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が経営会議・取締役会に年1回以上報告しています。

当社グループでは、サイバー攻撃によるリスクの最小化を推進するため、CTO直轄のサイバーセキュリティの推進体制を構築し、当社グループのサイバーセキュリティ統制（基準整備・対策実装・自己点検・内部監査）、サイバーセキュリティインシデント対応、サイバーセキュリティ教育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。昨今増加している「Emotet」と呼ばれるマルウエアへの感染防止対策として、パスワード付き圧縮ファイルを添付したメール受発信を禁止しました。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、教育と合わせて社内ポータルを使った情報発信と共有により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などにより基準への適合状況を確認しています。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・課題を踏まえて、基準類を見直しています。当社グループ各社がお客さまに提供する製品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、製品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、便利で快適な生活、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（Computer Security Incident Response Team）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、取締役および社内関係者へ報告するとともに、社の危機管理体制で対応します。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。

サイバーセキュリティ教育

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※3、Charter of Trust※4、経団連サイバーセキュリティ経営宣言に関する取組み（2020年3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。

※3 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
※4 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