須賀川市情報セキュリティ基本方針

今般の新型コロナウイルス感染症の拡大に伴い、人々の行動が制限される中、ＳＮＳを利用した情報の発信やコミュニケーションの多様化によって、社会の在り方や人々の生活様式が大きく変わりつつあり、行政においても、デジタル化が急速に進展しています。

一方で、情報資産の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊、改ざん等の事故が多数発生しており、職員及び外部委託事業者による誤操作などを起因とするシステム運用の機能不全に陥る事故も発生しております。

市は、市民の個人情報や行政運営上重要な情報などを多数取り扱っている中で、電子自治体の構築が進み、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ことから、これらの情報資産を様々な脅威から防御することは、市民の権利、利益を守るためにも最優先課題であり、行政の安定的、継続的な運営のためにも必要不可欠です。

こうした状況を十分に認識し、環境の変化や技術の進歩に的確に対応するため、今回、国による「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定に併せて本市における、情報セキュリティ対策への取組を更に実効性あるものとするため、情報セキュリティポリシーの見直しを行いました。

行政サービスの基盤となる情報資産を守り、市民から信頼される市政経営を実現するため、全組織・全職員が一丸となって、情報セキュリティ対策に取り組みます。

【情報セキュリティポリシーの基本的な考え方】

１　情報セキュリティマネジメントシステムの体制整備

「情報セキュリティ委員会」の体制としては、最高情報統括責任者（ＣＩＯ）、最高情報セキュリティ責任者（ＣＩＳＯ）、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム責任者、情報システム管理者を任命するとともに、情報セキュリティインシデントに迅速に対処するため、ＣＳＩＲＴ※を組織化します。

※ＣＳＩＲＴ（Computer Security Incident Response Team）とは、コンピュータセキュリティにかかるインシデントに対処する組織。
インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集し、分析し、対応方針や手順の策定などの活動をする。

２　情報セキュリティ対策基準の策定

具体的な順守事項、判断基準等を定めた対策基準を策定します。

３　情報セキュリティ実施手順の策定

具体的な情報システム又は業務において、どのような手順に従って実行していくかを定めた実施手順を策定します。

４　研修・訓練の実施

全職員に対し、定期的な研修・訓練を実施します。

また、情報セキュリティの機密性、並びに適正な情報の取扱い及び管理について、周知徹底を図ります。

5　情報セキュリティインシデント、及び情報セキュリティアクシデントへの対応

職員は、日常において情報セキュリティインシデント（潜在的事例）の発見に努めます。

発見した場合は、インシデントレベルにより、本市が定めた報告体制に基づき、適正な対応を段階的に進めます。

重大な情報セキュリティインシデントの場合は、情報セキュリティ委員会で協議を行い、対応について決定します。

情報セキュリティアクシデント（事件・事故となった場合）は、情報セキュリティ委員会で被害の特定、対応方針の決定、被害者への連絡及び関連機関への報告を行うとともに、再発防止策を定めます。

また、これらの対応をＣＳＩＲＴにより迅速に対応します。

6　事業継続の確保

偶発的に発生する、災害、故障及び過失、並びに意図的に発生する情報の悪用等による事業の中断を可能な限り抑えるため、全職員が高い情報セキュリティ順守の意識を持ち、事業の継続を確保します。

7　継続的改善

情報セキュリティポリシーの遵守状況を定期的に監査するとともに、環境の変化及び技術の進歩に的確に対応し、基本方針、対策基準、実施手順の見直しを適宜行います。

8　法令等の順守

職員は、本市が定めた情報セキュリティポリシー、関連する法令、市例規等を順守します。

また、違反する行為があれば厳しく対処するとともに、再発防止策を定め、適正な情報管理に努めます。

令和４年４月１日

須賀川市長　橋本克也