ISO27001 の取得について

情報社会が高度化する中、当社は機密情報を含むお客様の大切な情報をお預かりする立場として、情報セキュリティの重要性を認識し、以下に示す ISO 認証を取得し管理体制の強化に努めております。

■認証取得情報

認証取得規格　　ISO27001（情報セキュリティ）
事業者名 株式会社平プロモート
初回登録日　　2009 年 10 月 9 日
認証登録番号　　ASR J0128

■情報セキュリティ基本方針

当社の情報セキュリティ方針を、以下のように定めます。

１．情報セキュリティ宣言

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は、生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏洩、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害にも備える必要がある。

当社は、顧客情報や経営上重要な情報などを多数取り扱っている。また、コンピュータ化・インターネット化が進み、多くの業務が情報システムやネットワークに依存している。したがって、これらの情報資産を様々な脅威から防御することは、顧客及び社員の権利、利益を守るためにも、また、会社の安定的、継続的な運営のためにも必要不可欠である。

これらの状況を鑑み、当社における情報資産に対する安全対策を推進し、顧客からの信頼を確保し、さらなる会社の発展のため、以下の項目に積極的に取り組むことを宣言する。

（1）情報セキュリティ対策に取り組むための全社的な体制を確立する。
（2）情報セキュリティ対策の基準として、情報セキュリティ対策基準を策定し、その実行のための手順等を盛り込んだ実施手順を策定する。
（3）会社の保有する情報資産を適切に管理する。
（4）情報セキュリティに関する事故が発生した場合、またはその予兆があった場合に、速やかに対応するため

緊急時対応計画を定める。

（5）情報セキュリティ対策の実施状況の監査および自己点検等を通して、定期的に対策の見直しを実施する。

（6）すべての社員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって、情報セキュリティ基本方針、情報セキュリティ対策基準および情報セキュリティ実施手順を遵守する。

２．情報セキュリティの目的

情報セキュリティに関して重大な事件・事故(以下、「情報セキュリティインシデント」という)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る。お客様の信頼を保持し、より良い商品と技術、及び、サービスを提供するためには、情報資産に対して適切な安全対策を実施し、紛失、盗難、不正使用や誤用から保護しなくてはならない。よって、従業員がセキュリティに対して高い意識をもち、適切な行動をとることを目的として、本規定の内容に取り組むこととします。

なお、当社の情報セキュリティの目標は次の通りとします。

（1）情報セキュリティインシデントを未然に防止し、発生ゼロを目指す。

（2）万が一情報セキュリティインシデントが発生した場合も、その被害を最小限にとどめ迅速な復旧を行い、また再発を防止する。

（3）情報セキュリティに関する法令、規制その他のガイドラインを遵守する。

上記の目標を持って、情報セキュリティ活動を実施します。

なお、目標の達成度評価は別紙にて行うこととします。

３．情報セキュリティのための方針群

3.1 情報セキュリティ基本方針

1.目的

当社が保有する情報資産を脅威から適切に保護し、情報セキュリティの水準を総合的、体系的かつ継続的に確保することを目的とします。

2.適用範囲

当社の業務遂行エリアを適用範囲とし、その情報資産を取扱うすべての社員等を対象者とします。

3.社員等の義務

情報資産を取扱う社員等は、情報セキュリティの重要性について共通の認識を持ち、社内規程や情報セキュリティに関する法令等を遵守するものとします。もし、違反した場合には当社就業規則の罰則規定を適用します。

4.管理体制

当社は、情報セキュリティに関する管理体制を整備し、情報資産のセキュリティ対策を推進します。

5.情報資産の管理

情報資産を機密性・完全性・可用性の３つの基準にもとづき分類し、重要度に応じたセキュリティ対策を講じます。

6.セキュリティ対策

情報資産の取扱いにあたり、人的、物理的、技術的セキュリティ及び運用面から総合的にセキュリティ対策を講じます。

（1）人的セキュリティ対策

情報セキュリティに関する権限や責任を定めるとともに、情報セキュリティポリシーを理解し、実践するための教育や訓練を計画的に実施します。

（2）物理的セキュリティ対策

電子計算機室への不正な立ち入り、損傷・盗難等から保護するため、入退室管理等の物理的な対策を講じます。

（3）技術的及び運用におけるセキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウイルス対策等を実施します。

7.対策基準の策定

情報セキュリティを実現するために、社員等が遵守すべき事項及び判断等の基準となる基本的要件を明記した情報セキュリティ対策基準を策定します。

8.実施手順の策定

対策基準を満たすために、必要な実務レベルの実施手順を策定します。

9.情報セキュリティインシデント管理

情報セキュリティの事象及び弱点の報告・対処の手順を確立します。また、情報セキュリティインシデントに対し、一貫性を持って迅速かつ効果的に対応できるよう管理します。

10.事業継続管理

災害・故障・過失などの偶発的に発生する事故や意図的な業務の妨害、情報資産の悪用等による事業の中断を許容レベルに抑え、事業の継続を確保します。

11.評価・見直し

情報セキュリティポリシーの遵守状況の点検・評価のため、定期的に監査を行い、見直しを実施します。

12.個人情報保護方針

個人情報保護については、個人情報保護法に準拠した当社の「プライバシーポリシー」に基づき実施します。

3.2 個別方針

1.アクセス制御

（1）当社への入退出は電子錠で管理することにより、情報資産の安全を確保します。

（2）情報システムおよびファイルへのアクセスの資格、権限を明確にし、アクセス権限は、個別のユーザ単位

に設定します。

2.ウイルス対策

（1）ネットワークや各種機器・媒体を経由して侵入するウイルスを水際で防止し、社内に侵入させません。

（2）当社で使用する機器はウイルス対策ソフトを導入し、社外へ持ち出しおよび納入する電子媒体は、その都度ウイルス検査を実施します。

（3）ネットワークより送信するファイルは、事前にウイルスに感染していないことを確かめます。

3.情報の暗号化

暗号化する場合、共通鍵方式により、運用業務の担当者と顧客間で秘密に処理され、当事者以外はアクセスできないように管理します。

4.クリアデスク・クリアスクリーン

（1）机上にある書類は、一般書類と重要書類（データ等）を区別できるように整理します。

（2）重要書類（データ等）は、帰宅時にセキュリティが確保された保管庫等に格納します。

（3）ＰＣ端末やプリンタを使用中に離席する場合、ログオンの状態や、印刷したまま放置しないようにします。ＰＣ端末は、スクリーンセイバーを利用し、直ちに作動させる。長時間、使用しないときにはキーロックや、パスワードをかけるなどの保護対策を実施します。

（4）重要な情報や秘密情報を印刷した場合、出力後、プリンタに放置せず、すみやかに取り除きます。

（5）帰宅あるいは長時間、離席する時は、PC をログオフさせるかシャットダウンします。

5.バックアップ

社内機密情報に関するデータの管理は、定期的にサーバー内のデータをバックアップし、そのログ管理を行います。障害時に迅速に対応できるようにリカバリマニュアルを文書化して管理します。

6.情報の転送

情報の転送においては、その種類、機密度、及び顧客要求事項に従い、その保護方法、転送方法を決定し誤操作等が起きないよう十分に注意して行います。

7.供給者関係のための情報セキュリティ

供給者など外部の関係者が自社の情報資産を利用したり、アクセスしたりする場合には当社の情報セキュリティ方針に従うことを合意し、機密保持契約書などを締結します。

8.セキュリティに配慮した開発のための方針

セキュリティに配慮した開発の推進を行います。開発環境及び試験環境、運用環境は許可されていないアクセスまたは変更のリスク低減のために分離します。

令和 6（2024 年）年 6 月

IT セキュリティ統括責任者

代表取締役　平　知恭