

情報セキュリティマネジメントシステム(ISMS)基本方針

株式会社 FJ ネクストホールディングス
代表取締役社長 永井 敦

1 基本声明

高度情報化社会の急速な発展が経営資源に及ぼす影響を増大させている現在、情報資産を様々な脅威から守ることは、企業の発展において重要な経営課題となっている。社会を構成する一員として情報セキュリティ確保は企業の社会的責務と言えよう。

FJネクストグループの会社(以下、総称して「当グループ」という)は、これらの認識に基づき、経営陣と全ての従業員が情報セキュリティに対して高い意識をもち、法令遵守に止まらずコンプライアンス及びセキュリティ上の規程を遵守した行動を円滑に進めるために、当社の情報セキュリティマネジメントの基本原則として ISMS 基本方針(以下、「基本方針」という)を定め、これを全従業員に周知徹底させ、日々の業務において実践し、情報セキュリティレベルを継続的に改善することを宣言する。

(*)「当グループ」とは、以下のFJネクストグループの会社を指すものとします。

- 株式会社FJネクストホールディングス
- 株式会社FJネクスト
- 株式会社FJネクストレジデンシャル
- 株式会社エフ・ジェー・コミュニティ
- 株式会社レジテックコーポレーション
- 株式会社アライドライフ

(2023年11月30日時点)

2 情報セキュリティマネジメントシステム(ISMS)の目的

当グループは ISMS の目的を下記の通り定めるものとする。

- 2.1 情報セキュリティ事故を未然に防止すると共に、業務の円滑な遂行が可能な情報基盤を確立する。
- 2.2 万一情報セキュリティ事故が発生した場合、その被害の最小化、迅速な復旧、同種事故の再発を防止する。

3 情報セキュリティの意義

情報セキュリティとは、情報の機密性、完全性及び可用性の全てを維持することにあるが、当グループはその中でも特に機密性の維持を最優先事項とし、次いで完全性の維持及び可用性の維持を図るものとする。

4 ISMSの適用範囲

当グループにおけるISMSの対象組織・対象業務・対象資産は、「ISMS適用範囲定義書」に定めるものとする。

5 情報セキュリティの目標

当グループは情報セキュリティの目標を下記の通り定めるものとする。

- 5.1 個人情報保護の徹底

5.2 情報資産の重要度に従った適切な取扱いの徹底

6 ISMS 環境の整備

6.1 適切に情報セキュリティ管理体制を推進・管理するために、統括情報管理者を定め、ISMS の組織と運営体制を整備し、役割と責任の明確化を図る。

6.2 適用範囲における管理対象資産を洗い出し、その資産価値を評価し、又、各資産に関わる脅威及び脆弱性を分析評価し、リスクを評価するに当たっての基軸を確立し、リスクアセスメントを実施する。

6.3 ISMS の確立を行い、組織的なリスクマネジメントを継続的に行う。

7 関連法規等の遵守

事業上の要求事項、法的又は規制要求事項、並びに契約上のセキュリティ義務を特定し、必要に応じて随時参照可能な環境を整備し、コンプライアンス経営を徹底する。

8 情報セキュリティ施策に関する基本方針

当グループの情報資産を保護する「情報セキュリティマネジメント」を実施するために「ISMS マニュアル」、及び当グループの情報資産を、故意や偶発という区別に関係なく、改ざん、破壊、漏洩等から保護する為の管理策をまとめた「情報セキュリティ管理規程」を策定する。

尚、本「基本方針」、「ISMS マニュアル」及び「情報セキュリティ管理規程」を総称して「情報セキュリティポリシー」と呼称する。

8.1 物理的セキュリティ対策

適用範囲への入退出を厳重に管理するとともに、適用範囲内にある情報資産は重要度に応じて施錠を施す等の対策を講じる。

8.2 人的セキュリティ対策

従業員が情報セキュリティの重要性を認識の上、情報セキュリティポリシーを理解し、遵守するため、十分な教育・訓練及び啓発が図られるように必要な対策を講ずる。

8.3 技術的セキュリティ対策

不正アクセス等から情報資産を適切に保護するため、情報システム及びネットワークの管理、情報資産へのアクセス制御、情報システムの開発・導入の基準、コンピュータウイルス対策等の必要な対策を講ずる。

8.4 運用におけるセキュリティ対策

情報セキュリティポリシーの実効性を確保し、当社の情報システムのセキュリティレベルを保持するために、情報セキュリティポリシー遵守状況の確認等の対策を講ずる。また、緊急事態が発生した際の迅速な対応に必要な連絡体制を確保するとともに重要な情報システムについては、緊急対応計画等を作成する。

9 評価・見直しの実施

9.1 情報セキュリティポリシーが遵守されていることを確認するため、定期的に情報セキュリティ実施状況の検証(内部監査)を行う。

9.2 適用範囲並びにセキュリティ対策の有効性及びリスクアセスメントの方法に関して、定期的にレビューする。

10 違反への対応

10.1 従業員は、情報セキュリティポリシーを遵守し、ISMS の維持、向上に努めなければならない。

10.2 情報セキュリティポリシーに故意又は重大な過失によって違反した場合は、「就業規則」に基づき、懲戒処分等の対象とする。

以 上

2005年4月11日制定
2023年11月30日改定