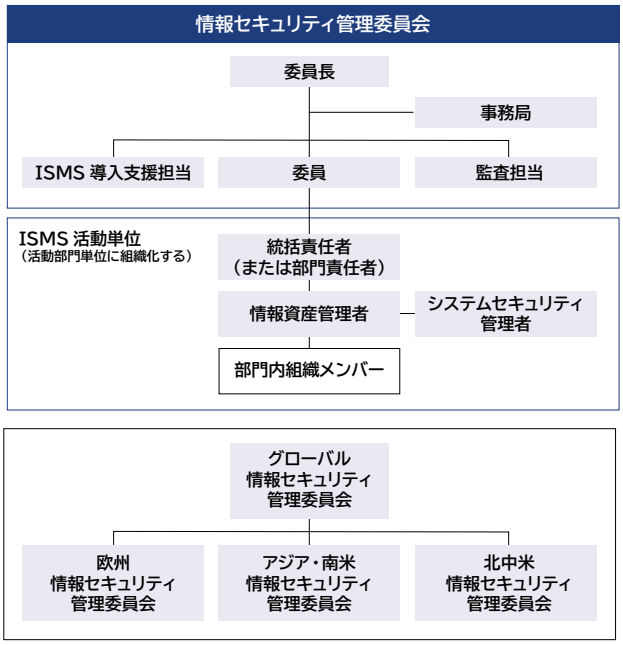
情報セキュリティ

基本的な考え方

近年、組織化されたプロ集団によるサイバー攻撃が増加しており、その標的は国家・企業を問いません。攻撃手口も複雑で発見しにくいものとなっており、サイバー攻撃によって情報漏えい事件・事故が発生した場合、お客様をはじめとするステークホルダーからの信用低下や利益の損失につながる恐れがあります。

矢崎グループでは、業務上知り得たお客様の個人情報を含むさまざまな機密情報の保護をするとともに、お客様の視点に立ち、製品に関する必要な情報を適切に管理するため、プライバシーポリシーを含む各種ルールを制定し、情報セキュリティへの取り組みに注力しています。

情報セキュリティ推進体制図



推進体制

矢崎グループでは、「情報セキュリティ管理委員会」を設置し、部門ごとに委員を配置しています。隔月で開催している委員会では、委員27名が各部門の情報セキュリティ活動の状況確認および標準化・共通施策・教育に関する検討を行っており、高いセキュリティレベルの維持に努めています。

また、欧州GDPR※をはじめ各国の個人情報保護法、セキュリティ対応のために、グローバルの各地域（欧州、アジア・南米、北中米）で推進体制を整備しています。

今後も情報セキュリティ活動を推進することで、お客様をはじめとするステークホルダーからの信頼獲得に努めていきます。

※GDPR：General Data Protection Regulation（一般データ保護規則）

運用

情報セキュリティマネジメントシステム（ISMS）によるPDCAを1年間で回す活動を継続することにより、セキュリティの維持・強化に努めています。

また、セキュリティ事故発生時には、情報セキュリティ管理委員会に報告し、初動対応の迅速化、再発防止の徹底を図っています。

サイバー攻撃に対しては、模擬メール訓練、ログ監視、脆弱性評価、ネットワーク監視などの対策強化を実施しています。