情報セキュリティ基本方針

制定日：2004 年 4 月 1 日
改定日：2020 年 4 月 1 日
名村情報システム株式会社
代表取締役　嶋﨑 徹夫

1. 目的

この情報セキュリティ基本方針(以下、基本方針)は、当社の情報セキュリティマネジメントシステム(以下､ISMS)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。今後はこの基本方針を ISMS の拠り所として位置づける。

2. 基本声明

基本方針の趣旨は、内部的であるか外部的であるか、故意であるか偶発的であるかを問わずすべての脅威から、当社が保有するもしくは利害関係者から預かった重要な情報資産を適切に保護し当社の事業上の目的を達成することにある。当社においては、情報資産の適切な保護を経営上の重要項目として認識し、必要な経営資源を適切に割り当てる。しかるに、当社の従業員及び利害関係者はその意図を十分に理解し実践する事が望まれる。

3. 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・可用性を保護し維持することを言う。機密性・完全性・可用性とは次のような意味を持つ。

機密性：　アクセスを認可された者だけが、情報にアクセスできることを確実にすること。
完全性：　情報および処理方法が正確であること及び完全であることを保護すること。
可用性：　認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

4. 情報セキュリティの目的

当社の重要な業務は、顧客から依頼を受けて行なわれる情報システムの開発・保守及び運用業務である。このようなことを考慮すると、顧客から提供された情報及び当社において作業を行ない顧客に提供される情報は当社の事業の目的を達成していく上で最大限の注意を払うべき重要な情報である。

この重要な情報及びこれを支える情報機器を保護する事が情報セキュリティの最大の目的である。我々はこの情報にたいして顧客からどのような条件を示されているかを認識しそれを遵守するとともに、その内容がお互いの事業の目的にとって不十分である場合は、適切な提言を行ない、お互いの信頼関係を確固たるものとし、お互いの繁栄を達

成する事にある。

5. 個人情報保護方針

当社は経営上の重要項目である「情報資産の適切な保護」の方針の基、個人情報の保護を重要事項として位置づけ、「個人情報保護方針」を定め実施する。

(1) 個人情報の収集、利用、提供

当社の事業内容及び業務実態に応じた、個人情報を収集・利用・提供するにあたって、適法かつ当社が定めた規程に従い適切に取り扱う。

(2) 安全対策の実施

当社は、個人情報が社外に流出し、不当に改ざんされるトラブルを引き起こさないよう、規程を定め安全対策を実施し、個人情報への不正アクセス、個人情報の紛失、破壊、改ざん、漏えいを予防する。

(3) 権利の尊重

当社は、個人情報に関する個人の権利を尊重し、自己の個人情報について開示、訂正、削除を求められたときは、総務部を窓口として適切に対応する。

6. コンプライアンス

当社に関わる法的、契約上の事項を遵守する事は情報セキュリティの第一歩である。又、顧客との契約に関わる知的所有権についての理解を深めその重要性を認識する事が、顧客からの信頼を勝ち得る為に大変重要であり、以下のような事を徹底する。

(1) 情報セキュリティに関連する契約条件を遵守すること

(2) 就業規則を遵守すること

(3) ISMS で規定した規則を遵守すること

(4) 下記を含む法規制を遵守すること

① 刑法
② 民法
③ 商法
④ 個人情報保護法
⑤ 知的財産権
⑥ 不正競争防止法
⑦ 労働者派遣法
⑧ 暗号に関する各国の規制
⑨ 消防法/同施行令/同施行規則
⑩ 不正アクセス行為の禁止等に関する法律
⑪ 訴訟関連資料
⑫ 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律

7. 社員の責任と義務

基本方針に基づく、ISMS の確立、運用、維持、改善に関する実行主体は情報セキュリティ委員会が担う。情報セキュリティ委員会の活動に対して私は定期的なチェックを行なう。情報セキュリティ委員会より任命された情報セキュリティ管理者は、適切な基準及び実施手順に基づき、基本方針の実施を促進する。すべての従業員及び協力会社は、

本情報セキュリティ基本方針を維持するために策定された手順に従わなければならない。すべての従業員及び協力会社は、事故及び特定された弱点を報告する責任を要する。

8. リスク評価方針

基本方針に基づき当社の状況に適したリスクアセスメントの方法を決定し、これを首尾一貫して適用する事により、本当のリスクの実態や変化が明らかになる。リスクアセスメントの方法は資産価値、脅威及び脆弱性についてその相対的な重みを明らかにし、管理策の内容及び程度を決定する事に通じるものであるべきである。

9. 運用方法

基本方針の運用は運用手順に従い、定期的に内部監査を行い基本方針が遵守されているか確認する。

10. 罰則

当社、顧客、協力会社の情報資産の保護を危うくする故意の行為を行った場合は、懲戒処分/法的処分の対象となる。

11. 関連文書

本文書では以下の具体的な諸基準を参照する。

① 適用範囲宣言書
② リスク分析規程
③ リスク対応計画規程
④ 内部監査規程
⑤ 情報セキュリティ教育規程
⑥ 記録・文書管理規程
⑦ 情報セキュリティ委員会規程
⑧ セキュリティ管理者規程
⑨ システム管理者規程
⑩ 資産分類・資産管理台帳作成規程
⑪ 情報取り扱い規程
⑫ ユーザ規程
⑬ ウイルス対策規程
⑭ 情報セキュリティインシデント報告手続き規程
⑮ 物理的アクセス規程
⑯ 人事規程
⑰ 事業継続管理規程

12. 見直し

(1) 私は、この基本方針を作成し、レビューを行う。
(2) 基本方針は、定期的(年一回)または、必要性が生じた場合に、レビューを行う。また、基本方針の変更が生じた場合、下位(規程/手順書)の見直し、変更が必要な物はレビューを行う。
(3) 基本方針/規程/手順書のレビューが行われた物に対し、妥当性及び有効性を確認する。

以上