サイバーセキュリティ

企業活動における情報（知的財産、技術情報、営業情報および個人情報等を含む）を守っていくことは、社会に多くの重要インフラを提供する三菱重工グループの責務との認識から、サイバーセキュリティの確保と向上を目指し、当社グループのサイバーセキュリティ基本方針およびサイバーセキュリティ戦略を策定しています。また、当社グループではサイバーセキュリティリスクを重要なリスクの一つと認識し、マテリアリティ（重要課題）として定期的にモニタリングを実施し、CEOがサイバーセキュリティ戦略を監督するとともに、CTOがサイバーセキュリティ委員会で審議した結果を経営会議・取締役会に年1回以上報告します。

当社グループでは、サイバー攻撃によるリスクを最小化するため、CTO直轄のサイバーセキュリティ推進体制を構築し、サイバーセキュリティの統制、インシデント対応、教育・訓練等を実施するとともに、グローバルレベルのフレームワーク構築に貢献しています。

サイバーセキュリティ統制

当社グループでは、NIST CSF※1を参考にサイバーセキュリティの基準を整備し、複数の外部インテリジェンスサービスも活用したサイバーセキュリティリスクの把握・是正等により、ウイルス等の侵入の未然防止のみならずサイバー攻撃に対する多層的な防御措置を講じています。セキュリティリスクの予兆が発見された際には、躊躇なく緊急対策を展開します。さらに、サイバーセキュリティの維持・向上のため、脆弱性診断や脅威情報の収集・分析等を通じて、巧妙化するサイバーセキュリティの最新情報を把握し、教育・訓練を行い社員のセキュリティ意識の向上を図るとともに、定期的な自己点検や内部監査を実施しています。また、サイバーセキュリティ経営ガイドライン※2等、政府・団体からのガイドライン策定・改訂状況を参考に、当社グループの適合状況・課題を踏まえ、基準類を見直しています。当社グループがお客さまに提供する製品・サービスの制御システムについても、セキュリティリスクをコントロールするフレームワークを構築し、ビジネスパートナーと共に製品・サービスの継続的なサイバーセキュリティ対応を進化させていきます。この分野における次世代ソリューションの開発を促進し、安全・安心な社会の構築に貢献していきます。

※1 NIST CSF: National Institute of Standards and Technology Cyber Security Framework
※2 経済産業省が2016年12月に公開

サイバーセキュリティインシデント対応

万一、サイバーセキュリティインシデントが発生した場合には、インシデントの分析調査、原因究明、システムの復旧、再発防止措置等をリードするCSIRT※3を設置し迅速に対応するとともに、関係省庁を含むステークホルダーへの報告や公表等も実施します。重大なインシデントの場合は、取締役への報告とともに、社の危機管理体制で対応し、事業継続計画策定による速やかな復旧を図ります。より迅速な経営判断・情報発信が求められるランサムウェア攻撃の流行に対応すべく、インシデント対応訓練を通じて、有事の際の組織の対応能力・課題を確認し、見直しています。

※3 CSIRT: Computer Security Incident Response Team

サイバーセキュリティ教育・訓練

当社グループでは、役員を含む全社員を対象に、役割に合わせたサイバーセキュリティ教育・訓練を定期的に実施し、社員のセキュリティレベルの維持・向上を図っています。また、各製品・サービスのセーフティとセキュリティの両方を考慮できる技術者の育成を図っています。

グローバルレベルのフレームワーク構築に貢献

産業サイバーセキュリティ研究会※4、Charter of Trust※5、経団連サイバーセキュリティ経営宣言2.0に関する取り組み（2022年10月に公表）等への参加を通じて、グローバルレベルのサイバーセキュリティ対策におけるフレームワーク構築に貢献しています。

※4 産業サイバーセキュリティ政策検討のための経済産業省主宰の活動。当社は2017年12月より参加
※5 サイバーセキュリティ信頼性構築のための民間企業レベルの活動。当社は2019年4月より参加