豊岡市情報セキュリティ基本方針

令和８年３月

１．目的

本基本方針は、豊岡市の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、情報セキュリティ対策の基本方針を定めることにより、情報資産の適正な管理をすることを目的とする。

２．定義

（１） 情報システム

コンピュータ、ソフトウェア、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。

（２） ネットワーク

コンピュータを相互に接続するための通信網及びその構成機器をいう。

（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

本基本方針及び豊岡市情報セキュリティ対策基準をいう。

（５） 機密性

認められた者のみが、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、改ざん又は消去をされていない状態を確保することをいう。

（７） 可用性

認められた者のみが、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） 重要性

情報資産の分類及び取扱いの実効性を高めるために、機密性、完全性及び可用性を総括した基準をいう。

（９） マイナンバー利用事務系

個人番号利用事務（豊岡市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に基づく個人番号の利用に関する条例（平成27年豊岡市条例第47号）第４条の規定による事務をいう。）又は戸籍事務等に関する情報システム及びデータをいう。

(10) 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。

(11) インターネット接続系

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。

３．対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（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、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、重要情報の詐取、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の規定違反、設計及び開発の不備、プログラム上の欠陥、操作及び設定の誤り、メンテナンスの不備、内部及び外部の監査機能の不備、委託管理の不備、マネジメントの欠陥並びに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、休止等

（４） 疾病のまん延による要員不足に伴うシステム運用の機能の不全、遅延等

（５） 電力供給の途絶、通信の途絶、水道供給の途絶等の社会基盤の障害からの波及

（６） 搬送中の事故

４．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、市長部局、議会、消防本部、公営企業管理者、教育委員会、会計管理者、固定資産評価審査委員会、監査委員、選挙管理委員会及び農業委員会（以下「対象機関」という。）とする。

（２） 情報資産の範囲

本基本方針が対象とする情報資産は、次に掲げるものとする。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報（これらを記述した書面及び印刷した文書を含む。）

③情報システムの仕様書、ネットワーク図等のシステム関連文書

５．職員の遵守義務

職員、非常勤・会計年度任用職員等（以下「職員等」という。）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、情報セキュリティ実施手順その他の関連する法令等を遵守し、情報資産を適切に管理しなければならない。

６．情報セキュリティ対策

上記３に掲げる脅威から情報資産を保護するため、以下の情報セキュリティ対策を講ずる。

（１） 組織体制

豊岡市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（２） 情報資産の分類と管理

豊岡市の保有する情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３） システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる

①マイナンバー利用業務系においては、原則として、他の領域と通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN接続系においては、LGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③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。

（４） 物理的セキュリティ対策

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

（５） 人的セキュリティ対策

情報セキュリティに関し、職員等が順守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（６） 技術的セキュリティ対策

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、不正アクセス対策等の技術的対策を講じる。

（７） 運用におけるセキュリティ対策

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、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（８） 業務委託と外部サービス（クラウドサービス）の利用に対するセキュリティ対策

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要な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じる。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規程を整備して対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディア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。

（９） 評価・見直し

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、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は見直しを行う。

７．監査及び自己点検の実施

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する。

８．見直しの実施

情報セキュリティ監査及び自己点検の結果等により、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や、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になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで見直す。

９．情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するに当たって、具体的な遵守事項及び判断基準を定める情報セキュリティ対策基準を策定する。

10．情報セキュリティ実施手順の策定

情報セキュリティ対策基準により、対象機関及び所管するシステムにおける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するものとする。

11．情報セキュリティ対策基準等の非公開

情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより豊岡市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。