最終更新日：2025 年 10 月 20 日

情報セキュリティ基本方針（改訂版／ISO 対応）

昭栄印刷株式会社（以下、「当社」）は、印刷事業およびデジタル・クリエイティブサービスを通じてお客様の大切な情報をお預かりし、社会の信頼の上に成り立つ事業活動を行っています。この責任を十分に認識し、情報資産をあらゆる脅威から保護し、安心・安全なサービスを提供するため、ここに情報セキュリティ基本方針を定め、全社を挙げて推進いたします。

1. 目的

当社は、顧客情報・取引先情報・従業員情報および自社が保有する全ての情報資産を適切に管理し、不正アクセス・漏えい・改ざん・破壊・紛失等のリスクから保護することを目的とします。あわせて、情報セキュリティマネジメントシステム（ISMS）を構築し、継続的な運用改善を図ります。

2. 適用範囲

本方針は、当社が保有または管理するすべての情報資産（紙媒体・電子データ・システム・ネットワーク・設備等）に適用します。また、当社の役員、従業員、契約社員、派遣社員、外部委託先など、当社業務に関わるすべての関係者に対して適用します。

3. 体制と責任

当社は情報セキュリティ管理責任者（CISO）を設置し、情報セキュリティ委員会を中心として全社的な管理体制を整備します。経営層は本方針の実施と維持に必要な資源を提供し、定期的なレビューを行います。各部門責任者は自部門の情報資産管理に責任を持ち、全社員がその重要性を理解し、日常業務において遵守します。

4. リスクマネジメント

当社は、情報資産に対するリスクを特定・分析・評価し、発生可能性および影響度を踏まえて許容可能なリスク水準を設定します。そのうえで、適切な対策を講じ、リスク低減と再発防止に努めます。

5. 法令・規範の遵守

当社は、個人情報保護法、不正アクセス禁止法、著作権法、マイナンバー法などの関連法令、およびお客様との契約・社内規程を遵守します。個人情報の取扱いに関しては、別途定める「個人情報保護方針」に基づき、より厳格な管理を行います。

6. 情報資産の管理

当社は、情報資産を重要度に応じて分類し、アクセス権限・利用目的・保存期間を明確に定め、適切に管理します。情報資産は機密度に応じて「極秘」「社外秘」「社内限定」等に区分し、最小権限の原則に基づいてアクセスを制限します。

7. 物理的セキュリティ

当社は、施設への入退室管理、監視カメラ、鍵管理などの物理的対策を講じ、情報資産の不正持ち出し、盗難、紛失を防止します。また、印刷物や原稿等の保管・廃棄においても、セキュリティ基準に従って適切に処理します。

8. 外部委託先の管理

当社は、外部委託先に対して情報セキュリティに関する契約を締結し、必要に応じて監査・評価を実施します。委託先で発生した事故が当社へ影響を及ぼさないよう、管理体制を整備し、是正指導を行います。

9. 教育・啓発

全社員および関係者に対し、定期的な情報セキュリティ教育・訓練を実施し、意識向上と知識定着を図ります。入社時・異動時・退職時には機密保持誓約を行い、情報漏えい防止を徹底します。

10. インシデント対応

情報漏えいや不正アクセス等のインシデントが発生した場合、社内通報フローに基づき、速やかに情報セキュリティ管理責任者へ報告します。被害範囲の特定、原因分析、対策実施および記録保管を行い、再発防止策を講じます。必要に応じてお客様および関係当局への報告を行います。

11. 継続的改善

当社は、内部監査を定期的に実施し、情報セキュリティマネジメントシステムの有効性を評価します。社会環境、技術動向、法令改正等の変化に応じて PDCA サイクルを回し、継続的な改善を推進します。

12. 見直し

本方針は、事業環境や社会的要請の変化に応じて随時見直しを行い、常に最適な内容を維持します。

制定日：2025 年 10 月 20 日（改訂）

昭栄印刷株式会社

代表取締役社長　坂井 雅之