情報セキュリティ基本方針書

1 目的

弊社の保有する情報資産は経営資産そのものであり、事業運営および継続のために非常に重要な要素です。その情報の機密性、完全性、可用性を確保することが、経営上の重要な課題となります。

また弊社は、お客様のシステム開発を請け負うこと、お客様のシステムの性能分析・診断のコンサルティングを行うこと、十分なセキュリティ水準を満たしたシステムの開発方法を教育すること、個人情報の登録を伴う安全なコミュニティサイトを運営することなどを事業の中心とする企業であり、その面から鑑みても、情報資産を適切に維持管理することは、対外的な弊社の価値を高めることになり、取引において重要な競争優位性を生むことになります。

お客様との関係において、情報セキュリティ事件・事故が発生した場合は信用の失墜、営業機会の損失などの影響が大きいものとなります。

したがって、弊社は情報やコンピュータおよびネットワークなどの情報システムを情報資産と位置づけて、ISO/IEC 27001 に基づく情報セキュリティマネジメントシステム(ISMS)を確立、導入、運用、監視、レビュー、維持、及び改善することにより、企業の社会的責任を果たすことを目的とします。

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】:株式会社シーマーク
【施設】:本社オフィス
【業務】:エンタープライズ事業部・エリアコミュニティ事業部・経営企画室
【資産】:上記業務、サービスにかかわる書類、データ、情報システム

【ネットワーク】: 全社ネットワーク

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情報セキュリティマネジメントシステムを確立、導入、運用、漢詩、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、定期的な見直しをするものとする。

(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に実施するものとする。

5 責任と義務及び罰則

(1) 情報セキュリティの責任は、代表取締役および経営企画担当取締役が負う。そのために代表取締役および経営企画担当取締役は、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。

(2) 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。

(3) 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。

(4) 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。

(5) 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、社員就業規則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に実施するものとする。

日付 2008/7/17
改訂 2014/9/26
代表取締役社長 山本 高志
経営企画担当取締役 三浦 建太郎

