

情報セキュリティ基本方針

oVice 株式会社（以下「当社」といいます。）は、バーチャル空間「ovice」及び複数の人工知能（AI）を横断的に利用することができるプラットフォームサービス「AI Pass」並びにこれらに関連する各サービス（無償でのトライアル利用を含み、以下、これを総称して「本サービス」といいます。）を運営しています。当社は、本サービスの提供にあたり、お客様からお預かりした情報資産に対する機密性、完全性、可用性の確保・向上に努め、当社の従業員が当該情報資産の価値と重要性を認識するとともに、当該情報資産を事故・災害・犯罪などの脅威から守ること、そして、お客様が利用する当社の情報システム環境を可能な限り安定的に維持する責務があると認識しています。お客様並びに社会の信頼に応えるべく、以下の方針に基づき、全社で情報セキュリティに取り組みます。

1. 経営陣の責任

当社は、経営陣主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2. 社内体制の整備

当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。これには、経営陣が参画する組織を確立し情報セキュリティの改善・向上に努めること、お客様の情報資産の管理に対する役割と責任を定め、情報セキュリティマネジメントシステムの運用に万全を期すこと、情報セキュリティマネジメントシステムを定期的にレビューし、その有効性を評価し、必要に応じ改善を行うとともに、定められた規則に適合していることを明確にするための定期的な内部監査を実施すること、そして、お客様の情報資産に対するリスクを評価する基準を定め、当該情報資産のリスクを明らかにし、リスク対応計画を実施すること、が含まれます。

3. 従業員の取組み

当社の従業員は、情報セキュリティのために必要とされる知識や技術を習得し、情報セキュリティへの取り組みを確かなものにします。これには、本情報セキュリティ基本方針の適用範囲にある情報資産に関わる全て従業員等に対し、業務に必要な力量を

持つための教育と情報セキュリティについての基本方針、関係する基準や手順について教育及び訓練を実施することが含まれます。

4. 法令及び契約上の要求事項の遵守

当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。

5. 違反及び事故への対応

当社は、情報セキュリティに関わる法令違反、契約違反及び事故や災害等が発生した場合には適切に対処し、再発防止に努めます。これには、平時においてセキュリティインシデントの発生を前提としたインシデント対応のポリシーや体制及び対応手順を予め整備し、有事の際には組織としてエスカレーション・対応・復旧・通知という一連の対応を迅速に実施できるよう取り組むことが含まれます。

oVice 株式会社

代表取締役 ジョン・セーヒョン

【2021年2月1日制定】

【2025年9月5日改定】