須賀川市情報セキュリティ基本方針

今般、クラウドサービスの普及やＡＩ技術の発展に伴い、社会の在り方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、多くの業務が情報システムやネットワークに依存しており、これらに対する脅威に備えるとともに、情報資産を適正に管理することが最優先課題となっています。

こうした状況を踏まえて、環境の変化や技術の進歩に的確に対応するため、市では、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」に基づき、必要に応じて情報セキュリティポリシーの見直しを行っていきます。

また、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　定義

（１）ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器をいう。

（２）情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（３）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（４）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（５）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（６）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（７）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（８）マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（９）LGWAN 接続系

LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

（10）インターネット接続系

メール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（11）通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（12）無害化通信

メール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

2　対象とする脅威

情報資産に対する脅威として以下を想定し、情報セキュリティ対策を実施します。

（１）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３）地震、落雷、火災等の災害によるサービス及び業務の停止等

（４）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

3　適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局及び地方公営企業とします。

（２）順守する職員

本基本方針は、雇用の形態及び職位に関わらず、又は市の業務に日常的若しくは非日常的に従事するかに関わらず、市が所管する情報資産を取り扱う正規職員、会計年度任用職員（以下「職員等」という。）が順守します。

4　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」として、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し、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。

5　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。

6　情報セキュリティ実施手順の策定

情報システム又は業務における、具体的な手順を定めた実施手順を策定します。

7　研修・訓練の実施

職員等に対し、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。

8　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

職員等は、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。

9　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､職員等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。

10　継続的改善

情報セキュリティポリシーの順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。

11　法令等の順守

職員等は、情報セキュリティの重要性について共通の認識を持ち、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。

12　その他

上記のほか、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趣旨に則った対応をするよう努めます。

令和８年４月１日

須賀川市長　大字 正晃