情報セキュリティ基本方針

株式会社 AIHOBS（以下「当社」）は、医療機関や医療機器メーカーなど、安全性が極めて重要な領域における通信・データ連携を支える「セキュアなネットワークプラットフォーム」を提供する企業として、取り扱う情報資産を確実に保護し、安心してご利用いただけるサービスを提供することを最優先の使命としています。

当社は、情報セキュリティを経営の最重要課題の一つと位置づけ、組織全体でその確保・維持・向上に取り組みます。
ここに情報セキュリティ基本方針を定め、役員・従業員をはじめとするすべての関係者がこれを遵守し、信頼される企業として社会的責任を果たしてまいります。

---

1. 経営者のコミットメント

当社は、情報セキュリティの確保を経営の根幹と捉え、経営者自らが率先して体制整備、資源の投入および継続的改善を推進します。

2. 体制および管理の整備

当社は、情報セキュリティマネジメントシステム（ISMS）の考え方に基づき、情報セキュリティ管理責任者を中心とする組織体制を整備し、社内規程・手順を策定して、情報の機密性・完全性・可用性を確保します。

3. リスクの識別と対応

当社は、情報資産に対するリスクを定期的に特定・評価し、技術的・組織的な対策を講じてリスクを適切に管理します。
また、リスク状況の変化に応じて速やかに対応し、継続的な改善を行います。

4. 人材の育成と意識向上

当社の役員・従業員および業務委託者は、情報セキュリティの重要性を十分に理解し、
定期的な教育・訓練・啓発活動を通じて高いセキュリティ意識を維持します。

5. 法令・規範・契約の遵守

当社は、情報セキュリティに関連する法令、規範、ガイドラインおよび契約上の義務を遵守します。
また、関係省庁・業界団体が定める最新の基準やガイドラインを踏まえ、適正な管理を行います。

6. 技術的および物理的保護対策

当社は、アクセス制御、暗号化通信、監視・検知、バックアップおよび災害対策等を適切に実施し、情報資産を不正アクセス、漏えい、改ざん、紛失、破壊などの脅威から保護します。

7. クラウドサービス・委託先の管理

当社は、クラウドサービスや業務委託先に対しても、契約や監査等を通じて十分な情報セキュリティ水準を確保します。
また、サプライチェーン全体にわたるセキュリティ対策を推進します。

8. インシデント対応および事業継続

当社は、情報セキュリティインシデントが発生した場合には、迅速かつ適切に対応し、
原因分析・影響評価・再発防止策を実施します。
また、自然災害や障害発生時にも重要業務を継続できるよう、事業継続計画（BCP）を策定し運用します。

9. 継続的改善

当社は、社会・技術環境・法令の変化に対応し、情報セキュリティマネジメント体制を継続的に見直し・改善します。

制定日：2025 年 11 月 4 日
株式会社 AIHOBS
代表取締役　八田　泰秀