情報セキュリティ

基本的な考え方

企業のDX戦略が加速する中、さまざまな「モノ」や情報がつながることで、新たな価値が世の中に生み出されています。その一方、日々巧妙化するサイバー攻撃などの脅威や「会社情報」「得意先・お客様情報」などの情報漏洩に関するリスクマネジメントは、企業の持続的成長における重要課題の一つと捉えています。

方針

「アイシングループ情報セキュリティ基本方針」を定め、組織的かつ継続的に情報セキュリティ対策に取り組んでいます。

アイシングループ情報セキュリティ基本方針

(1)法令遵守
(2)安定した経営基盤の維持
(3)安全な商品・サービスの提供
(4)安全なサイバー空間づくりへの貢献
(5)情報セキュリティマネジメント

WEB「アイシングループ情報セキュリティ基本方針」

めざす姿

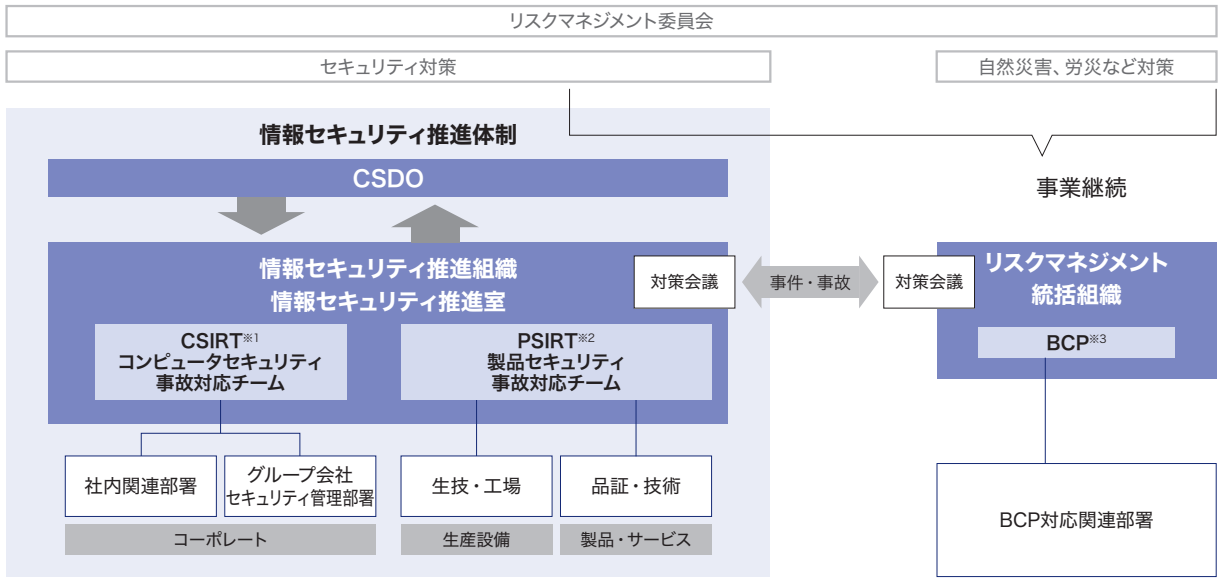
お客様や取引先から預かった、またはアイシンが保有する事業活動に関わる情報資産は、重要な資産であるとの考えのもと、企業の経営諸活動への脅威の変化や技術の進展を適切に捉え、網羅的な対策をグループ全体に実施していきます。

推進体制

CSDO※が経営戦略に沿った情報戦略やIT投資計画の策定などに責任を持ち、情報セキュリティ、および、個人情報の保護の実施・運用に関する責任・権限の役割を担っています。CSDOの下、サイバー攻撃や内部不正などのリスクから企業を守るため、セキュリティ専門組織である情報セキュリティ推進室を設置し、グループ全体でセキュリティ対策の活動を実施しています。情報セキュリティの方針、および対策については、リスクマネジメント委員会で提案し、グループ全体で認識の共通化を行い、セキュリティ水準の引き上げと着実な対策実施を図っています。

※ CSDO : Chief Software & Digital Officer

情報セキュリティ推進の体制図



※1 CSIRT : Computer Security Incident Response Team
※2 PSIRT : Product Security Incident Response Team
※3 BCP : Business Continuity Planning

情報セキュリティの取り組み

アイシンはグループ全体のセキュリティ対策をグループ本社に集約し、巧妙かつ高度化しているサイバー攻撃、内部情報漏洩に対するセキュリティ、各国法などへの対応に取り組んでいます。また、生産停止などにつながるセキュリティ重大事案が発生した際には、速やかにCSDO、リスクマネジメント関係部署に報告し、調査・分析を行い、対策を講じています。

情報セキュリティ対策

国際規格 ISO 27001/27002(2022年4月認証取得)、および日本自動車産業サイバーセキュリティガイドラインに準拠したセキュリティガイドラインを策定し、顧客のセキュリティ対策要求へ備え、サプライチェーン全体の相互レベルアップに活かす取り組みを進めています。

セキュリティガイドライン

管理項目	対策内容
組織	推進体制、ルール、手順
教育	教育実施、啓蒙、訓練
技術的対策	資産管理、アクセス制御、ネットワークなど
物理管理	ファシリティ、エリア制御
事件・事故体制	報告体制、ルール

製品セキュリティ対策

法規対象車両の拡大を見据え、PSIRTを中心とした車両のセキュリティ対策に取り組んでいます。また、日米のAUTO-ISAC※1に加盟し、業界内で発生したリスク情報を収集して自社開発に活かす活動を推進するとともに、ISO21434への対応も行っています。

※1 AUTO-ISAC：Automobile Information Sharing and Analysis Center／北米の自動車サイバーセキュリティ組織

個人情報保護対策

個人情報保護対策では、GDPR※2をはじめとした各国法への対応が重要になります。DX戦略を加速していく中では、各国間での個人情報の移転が必要になります。そこで、アイシンではグループ全体で個人情報の移転を可能にするグループ包括SCC契約※3を、グループ会社間で締結しました。

今後も各国法を注視するとともに、全従業員への教育・周知を実施し、確実な個人情報の取り扱いに努めていきます。

※2 GDPR：General Data Protection Regulation／EU一般データ保護規則
※3 SCC契約：Standard Contractual Clause／標準契約条項

セキュリティ意識の醸成

セキュリティの向上は、全従業員が自分ごととして意識し、常に身近なものとして認識し行動することが不可欠です。入社時・昇格時の階層別研修、海外赴任などのイベント時の教育、不審メール対応訓練、情報セキュリティ強化月間での啓発活動など、グループ全体で取り組んでいます。

例えば、教育用の動画コンテンツを自社で作成する、教育実施の後に理解度テストを実施する、各国の従業員から募集した情報セキュリティ標語を「サイバーセキュリティニュース」で公開するなど、全従業員一人ひとりの参画、およびセキュリティ意識の醸成を図っています。

教育・啓発活動の実施例

① 入社時・昇格時など階層別の研修実施 （2022年度：グループ3,000人）
② 海外赴任時・出向受け入れ時などイベントごとに研修実施
③ 全従業員対象の不審メール対応訓練実施（1回/年）
④ 情報セキュリティ強化月間（1回/年）や社内報配布（1回/月）を通じた、啓発活動実施