情報セキュリティ基本方針

【情報セキュリティポリシー】

１．全般的認識及び原則

当社は前述の経営陣から発せられた言葉に則り、当社のＩＳＭＳを日本産業規格 情報セキュリティマネジメントシステム-要求事項（JIS Q 27001：2023）に準拠して、構築、運営管理する。

２．体制

当社は、経営陣直轄の組織として「ＩＳＭＳ推進委員会」を設置し、情報セキュリティを全社総合的に調整、推進する体制を整える。代表者は、最終的な責任者としてマネジメントレビューを実施する。

３．法的要求事項の遵守

当社ＩＳＭＳの確立及び運営管理にあたっては、事業上及び法令又は規制の要求事項、並びに契約上のセキュリティ義務を考慮する。

４．ＩＳＭＳの確立及び維持

当社のＩＳＭＳは本方針に従い確立及び維持する。また、当社の戦略的なリスクマネジメントの状況と調和を取る。

５．情報セキュリティ目的

ＩＳＭＳ推進委員会は､経営陣から年度当初に発せられる情報セキュリティ目的(ＩＳＭＳ目標)を達成するために計画を策定し、組織全体への展開を図る。ＩＳＭＳ組織要員は目標達成に向けて自らの活動を明確にし、積極的に活動するものとする。

６．リスク評価の基軸

通常想定できない「戦争」､「テロ活動」､「ライフラインの長期停止」等についてのリスクは、経営陣が保有するが、一般的に考えられる脅威、脆弱性については、可能な限り対応するものとする。また、情報セキュリティにおける３要素（機密性、完全性、可用性）については、その重要性を同等と考えリスク評価するものとする。

７．リスクマネジメント

ＩＳＭＳ推進委員会は、リスクマネジメントを的確に行うために、リスクマネジメントについての手順書を定め、ＩＳＭＳ組織要員全員で遵守する。ＩＳＭＳ推進委員会は、資産に対する脅威と脆弱性を識別し、判明したリスクを正当な規準を用いてリスク対応を評価する仕組みを確立し、定期的にアセスメントを実施するものとする。

８．資産の管理と取扱い

ＩＳＭＳ組織要員は、組織の業務上で必要かつ重要な資産を明確化し、適切な保護及び維持の仕組みを構築するものとする。

９．情報へのアクセス管理

ＩＳＭＳ組織要員は、情報のアクセスについて以下の管理を行う。

・情報の取り扱いに関して、各組織と従業員の職務権限を明確に定める。

・情報へのアクセス権限は、情報の種類および業務に応じて真に必要な者に限定して付与する。

・情報へのアクセスの際は、ユーザＩＤ・パスワード等による本人の認証を行う。

・情報へアクセスした場合、またはデータベースに変更を加えた場合等は、その証跡を記録し、一定期間保有する。

１０．入退室管理

外部からの不審者、入退権限のない者の侵入等を防ぐため『入退室管理規程』により管理する。

１１．業務委託先の管理

業務委託は、情報保護・セキュリティの観点から業者選定基準を設け、十分な審査を経て適格な相手先を選定する。また、委託契約等において情報の適切な管理のための必要な措置、秘密保持、再委託先の管理、検査への協力等情報の管理に関する事項について定める。

１２．情報の保有期間と廃棄又は返却

情報の種類毎に保有期間を定め、保有期間を経過した情報は定期的かつ安全・確実に廃棄又は返却する。

１３．教育・訓練

ＩＳＭＳ組織の要員は、職務に応じて必要な情報セキュリティに関する教育を定期的に受講する。

１４．内部監査

ＩＳＭＳについての内部監査を定期的に行い、是正等が必要な場合はそれらを積極的に実施する。

１５．ＩＳＭＳ組織要員に対する罰則

ＩＳＭＳ組織要員が、本方針及び情報セキュリティの関連規程に違反する行為を発見した場合は、ＩＳＭＳ推進委員会に報告する。

報告を受けたＩＳＭＳ推進委員会は、報告内容を協議し、以下の対応を行う。

【違反内容が軽微な場合】

・代表者の注意、指導、訓戒としその記録を残す。

【違反内容が故意、重過失の場合】

・従業員の場合は、当社が定める『就業規則』や『誓約書』の定めを適用する。

・役員の場合は、役員会の審議に従って対処する。