情報セキュリティ

体制（ガバナンス）

当社グループでは、情報セキュリティインシデント発生に備えた組織横断的機関である「SUMIBE-CSIRT」を設置し、定例会議などを通してトピックスの共有、情報セキュリティ事故発生を未然に防ぐための対策策定、事故発生時の対応手順の整備を行う一方で、有事の際には経営層を含めた対応や外部セキュリティ関係機関との連携を行う体制としています。

リスク管理

当社グループにかかわる情報セキュリティに係るリスクおよび機会の識別、評価、ならびに管理は、下記リンク先のページに記載のリスクマネジメント体制・リスクマネジメントプロセスに沿って実施しております。

リスクマネジメント

指標と目標

当社グループでは、サイバーセキュリティを「経営の重要課題」の1つとして選定、 重大なセキュリティインシデントの件数、情報セキュリティ教育受講率、情報セキュリティインシデント訓練の開催回数を「経営の重要課題」のKPIとして設定し管理しております。

経営の重要課題
サステナビリティ関連詳細データ（ガバナンス）＞リスクマネジメント関連

主な取り組み

情報セキュリティインシデントを予防するための具体的な取り組みとしては、不正攻撃の標的となる脆弱性への対応の徹底、セキュリティ対策製品の導入によるリスク検知、外部セキュリティ企業とも連携したサイバー攻撃の常時監視、外部機関によるセキュリティ評価等の対策を行っております。さらに、日本シーサート協議会やサイバー情報共有イニシアティブ(J-CSIP)等、サイバー攻撃に関する情報共有や対応強化を行う外部団体に参加し、積極的な情報入手を図っています。引き続き、外部セキュリティ企業支援のもと、グローバルで連携したインシデント対応体制の確立を進めていきます。
また、差し迫るサイバーリスクに対しては、適宜当社グループ内に注意喚起を発信、また国内外の全役員、従業員を対象に、サイバーリスクのトレンドを踏まえた情報セキュリティ教育を定期的に実施する等、情報セキュリティインシデントへの予防強化と情報セキュリティへの意識向上に取り組んでいます。
セキュリティインシデント発生時の被害の最小化と早期復旧を図るべく、社内でのインシデント発生訓練に 加え、外部団体との合同訓練にも参加する等、体制の強化にも取り組んでいます。
社内セキュリティ人材の強化策として、国家資格である「情報処理安全確保支援士」の取得を進めています。また、日本国外の拠点におけるセキュリティ人材配置・育成も進めていきます。


社内でのインシデント発生訓練