基本理念

今後 ISMS 認証取得をセキュリティ要求事項とする当組織の特定顧客との取引継続及び拡大、並びに自社の重要な情報資産とお客様の重要な情報資産の適切かつ妥当な保護による事業機会の増大のため、ISO/IEC27001:2013 に準拠した情報セキュリティマネジメントシステムを導入・運用することにより事業損害の最小化と事業継続を図る。

情報セキュリティ基本方針

（1）事業上及び法令上並びに契約上の要求事項への準拠

当組織は、システム開発という事業上の要求事項に準拠すると同時に、情報セキュリティに関する法令、規制、およびその他の規範を遵守するものとする。また、当組織の従業者は、取引先との契約事項や社内の情報セキュリティ関連規程及び運用手順書に従い行動するものとする。

（2）教育及び訓練の実施

当組織は、当組織のすべての従業者に対して、情報セキュリティの重要性を認識させるとともに、情報資産の適切な取り扱いを確実にするために、定期的に教育及び訓練を実施するものとする。

（3）体系的なリスクアセスメントの実施

当組織は、当組織が保有する情報資産に対するリスクを評価するための基準を明確にし、体系的なリスクアセスメントの構造を定義するとともに、定期的にリスクアセスメントを実施するものとする。

（4）適切な管理策の実施

当組織は、情報資産を漏えい・毀損・滅失等の脅威から保護するため、次に掲げる適切な管理策を実施するものとする。

- 物理的セキュリティ対策（情報システムを設置する施設への不正な立入り、情報資産への不正な物理的アクセス、損傷、妨害等を防ぐための物理的な対策）
- 人的セキュリティ対策（情報セキュリティ対策に関する権限および責任を定め、すべての従業者に本基本方針の内容を周知徹底する等十分な教育および啓発が行われるように必要な対策を講ずる）
- 技術および運用におけるセキュリティ対策（情報資産を、ネットワークを介した外部からの不正アクセス、ウィルス等の不正ソフトウェア等から適切に保護するため、情報資産への接続および操作の制御、ネットワーク管理等に関する技術面の対策を講ずるとともに、システム開発等の外部委託、ネットワークの監視および本基本方針の遵守状況の確認等に関する運用面の対策を講ずる）

（5）事業継続管理の実施

当組織は、当組織の事業活動の中断に対処するとともに、重大な障害または災害の影響から重要な情報資産並びに業務手続を保護するために、事業継続管理のための枠組みを確立し、

事業継続計画を作成、維持するものとする。

（6）情報セキュリティ事件・事故発生の予防並びに是正

当組織は、リスクアセスメントの結果に基づき、情報セキュリティ事件・事故に対する適切な予防処置を講じるものとする。また、万一情報セキュリティ事件・事故や違反が発生した場合には速やかに適切な是正処置を講じるものとする。

制定日：2005 年 6 月 7 日

代表取締役社長　石金正己