サイバーセキュリティ

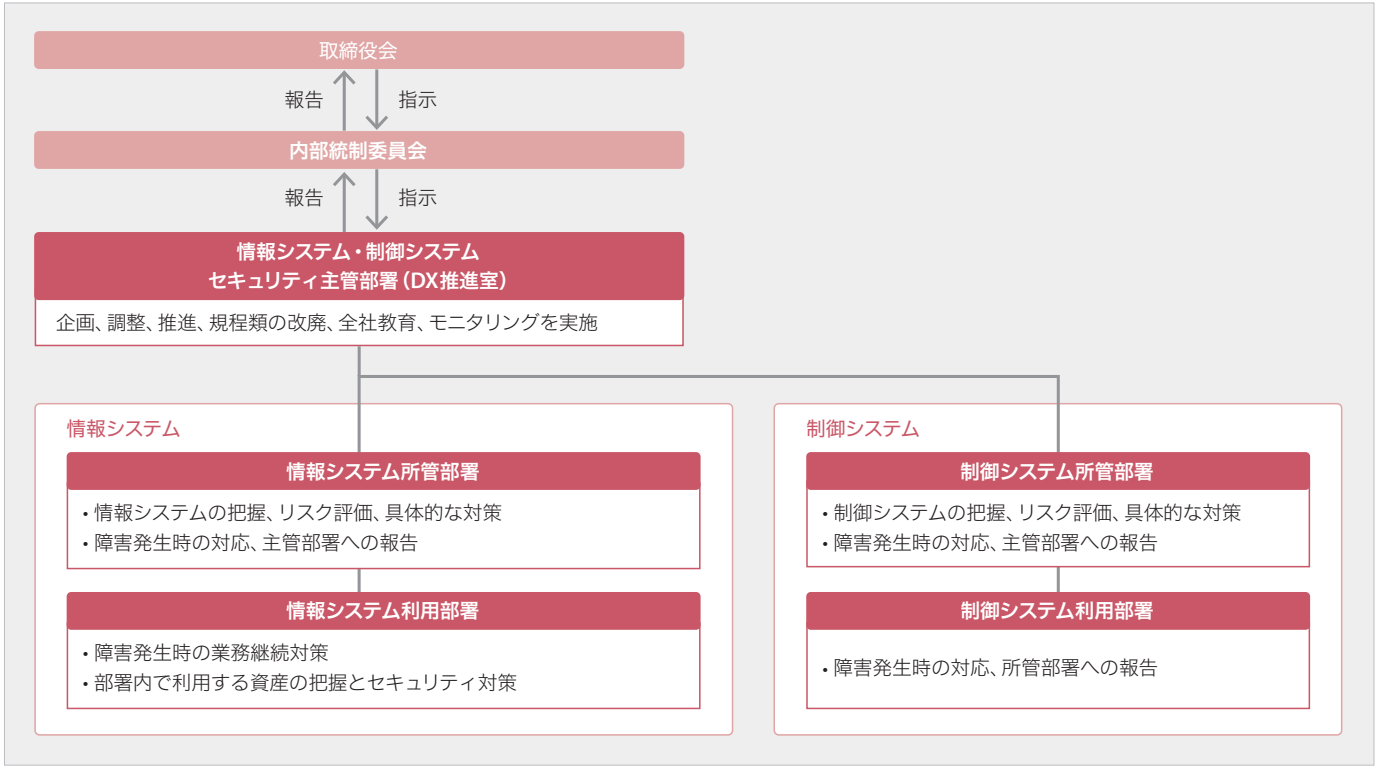
基本的な考え方

当社ではITの活用を通して「事業の競争力強化」「新たな価値創造」を追求するデジタル革新を加速していますが、一方でサイバー攻撃の巧妙化・高度化などにより情報システムや制御システムへのリスクも増大しています。サイバーセキュリティの目的は、情報システムの適切な管理による情報の漏洩や紛失の未然防止、制御システムの適切な管理を通じた健康・安全の確保や環境への影響防止、そしてセキュリティインシデント発生時の影響を最小限に抑えることなどです。当社は、重要インフラ事業者としての責任を果たすべく、サイバーセキュリティを経営上の重要課題として捉え、組織的・制度的・人的・技術的・物理的な側面から多面的なシステムセキュリティ対策を実施しています。

マネジメント体制

住友化学では、情報システムセキュリティおよび制御システムセキュリティについて以下の体制を構築して、PDCAサイクルを実施しています。

■ 情報システム・制御システム セキュリティ体制



目標・実績

組織の情報セキュリティの枠組みの国際規格であるISMS(Information Security Management System)の考え方に準じ、セキュリティポリシーを定め必要な対策を実施しています。

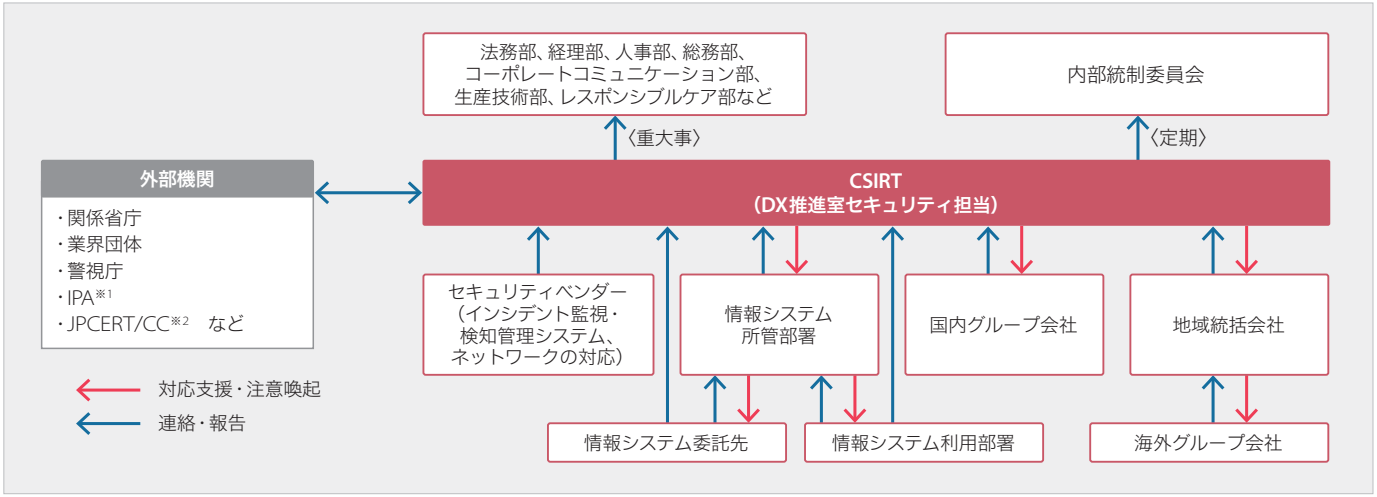
以下のような多面的なセキュリティ対策(多層防御と減災)を基本的な考え方としています。

対策分類	対策内容
組織的対策	・情報システムセキュリティ／制御システムセキュリティ対応体制構築 ・セキュリティインシデントに備え、事前に組織内外との情報共有体制を構築
制度的対策	・グループ会社を含めてセキュリティに関する標準、基準文書を制定 ・グループ会社を含めて定期的にITセキュリティ自己点検、ITセキュリティ内部監査を実施
人的対策	・eラーニングシステムなどを利用したセキュリティ定期教育を実施 ・注意喚起やセキュリティインシデント対応演習を実施
技術的対策	・サーバやパソコンなど個々のコンピュータやネットワークについて、アクセス制御対策、マルウエア対策、脆弱性対策などを実施
物理的対策	・入退室管理などの対策が完備されたクラウドサービスの利用

取り組み事例

情報システム・制御システムセキュリティ主管部署(DX推進室)内にCSIRT(Computer Security Incident Response Team)を設置し、外部機関からのセキュリティ情報の分析、当社グループ内への注意喚起や当社グループ内で発生したセキュリティインシデント情報を収集し、対応を全体管理しています。

■ セキュリティインシデント対応体制



※1 IPA:独立行政法人 情報処理推進機構
※2 JPCERT/CC:Japan Computer Emergency Response Team Coordination Center