# ＞サイバーセキュリティの取り組み

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、当社グループのサイバーセキュリティ方針を制定し、サイバーセキュリティの確保と向上に取り組んでいます。

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直轄にサイバーセキュリティ推進体制を構築し、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）、インシデント対応、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、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。

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／分析等を通して巧妙化するサイバーセキュリティ最新情報を把握するとともに、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。

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、製品への実装を推進します。この分野における次世代ソリューションの開発には継続的に重点を置いています。

※1 NIST CSF：National Institute of Standards and Technology Cyber Security Framework

## サイバーセキュリティインシデント対応

万一、サイバー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、関係省庁への報告等も実施します。

## サイバーセキュリティ教育

当社グループでは、役員を含む全社員に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。

## 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※2、Charter of Trust※3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。

※2 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催の活動。当社は2017年12月より参加
※3 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