情報セキュリティ基本方針

株式会社アルカディア

代表取締役社長　天白　成一

株式会社アルカディア（以下「当社」といいます）は、防災・減災ソリューションを提供するクラウドサービス事業者として、お客様からお預かりする情報および当社が取り扱う情報資産を適切に保護することが、重要な社会的責務であると認識しています。

特に、防災・減災に関する情報は、住民の生命、身体および財産の保護や、自治体等の災害対応に深く関わる重要な情報です。当社は、これらの情報資産を安全に管理し、サービスを安定的かつ継続的に提供するため、情報セキュリティの確保を重要な経営課題の一つと位置付けています。

当社は、情報セキュリティに関するリスクを適切に管理し、お客様に安心して当社サービスをご利用いただくため、次のとおり情報セキュリティ基本方針を定めます。経営者の責任のもと、役員および従業員は本方針を理解し、遵守します。

1. 情報資産の保護

当社は、お客様からお預かりした情報および当社が保有・管理する情報資産について、機密性、完全性および可用性を確保するため、情報資産の重要性やリスクに応じた適切な情報セキュリティ対策を講じます。また、不正アクセス、情報漏えい、改ざん、滅失、毀損等の防止に努めます。

2. 法令およ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連する法令、規制、国が定める指針および業界ガイドラインを遵守します。また、お客様との契約その他当社が受け入れた情報セキュリティ上の要求事項を確認し、これを遵守します。

3. 情報セキュリティ管理体制の整備と経営者の責任

当社の経営者は、情報セキュリティマネジメントシステム（ISMS）の確立、実施、維持および改善に責任を持ち、必要な経営資源を確保します。また、情報セキュリティに関する役割、責任および権限を明確にし、社内に周知します。クラウドサービスの提供に関わる委託先および関係事業者についても、リスクに応じて必要かつ適切な情報セキュリティ管理を求めます。

4. 情報セキュリティ目標の設定と教育・啓発

当社は、本方針に基づき、情報セキュリティ目標を設定し、その達成状況を定期的に評価します。また、役員および従業員に対して情報セキュリティに関する教育・研修を継続的に実施し、情報資産の適切な取扱いを徹底するとともに、情報セキュリティ意識の向上に努めます。

5. 情報セキュリティインシデントへの対応

当社は、情報漏えい、不正アクセス、サイバー攻撃、システム障害その他の情報セキュリティインシデントが発生した場合、速やかに状況を把握し、被害の拡大防止およびサービスの復旧に努めます。原因究明および影響範囲の特定にあたっては、システムログや関連データ等を適切に保全し、必要に応じてデジタルフォレンジック等の専門的な調査手法や外部専門機関を活用します。調査結果を踏まえて再発防止策を講じるとともに、法令および契約上の要求事項に従い、関係機関およびお客様への報告・連絡を適切に行います。

6. 点検・監査および ISMS の継続的改善

当社は、情報セキュリティ対策および ISMS の運用状況について、定期的に監視、測定、分析および評価を行い、内部監査等を通じてその有効性を確認します。評価や監査で明らかになった課題については、必要な是正措置および改善措置を講じ、ISMS の適切性、妥当性および有効性の継続的な改善に努めます。

7. 情報セキュリティ対策の継続的な見直し

当社は、サイバー攻撃等の新たな脅威、情報技術の進展および事業環境の変化を踏まえ、リスク評価の結果に応じて技術的・組織的な安全管理措置を見直し、情報セキュリティ対策の維持・向上に努めます。

本方針は、役員および従業員に周知するとともに、必要に応じて社外に公開します。また、事業内容や情報セキュリティを取り巻く環境の変化等を踏まえ、定期的に見直します。

制定　平成 26 年 7 月 1 日

改定　平成 29 年 10 月 31 日

改定　令和元年 8 月 26 日

改定　令和 5 年 11 月 20 日

改定　令和 8 年 11 月 20 日