

情報セキュリティマネジメントシステム基本方針

1 目的

この文書は、株式会社クロスフィールド（以下、「当社」という）の情報セキュリティマネジメントシステム（以下、「ISMS」という）を構築するにあたっての基本的な方針を明らかにしたものである。

当社は、お客様から信頼される企業として、お客様情報のセキュリティに関するインシデントの防止を図ることにより、お客様の信頼確保及び事業損失を最小限に留めることを目的とし、「情報セキュリティマネジメントシステム基本方針」を定める。

従業員に対し情報セキュリティに関する規程・関連事項の周知・教育を徹底し、従業員はそれを遵守しなければならない。

2 情報セキュリティの定義

情報セキュリティとは、機密性、完全性及び可用性を確保し維持することをいう。

- (1) 機密性：許可されていない個人、エンティティ（団体等）又はプロセスに対して、情報を使用不可又は、非公開にする特性。（情報を漏えいや不正アクセスから保護すること。）
- (2) 完全性：資産の正確さ及び完全さを保護する特性（情報の改ざんや間違いから保護すること。）
- (3) 可用性：認可されたエンティティ（団体等）が要求したときに、アクセス及び使用が可能である特性。（情報の紛失・破損やシステムの停止などから保護すること。）

3 適用範囲

【組織】：株式会社クロスフィールド

【施設】：本社（『適用範囲関連資料：フロア図』参照）

【業務】：コンサルティングサービス業務および当社の事業運営に係る管理業務

【資産】：上記業務にかかわる情報資産、経理・人事システム

【ネットワーク】：全社ネットワーク（『適用範囲関連資料：ネットワーク図』参照）

4 実施事項

- (1) 適用範囲の全ての情報資産を脅威（漏えい、不正アクセス、改ざん、紛失・破損）

から保護するための ISMS を確立、導入、運用、監視、見直し、維持及び改善するものとする。

- (2) 情報資産の取り扱いは、関係法令及び契約上の要求事項を遵守するものとする。
- (3) 重大な障害または災害から事業活動が中断しないように、予防及び回復手順を策定し、定期的な見直しを行うものとする。
- (4) 情報セキュリティの教育・訓練を適用範囲すべての社員に対して定期的実施するものとする。

5 責任と義務及び罰則

- (1) ISMS の円滑な推進を図るため、情報セキュリティ委員会を設置する。
- (2) 情報セキュリティ委員会は、情報セキュリティに関するリスクアセスメントの実施、管理策の策定、リスク対策の実施・評価を行う。
- (3) 情報セキュリティの責任は、代表取締役が負う。そのために代表取締役は、適用範囲のスタッフが必要とする資源を提供するものとする。
- (4) 適用範囲のスタッフは、お客さま情報を守る義務があるものとする。
- (5) 適用範囲のスタッフは、本方針を維持するため策定された手順に従わなければならないものとする。
- (6) 適用範囲のスタッフは、情報セキュリティに対する事故及び弱点を報告する責任を有するものとする。
- (7) 適用範囲のスタッフが、お客さま情報に限らず取り扱う情報資産の保護を危うくする行為を行なった場合は、「人的セキュリティ管理規程」に従い処分を行なうものとする。

6 定期的見直し

情報セキュリティマネジメントシステムの見直しは、環境変化に合わせるため定期的実施するものとする。

日付 平成 22年 2月 19日
役職 代表取締役社長
署名 磯貝 光一