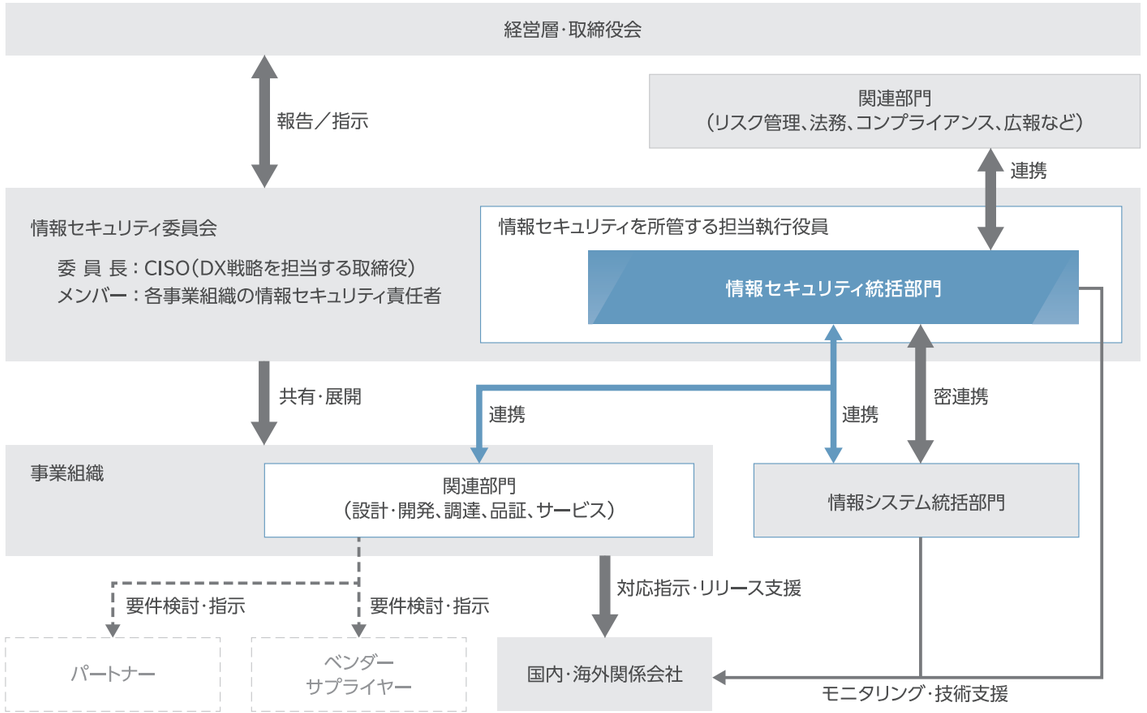
指示2 指示6

情報セキュリティの管理体制としては、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メンバーとして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本社内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



情報セキュリティリスクの管理

情報セキュリティリスクの認識

指示4

当社グループの事業活動においては、お客様やお取引先様の情報、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。

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

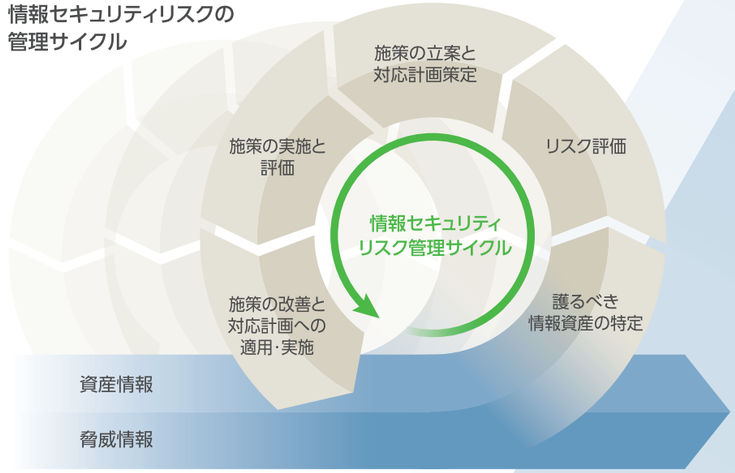
情報セキュリティリスクを低減させる取り組みとして、当社グループとして護るべき情報資産を特定するとともに、高度化するサイバー脅威を的確に捉えるため、情報処理推進機構（IPA）やJPCERT/CCなどの専門機関、セキュリティベンダー、セキュリティアナリストなどから発信された脅威情報を日々収集しています。収集した脅威情報を基に想定される攻撃者、攻撃手法、攻撃シナリオなどの分析、脆弱性の特定を行っています。その上で分析・特定した脅威や脆弱性から適切に情報資産が護られているかについて定期的にアセスメントを実施し、リスクの評価を行います。評価の結果に基づいて、必要となる情報セキュリティ施策を立案し、施策の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。

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

インシデント対応の体制と仕組み

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様に関わる情報や当社グループの情報資産を護るため、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

サイバー脅威を調査、分析し、インシデント対応をサポートします。

検知・分析機能

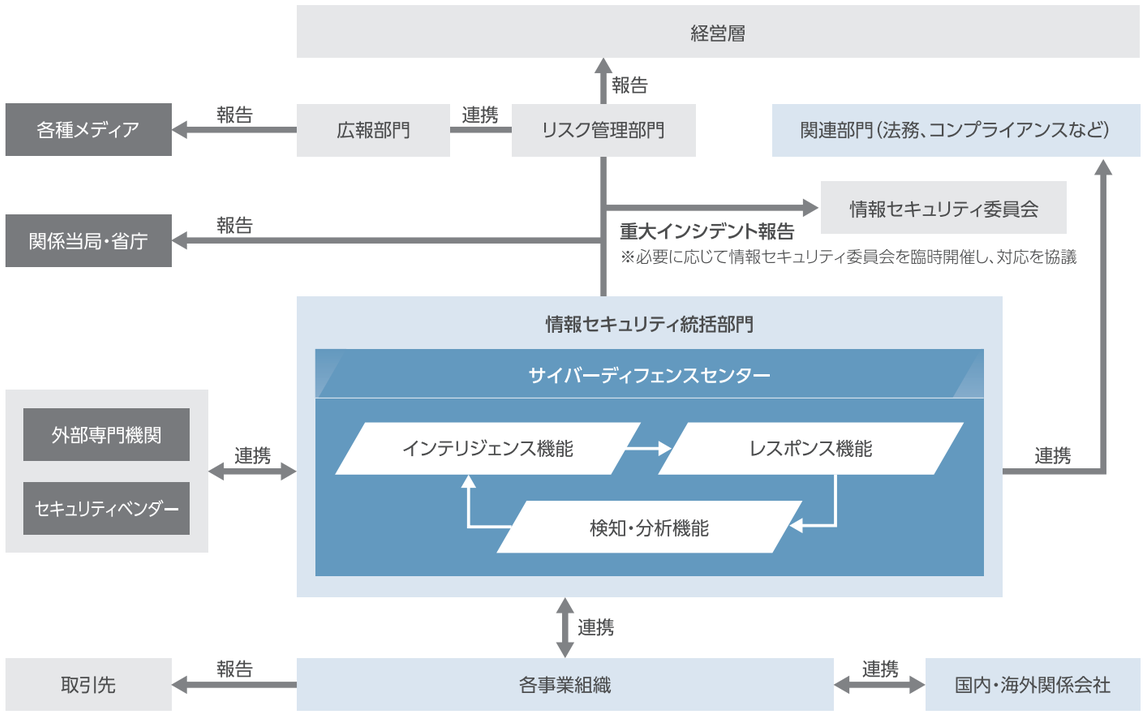
サイバー攻撃を常に監視し、異常を検知し、分析します。

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



インシデント対応の仕組み 指示5 指示7 指示8

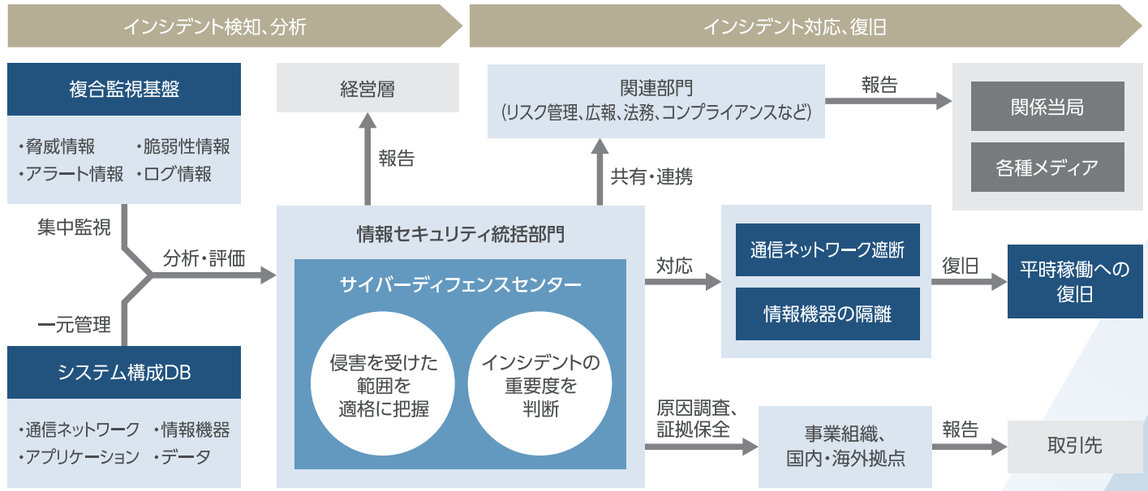
インシデント検知、分析

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、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。

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、お取引先様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。

情報セキュリティの教育と連携

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。

2022年度においては、情報セキュリティ教育を9,803名、疑似標的型攻撃メールによる訓練を2,308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、育成にも取り組んでいます。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。

関係会社、お取引先様との取り組み　指示9

関係会社における情報セキュリティ対策の取り組み

国内の関係会社においては、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、検知するための体制を整えています。また、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たセキュリティ対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。

お取引先様の情報セキュリティ対策の取り組み

当社グループでは、サプライチェーンにおける情報セキュリティ対策の取り組みも重要であると認識しています。
お取引先様向けのガイドラインなどを用意し、情報セキュリティ対策への取り組みを促し、お取引先様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。

認証および新たな取り組み

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 プロジェクト推進部
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

CSMS(IEC62443-2-1)※2認証取得組織

川崎重工業株式会社
　エネルギーソリューション&マリンカンパニー プラントディビジョン

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

※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。

※2 CSMS(IEC62443-2-1)(Control Systems Security Management Systems):産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムのこと。

製品セキュリティ、工場の生産セキュリティの取り組み

製品セキュリティの取り組み

当社グループの製品はネットワークやクラウドに接続し、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を受け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、規格およ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、製造から運用に至る製品ライフサイクル全般の活動において、適切なセキュリティを確保するためのガイドラインなどの整備を実施しています。

製品セキュリティ方針に基づいた活動を統括する専門組織(PSIRT※4)を設置し、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し、脆弱性と呼ばれる製品・サービスのセキュリティ上の弱点が含まれることのないように製品・サービスの品質向上に努めるなど、製品セキュリティに関するプロセスが適切に機能するよう取り組んでいます。

※4 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。

川崎重工グループ製品セキュリティ方針

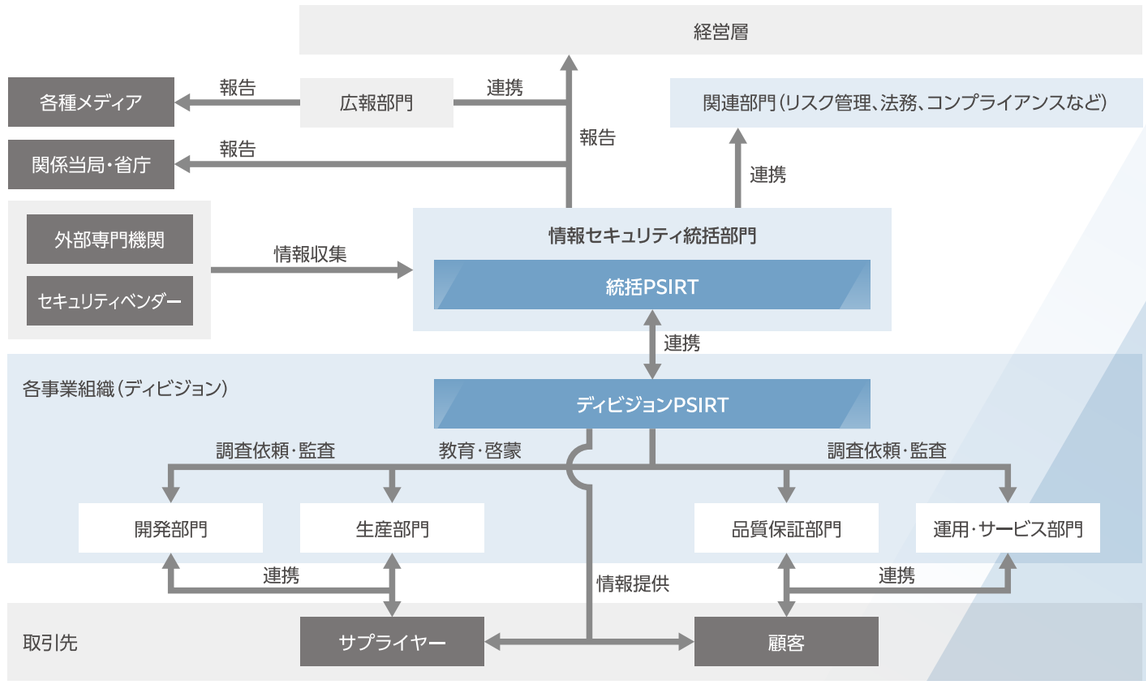
○法令および契約履行義務の遵守
製品・サービスに対するサイバーセキュリティ確保にあたり、関連する法令、規則、その他の規範およびお客様との契約の遵守を徹底する。

○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。

製品セキュリティの推進体制



認証および新たな取り組み

製品セキュリティ、工場の生産セキュリティの取り組み

工場の生産セキュリティの取り組み

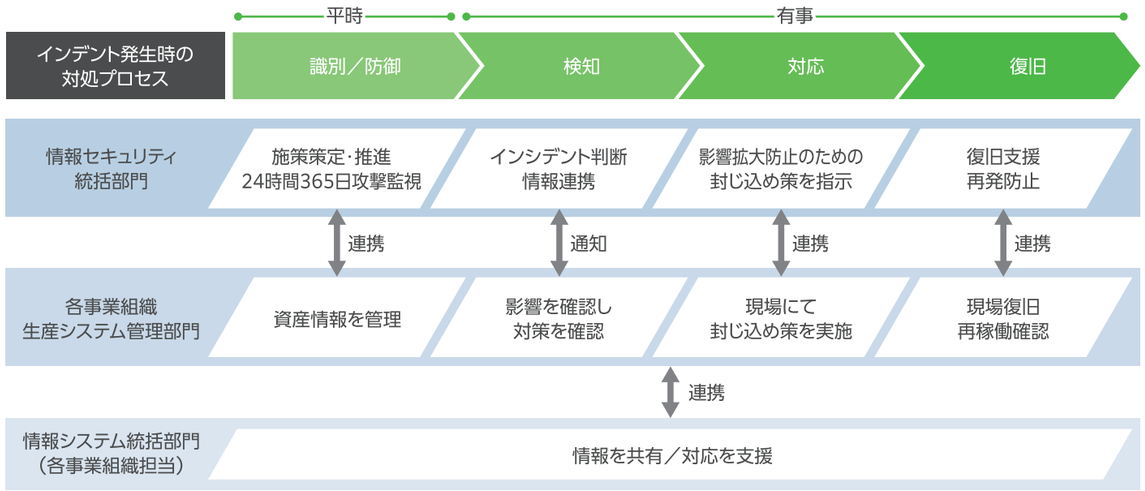
近年、様々な業務システムと生産系のシステム・製造設備を通信ネットワークで接続し、生産性向上を目的としてデータの蓄積・活用を行う取り組みが進んでいます。これによりサプライチェーン上の一企業へのサイバー攻撃による侵害から連鎖的に影響が広がり、生産停止に追い込まれる事例が多発するなど、工場の生産システムに対するサイバー脅威が大きな社会課題となっています。

このような状況から当社グループでは、制御システムの安全を護るための国際基準CSMS(IEC62443-2-1)に沿った対策として、生産現場・生産設備の安全確保はもとより、環境への影響の最小化、サプライチェーンを含めた生産活動の安定化を目的に、工場の生産システムや工場の稼働を支えるインフラのセキュリティ強化に取り組んでいます。

生産システムのセキュリティに関して基本方針の策定や生産管理部門と情報セキュリティ統括部門との連携体制を強化するなど管理体制の整備をしています。また定期的なリスク評価を通じてサイバー脅威を明確にし、そのリスクに応じて生産システムや工場内の通信ネットワーク、外部との通信ネットワーク等へのアクセスを必要最低限に制御するなどの対策を進めています。更に緊急時には迅速かつ効果的な対応ができるよう、インシデント対応体制の整備に取り組んでいます。

工場の生産セキュリティに対する取り組み状況

工場の生産セキュリティに対する役割と管理プロセス



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、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。

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。

2024年2月発行