情報セキュリティ

GRI 103-2, 418-1

情報セキュリティ方針

企業のDX戦略が加速する中、さまざまな「もの」や情報がつながることで、新たな価値が世の中に生み出されています。その一方、日々巧妙化するサイバー攻撃等の脅威や「会社情報」「得意先・お客様情報」等の情報漏洩に関するリスクマネジメントは、企業の持続的成長を阻害する重要課題のひとつと捉えています。

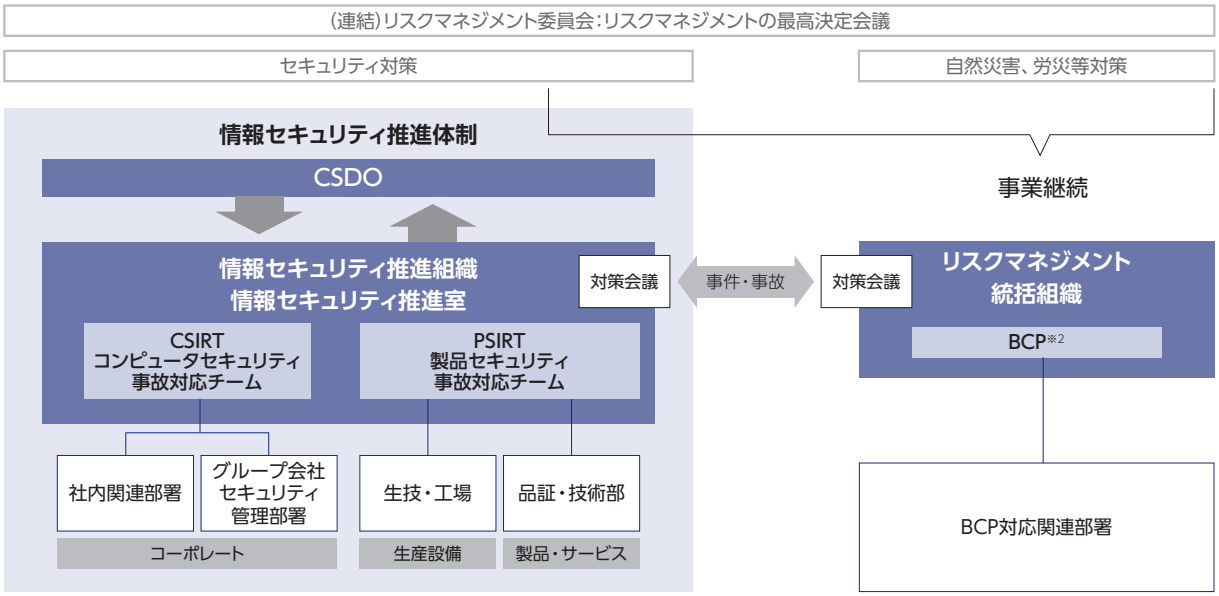
こうした背景のもと、「アイシングループ情報セキュリティ基本方針」を定め、お客様や取引先から預かった、またはアイシンが保有する事業活動に関わる情報資産は、重要な資産であるとの認識に立ち、組織的かつ継続的に情報セキュリティ対策に取り組んでいます。

情報セキュリティ推進体制

CSDO※1が経営戦略に沿った情報戦略やIT投資計画の策定などに責任を持ち、情報セキュリティ、および、個人情報の保護の実施・運用に関する責任・権限の役割を担っています。CSDOの下、サイバー攻撃や内部不正等のリスクから企業を守るため、セキュリティ専門組織である情報セキュリティ推進室を設置し、アイシン全体でセキュリティ対策の活動を実施しています。情報セキュリティの方針、対策については、(連結)リスクマネジメント委員会で提案し、グループ全体の情報セキュリティの向上を図っています。また、生産停止等につながるセキュリティ重大事案が発生した際には、速やかにCSDO、リスクマネジメント関係部署に報告・調査・分析を行い、対策を講じています。

※1 CSDO : Chief Software & Digital Officer

情報セキュリティ推進の体制図



※2 BCP:Business Continuity Planning