箕面市情報システムの管理運営に関する条例施行規則をここに公布する。

令和四年八月十日

箕面市長　上　島　一　彦　印

箕面市規則第四十四号

箕面市情報システムの管理運営に関する条例施行規則

箕面市情報システムの管理運営に関する条例施行規則（平成十六年箕面市規則第二十一号）の全部を改正する。

（目的）

第一条　この規則は、箕面市情報システムの管理運営に関する条例（平成十六年箕面市条例第七号。以下「条例」という。）の施行に関し、市が保有する情報資産の機密性、完全性及び可用性を維持するため、市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

（定義）

第二条　この規則において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　情報セキュリティポリシー　この規則及び対策基準（条例第六条第一項に規定する対策基準をいう。以下同じ。）をいう。

二　機密性　情報にアクセスする権限を有する者に限り、情報にアクセスできる状態を確保することをいう。

三　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。

四　可用性　情報にアクセスする権限を有する者が、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。

五　マイナンバー利用事務系　個人番号利用事務（社会保障、地方税又は防災に関する事務をいう。）又は戸籍事務等に関わる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。

六　ＬＧＷＡＮ接続系　総合行政ネットワーク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い、前号に掲げるものを除く。

七　インターネット接続系　インターネットメール、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。

八　無害化通信　インターネットメールの本文のテキスト化、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よう安全が確保された通信をいう。

九　情報セキュリティインシデント　情報セキュリティに関する障害及び事故並びに情報システム上の欠陥をいう。

（職員の遵守義務）

第三条　職員は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び第九条の情報セキ

ュリティ実施手順を遵守しなければならない。

（対象とする脅威）

第四条　実施機関は、次条の情報セキュリティ対策の実施に当たっては、次に掲げる情報資産に対する脅威を想定するものとする。

一　不正アクセス、ウイルス攻撃、サービス不能攻撃その他のサイバー攻撃、部外者の侵入、内部不正等の意図的な要因による情報資産の漏えい、破壊、改ざん又は消去、重要情報の詐取等

二　情報資産の無断持出し、無許可ソフトウェアの使用等の規程違反、設計又は開発の不備、プログラム上の欠陥、操作又は設定の誤り、メンテナンスの不備、内部又は外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器の故障等の非意図的な要因による情報資産の漏えい、破壊、消去等

三　地震、落雷、火災その他の災害によるサービス及び業務の停止等

四　大規模又は広範囲にわたる疾病のまん延による要員の不足に伴うシステム運用の機能不全等

五　通信の途絶、電力又は水道の供給の途絶その他のインフラの障害からの波及等

（情報セキュリティ対策）

第五条　実施機関は、前条の脅威から情報資産を保護するため、次の各号に掲げる項目に応じ当該各号に定める情報セキュリティ対策を講ずるも

のとする。

一　組織体制　市が保有する情報資産について、情報セキュリティ対策を推進する組織体制を確立すること。

二　情報資産の分類及び管理　市が保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づく適正な管理を実施すること。

三　情報システム全体の強靭（じん）性の向上　情報セキュリティを強化するため、業務の効率性及び利便性の観点を踏まえ、情報システム全体に対して次に掲げる三段階の対策を講ずること。

イ　マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報の持出しができない設定、端末への多要素認証の導入等を実施する。

ロ　ＬＧＷＡＮ接続系においては、インターネット接続系との通信環境を分離し、必要な通信に限り許可できるようにするとともに、両環境間で通信する場合は、無害化通信により実施する。

ハ　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施するために、自治体情報セキュリティクラウドの導入等を実施する。

四　物理的セキュリティ　サーバ、管理区域、通信回線及び職員の利用する端末等の管理について、物理的な対策を講ずること。

五　人的セキュリティ　情報セキュリティに関し、職員が遵守すべき事

項を定めるとともに、職員に対し十分な教育及び啓発を行う等の人的な対策を講ずること。

六　技術的セキュリティ　コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策その他の技術的な対策を講ずること。

七　運用　情報システムの監視、情報セキュリティポリシーの遵守状況の確認その他の情報セキュリティポリシーの運用面の対策を講ずること。

八　外部サービスの利用　次に掲げる情報セキュリティ対策を行うこと。

イ　外部委託する場合は、情報セキュリティ対策に関して委託を受けた事業者（以下「外部委託事業者」という。）が遵守すべき事項を明記した契約を締結するとともに、外部委託事業者において必要な情報セキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講ずること。

ロ　約款による外部サービスを利用する場合は、当該サービスの利用に係る規程を整備し、対策を講ずること。

ハ　ソーシャルメディアサービスを利用する場合は、当該サービスの運用手順を定め、当該サービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定めること。

（情報セキュリティ監査及び自己点検の実施）

第六条　実施機関は、情報セキュリティポリシーの遵守状況を検証するた

め、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施しなければならない。

（情報セキュリティポリシーの見直し）

第七条　実施機関は、情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要となった場合は、情報セキュリティポリシーを見直すものとする。

（情報セキュリティに関する組織の設置）

第八条　情報統括管理者は、市が保有する情報資産を適切かつ安全に管理し、情報セキュリティ対策を統一的に実施するため、箕面市情報セキュリティ委員会を設置する。

２　情報統括管理者は、情報セキュリティインシデントに迅速かつ適切に対応するため、箕面市ＣＳＩＲＴを設置する。

（情報セキュリティ実施手順の策定）

第九条　実施機関は、対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定しなければならない。

附　則

この規則は、公布の日から施行する。