情報セキュリティポリシー

1. 目的

- 本ポリシーは、当社が取り扱う顧客情報および業務上の情報資産の機密性、完全性、可用性を確保し、情報セキュリティ事故から顧客および事業を保護することを目的とする。

2. 適用範囲

- 本ポリシーは、昭和オートサービス株式会社の本社、およびカーベルふじみ野店に勤務する　全従業員（正社員、契約社員、派遣社員を含む）、外部委託先が利用する全ての情報資産（紙媒体、電子データ、システム、端末等）に適用する。

3. 定義

- 情報資産：顧客情報、契約情報、見積書、システム、ネットワーク、端末、紙文書等を含む。
- 個人情報：氏名、住所、電話番号、契約内容等、個人を特定し得る情報。
- 機密情報：業務上秘匿が必要な情報（顧客の保険契約内容、引受条件、内部方針等）。

4. 基本方針

- 当社は、情報資産の適切な管理と保護を経営上の重要課題と位置づけ、以下を実施する。
  - 情報セキュリティに関する法令・規範（個人情報保護法、金融関連ガイドライン等）を順守する。
  - 必要なリスク評価を実施し、リスク低減のための対策を講じる。
  - 従業員に対する教育・啓発を定期的に実施する。
  - セキュリティインシデントが発生した場合は迅速に対応し、再発防止策を講じる。

5. 組織と責任

- 経営陣：本ポリシーの承認、資源の確保、体制整備の推進。
- 情報セキュリティ責任者（CISOまたは管理者）：ポリシーの実行管理、監査、教育計画の策定。
- 部門長：自部門における方針遵守とリスク管理。
- 全従業員：本ポリシーおよび関連手順の遵守義務、異常発見時の報告義務。
- 外部委託先：契約にて本ポリシー準拠を要求し、適切な管理を実施させる。

6. 資産管理

- 情報資産の台帳を作成・維持し、所有者を明確化する。
- 資産ごとに分類（機密・社内限定・公開）と取り扱い基準を定める。

7. 人的セキュリティ

- 採用時・退職時における機密保持誓約の取得とアクセス権の適切な付与・剥奪を行う。
- 定期的なセキュリティ教育（年1回以上）とフィッシング等の訓練を実施する。

8. アクセス管理

- 最小権限の原則に基づき、ユーザーIDとアクセス権を付与する。
- パスワードポリシー（長さ、複雑さ、変更周期）を定める。可能な限り多要素認証（MFA）を導入する。
- 退職者・異動者の権限削除手続きを定める。

9. 端末・ネットワーク管理

- 社内ネットワークと外部ネットワークの境界制御を実施する（FW、IPS/IDS等）。

- ノートPC、スマートフォン等のモバイル端末に対してはMDMやデバイス暗号化、リモートワイプを導入する。
- 公衆Wi-Fi利用時のルール（VPN利用等）を定める。

10. データ保護（個人情報・機微情報）
- 顧客情報は業務目的以外では利用しない。第三者提供は法令または顧客同意に基づく。
- 保存データは適切に暗号化（保存時・送信時）する。
- データ保持期間と安全な廃棄手順（物理破壊、データ消去）を明確にする。

11. システム開発・変更管理
- システム導入・変更は影響分析、承認、テストを経て実施する。
- 外部ソフトウェア導入時は脆弱性評価とライセンス確認を行う。

12. 脆弱性管理・パッチ適用
- 定期的な脆弱性スキャンと優先順位付けに基づくパッチ適用を行う（重要パッチは速やかに適用）。

13. ログ管理・監視
- 重要システムのアクセスログ・操作ログを取得し、一定期間保存・定期レビューを行う。
- 不正アクセスや異常を検知した場合の監視体制を整備する。

14. インシデント対応
- インシデント発生時の報告ルート、初動対応、原因調査、顧客通知基準、再発防止策を定めたインシデントレスポンス手順を維持する。
- 関係当局（必要時：監督官庁、個人情報保護委員会等）への報告要件を遵守する。

15. 災害対策・事業継続（BCP）
- 重要業務の優先順位付け、代替手段、データバックアップ、復旧目標（RTO/RPO）を定義し、定期的にBCP訓練を行う。

16. 外部委託管理
- 業務委託先には契約でセキュリティ要件を明示し、監査や評価を実施する。
- 外部クラウド利用時は契約条件、データ保護措置、責任分担を明確にする。

17. 監査・見直し
- 定期的な内部監査と、必要に応じて第三者監査を実施する。
- 本ポリシーは年1回以上、または大きな事業環境変化時に見直しを行う。

18. 遵守事項・罰則
- 本ポリシー違反は懲戒の対象となる場合がある。具体的な処分は就業規則に従う。

19. 関連文書
- 個人情報保護規程、アクセス制御基準、パスワード運用規程、インシデントレスポンス手順、災害対応計画等。

付録（サンプル）
- 付録A：役割と責任（例：CISO、情報管理責任者、各部門長、IT管理者）

- 付録B：データ分類表（機密 / 社内限定 / 公開）と取り扱いルール
- 付録C：インシデント報告書フォーマット（発生日、影響範囲、初動、対応履歴、再発防止）
- 付録D：アクセス権付与・削除申請フォーム
- 付録E：セキュリティ教育計画（頻度、対象、実施方法）

当社は、顧客情報及び当社が保有する全ての情報資産を保護するため、適切な情報セキュリティ管理体制を構築し、関連法規の遵守、リスク評価、技術的・組織的対策の実施、従業員教育、及び監査を継続的に行う。

2025年10月1日改定
昭和オートサービス株式会社