野々市市情報セキュリティに関する要領

目次

第１章　総則

（趣旨）

第１条　この要領は、本市が保有する情報資産の機密性（利用を許可された者だけが情報の閲覧、更新等をすることができることをいう。以下同じ。）、完全性（情報源が明らかで、かつ、処理方法が正確になされている状態を完全に維持することをいう。以下同じ。）及び可用性（利用を許可された者が必要なときに情報の閲覧、更新等をすることができることをいう。以下同じ。）を維持することに関し、必要な事項を定めるものとする。

（定義）

第２条　この要領において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（１）個人情報　個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第２条第１項に規定する個人情報（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号。以下「番号法」という。）第２条第８項に規定する特定個人情報を含む。以下同じ。）をいう。

（２）ネットワーク　情報機器（コンピュータ、プリンタ、サーバ、通信制御装置等の機器をいう。以下同じ。）を相互に接続するための通信網並びに当該通信網に接続している情報機器及び記録媒体で構成し情報処理を行う仕組みをいう。

（３）情報システム　情報機器、ソフトウェア、ネットワーク及び記録媒体で構成されるものであって、これら全体で情報処理を行う仕組みをいう。

（４）内部業務系ネットワーク　総合行政ネットワークシステム、文書管理システム、財務会計シス

テム等を扱うネットワークをいう。

（５）インターネット系ネットワーク　インターネット、ホームページ作成システム等を扱うネットワークをいう。

（６）基幹系ネットワーク　住民情報、税情報、福祉情報等を扱うネットワークをいう。

（７）電子データ　電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。）のうち、コンピュータによる処理が可能な状態で記録されているものをいう。

（８）情報資産　次に掲げるものをいう。

ア　ネットワーク及び情報システム並びにこれらに係る機器及び設備

イ　情報システムの設計図書、ネットワーク構成図等（以下「システム関連文書」という。）

ウ　職員等（第３条に規定する職員等をいう。）が業務上作成し、又は取得した電子データ

（９）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。

（10）セキュリティ障害　次に掲げる事由による情報資産の漏えい、改ざん、消去等により、業務が停止することをいう。

ア　不正アクセス（不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）第２条第４項に規定する不正アクセス行為をいう。以下同じ。）、不正プログラム等による情報資産への攻撃又は妨害

イ　情報資産の破壊又は盗難

ウ　情報システムの欠陥又は故障

エ　地震、落雷、火災等の災害

オ　この要領その他の遵守すべき事項の違反行為

（不正プログラム：コンピュータウィルス、スパイウェア等のコンピュータに対して意図的に悪影響を及ぼすように作られたプログラム又はソフトウェアのこと。）

（適用範囲）

第３条　この要領は、市長及びその他市の執行機関に属する委員並びに市の職員（議会事務局の職員、会計年度任用職員、臨時的任用職員及び労働者派遣契約（事業所等が労働者派遣をすることを約する契約をいう。以下同じ。）により派遣されている者並びに石川県教職員定数条例（昭和 44 年石川県条例第 13 号）第２条第２項第２号に規定する職員を含み、同項第１号に規定する校長及び教員を除く。以下「職員等」という。）に適用する。

第２章　情報セキュリティ基本方針

（情報セキュリティ対策等の実施）

第４条　情報セキュリティの維持及びセキュリティ障害の発生を防止するため、組織体制の整備、情報資産の分類及び管理並びに次に掲げる対策（以下「情報セキュリティ対策」という。）を実施する。

（１）物理的セキュリティ対策　ネットワーク及び情報システムに係る情報機器の設置環境等において必要な措置を講ずること。

（２）人的セキュリティ対策　職員等及び事業者（情報機器、ソフトウェア等の販売、保守又は改修、

通信網の整備、電子データの情報処理等を業務として営む者をいう。以下同じ。）の行動及び作業の制限並びに職員等を対象とする研修及び緊急時に対応するための訓練を実施すること。

（３）技術的セキュリティ対策　ネットワーク、情報システム等の利用環境の制限、不正アクセスの防止及び不正プログラムの感染防止のための技術的な措置を講ずること。

（４）運用面におけるセキュリティ対策　情報セキュリティ実施手順（情報セキュリティ対策を実施するための手順をいう。以下同じ。）及び緊急時の対応計画の策定並びに情報システムの利用状況の監視、コンピュータの利用状況の調査及びこの要領の遵守状況の確認等を実施すること。

（監査及び自己点検の実施）

第５条　情報セキュリティ対策、情報セキュリティ実施手順及びこの要領の遵守状況を検証するため、定期的に又は必要に応じ、監査及び自己点検を実施する。