ISMS 基本方針

2025 年 1 月 20 日
代表取締役社長　田中　雅貴

1. 目的

当社では、情報化を積極的に推進し、情報ネットワーク事業を行う企業であり、また、顧客の重要な情報を預かり、サービスを提供している。

一方で、情報資産を脅威にさらす各種要因が社会的にも注目を集めており、当社としても情報セキュリティを確立し、信頼のおける製品、サービスを開発、販売することが必要である。不正アクセスや災害等の脅威によって何らかの被害が引き起こされた場合、損害賠償はもちろんのこと、当社のイメージや信頼を著しくそこなう結果となる。このようなことに鑑み、セキュリティに関する事件・事故の防止を図ることにより、当社の信頼確保及び事業損失を最小限に留めることを目的とする。

2. 原則

当社は「1. 目的」にしたがい、当社の ISMS を JIS-Q-27001:2023 に則って構築し、管理する。

3. 適用範囲

社長、従業員、当社の情報資産を利用するすべての者を対象とする。

当社の管理下にある以下の事業活動及び外部委託情報設備に係わる全資産を対象とする。

a) 組織

株式会社　カルク

b) 施設

本社　〒409-3812　山梨県中央市乙黒 158-2

支社　〒900-0015　沖縄県那覇市久茂地 2-8-7　久茂地 KM ビル 3F

c) 対象者

社長及び全社員

d) 業務

本社

1) 顧客要求事項に基づくセキュリティサービスの設計・開発・構築・運用・保守・監視
2) 顧客要求事項に基づくネットワークシステムの設計・開発・構築・運用・保守・監視
3) 顧客要求事項に基づくソフトウェアの設計・開発・導入・保守
4) 顧客要求事項に基づく情報機器の販売・設置・保守

支社

1) 顧客要求事項に基づくソフトウェアの設計・開発・導入・保守

e) 資産

上記業務、サービスに関わる資産

f) ネットワークセキュリティ境界

1) 当社敷地内ネットワーク

2) 監視目的で社外に設置された当社資産及びその間を結ぶネットワーク

4. 情報セキュリティの定義

情報セキュリティとは情報資産の機密性、完全性および可用性を維持することである。

a) 機密性

アクセスを許可された者だけが情報にアクセスできる事を確実にすること。

b) 完全性

情報及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。

c) 可用性

許可された利用者が、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。

5. 実施事項

a) 適用範囲の情報資産を脅威から保護するための情報セキュリティマネジメントを確立、導入、運用、監視、見直し、維持及び改善するものとする。

b) 情報資産を扱うすべてのものに対し、情報セキュリティの教育を定期的に行うこととする。

c) 当社の情報セキュリティが侵害されたと思われる事象が判明した場合は、速やかに準備された対応方法に従って対応を行う。

6. 義務及び責任

a) 社長の義務

社長は情報セキュリティマネジメントシステムへの支持・支援を表明し、率先して情報セキュリティマネジメントを推進しなければならない。

また、ISMS 委員会を設置し、ISMS 委員会は情報管理セキュリティ責任者及び各部門から ISMS 委員を代表者として任命する。代表者は各部門における ISMS の推進に努めること。

b) ISMS 委員会の義務

ISMS 委員会は全社的に ISMS の推進を図り、主な役割として以下がある。

・情報セキュリティマネジメントシステム文書の配布

・情報セキュリティマネジメントシステム遵守状況の評価及び改訂

・監査結果の評価及び改訂

c) 従業員の義務

当社従業員は、情報資産を扱う上で、業務利益の維持・向上および顧客満足のために「情

報セキュリティ基本方針」、「ISMS マニュアル」および情報セキュリティの各手順書に応じ行動する。また、これに違反した者は、その結果について責任を負わなければならない。また直接情報を持たない資産であっても、資産を破損させる事の無い様に、備品は大切に取り扱わなければならない。

7. 法的要求事項への準拠及び義務

当社は、法令、その他の規範及びガイドラインに基づいて法的要求事項及び契約上のセキュリティ義務を順守することを確実にする。

8. 違反時における罰則

当社は、ISMS 基本方針の違反者に対し、厳格な処置をとることとする。

情報セキュリティ管理責任者は ISMS 基本方針に違反した事項の重要度を評価し、適切な処置を講じることとする。

罰則の決断は社長が行う。

9. 執行期日

本方針は、2025 年 1 月 20 日より施行する。マネジメントレビューで社長が見直し、必要があれば更新を行う。

見直しの際には、情報セキュリティの目標の適合性および達成のレビューを行い、必要に応じて更新を行う。