情報セキュリティのための方針群

株式会社フィデア情報総研（以下、「当社」という）はお客様の重要な情報資産をお預かりし、情報処理サービスを提供しております。保有する情報資産を漏洩、改ざん、破壊、紛失、不正アクセス等の脅威から守り、リスクを最小限に抑え適切に保護することが、当社の事業継続に関わる最重要課題のひとつと認識しております。

当社は情報資産の機密性・完全性・可用性の維持・向上に万全を期し、社会とお客様の信頼に応えるため、「情報セキュリティのための方針群」を以下のとおり定め、実施いたします。

「情報セキュリティのための方針群」は、「情報セキュリティ方針」および「個別方針」で構成されています。

情報セキュリティ方針

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**

   データセンタ部門および人事総務部門の情報処理サービス業務を適用範囲とし、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、プライバシーマーク制度（ＪＩＳ　Q15001：2006）に準拠した当社の「個人情報保護基本規程」に基づき実施します。

個別方針

1. **アクセス制御**

（1）データセンタへの入退出は、「テンキー錠」「監視カメラ」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）社外へ持ち出す機器、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。

（4）使用する機器は、定期的にウイルス検査を実施します。

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**

（1）社内機密情報が含まれる情報の通信には、原則電子メールを使用しません。

（2）重要な社内機密情報を含む文書をＦＡＸで送受信する場合には、着信を電話連絡等で確認します。また、送信時には複数人でＦＡＸ番号を確認する等厳重に安全確保に努めます。

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。

制定日：2005 年 9 月 1 日
改訂日：2025 年 4 月 1 日

株式会社　フィデア情報総研
代表取締役社長　石原　敏之