情報セキュリティ基本方針

アイシングループ情報セキュリティ基本方針

アイシングループは、お客様や取引先からお預かりした、または当社が保有する事業活動に関わる情報資産（以下「情報資産」）は、当社の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に取り組むことを目的として、『アイシングループ情報セキュリティ基本方針』（以下、「本方針」という）を定める。

1. 基本的な姿勢

（1）法令遵守

情報セキュリティに関係する法令、国が定める指針、契約上の義務、およびその他の社会的規範を遵守する。

（2）安定した経営基盤の維持

情報資産を適切に管理・保護することにより、競争力および事業継続性の確保など安定した経営基盤の維持に努める。

（3）安全な商品・サービスの提供

商品・サービスの開発・設計・製造・販売等、自社の事業活動において、情報セキュリティの対策を講じることにより、お客様や社会に対し、安全な商品・サービスを提供する。

（4）安全なサイバー空間づくりへの貢献

情報システムや情報通信ネットワークなどにより構成され、情報が流通するインターネット、拡大するAIの活用機会、その上で多様なサービスやコミュニティなどが形成される仮想的な空間（以下、「サイバー空間」という）を利用者が安心してその恩恵を享受できるよう、安全なサイバー空間づくりに貢献する。

（5）情報セキュリティマネジメント

ガバナンス体制の構築とともに、事故対応を含めたリスクマネジメントを行ない、情報セキュリティの継続的な推進および改善を行なう。

2. 情報セキュリティの取り組み

（1）任務・責任体制の明確化

情報資産の適切な管理・保護を実施するために、情報セキュリティにおける推進体制を整備し、その任務と責任を明確にする。

（2）情報セキュリティ規程の整備

情報セキュリティに関する規程を定め、規程に基づく具体的な管理要領・手続きを整備する。

（3）リスクマネジメント

①守るべき情報資産およびそれに対する情報セキュリティの脅威を特定する。
②特定した脅威に対する備えの状況および脅威の影響度合いに基づき、情報資産を損なう事象の発生防止に向けた必要な対策を講じる。
③情報資産を損なう事象が発生した場合には、速やかに、当該事象の収束、被害拡大防止、原状への復旧および再発防止などに向けた適切な対応を行う。

（4）教育・啓発

役員および従業員等に対し情報セキュリティに関する意識向上を図るために、必要な教育および啓発活動を実施する。

（5）継続的改善

情報セキュリティにおけるPDCAサイクルを回し、情報セキュリティに係る仕組みを継続的に見直し・改善する。

3. 取り組み状況の点検・監査

本方針に基づく取り組み状況について、定期的な点検・監査（内部監査を含む）を実施し、当該結果をリスクマネジメントに関係する経営層に報告するものとする。

2025年6月
株式会社アイシン
DX戦略センター長
牛田孝一