

砺波広域圏事務組合
情報セキュリティ基本方針

令和 8年 4月 1日 策定

1 目的

砺波広域圏事務組合（以下「本組合」という。）が保有する情報資産には、個人情報や本組合の運営に関わる重要情報が含まれており、情報セキュリティ対策を徹底することは、住民の財産やプライバシー保護、事務の安定運営のために必要不可欠であり、ひいては住民からの信頼の維持向上に寄与するものである。

また、ICTの進展に伴い電子自治体の実現が進む中、情報システムやネットワークの機密性、完全性及び可用性を維持するため、本組合は情報セキュリティ対策を整備し、「情報セキュリティ基本方針」を定める。

2 定義

この情報セキュリティポリシーにおいて、次の各号に掲げる用語の意義は、「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）及び「個人情報保護に関する法律」（平成15年法律第57号）、「砺波広域圏事務組合個人情報の保護に関する法律施行条例」（令和5年砺広組条例第3号）の定めるもののほか、それぞれ当該各号に定めるところによる。

(1) 部局等

本組合における事務局、組合議会、監査委員及びその他執行機関等のすべての組織をいう。

(2) 情報資産

電子計算組織で取扱う全てのデータ及び電子計算組織の開発と運用にかかる全ての情報並びに電子計算組織を構成する機器及び電磁的記録媒体をいう。

(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) 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。

(5) 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。

(6) 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。

(7) 情報セキュリティ対策

情報セキュリティの阻害要因から情報資産を守るための手段をいう。

3 情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本組合が所管する情報資産に関する情報セキュリティ対策について、総合的かつ体系的にとりまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

4 職員等及び外部事業者の遵守義務

本組合が所管する情報資産に関する業務に携わる職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

5 情報セキュリティ管理体制

情報セキュリティポリシーを適正に運用し、情報セキュリティを確保するため、情報セキュリティ対策を推進する本組合全体的な組織体制を確立する。なお、必要に応じ、構成市と連携した体制を構築する。

6 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、重要情報の詐取、内部不正等
- (2) 情報資産の無断持出、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、外部委託管理の不備、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等の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障害からの波及等

7 適用範囲

(1) 行政機関の範囲

情報セキュリティポリシーが適用される行政機関は、本組合における部局等とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

- ア 電子計算組織を構成する全ての機器及び電磁的記録媒体
- イ 電子計算組織及び電算処理で取り扱うデータ（これらを印刷した文書を含む。）
- ウ 電子計算組織及び電算処理の仕様書及びシステム関連文書
- エ 本組合が利用する外部サービス（クラウドサービスその他のインターネットを通じて提供される情報システムを含む。）において取り扱う情報及び当該サービスの利用に係る認証情報等

なお、本組合において取り扱う個人番号については、番号法その他関係法令及び本組合の関係規定に基づき、特定個人情報の適正な取扱いを徹底する。

8 対策

情報セキュリティを確保するため、以下の対策を講ずる。

(1) 情報資産の分類と管理

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、重要度に応じた適切な管理を行う。この際、国が明示する「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」における機密性分類を踏まえ、本組合の業務実態に即した分類基準を定める。

特に、個人情報その他の重要情報については、暗号化、アクセス制限、ログの取得・保管等の厳格な保護措置を講じる。

(2) 物理的セキュリティ

データサーバ、通信回線装置及び職員等の端末等の管理について、盗難、破壊、不正侵入等を防止するための物理的な対策を講じる。

(3) 人的セキュリティ

職員等に対し、情報セキュリティに関する法令や規定の遵守を義務付けるとともに、定期的な教育・研修を実施し、意識の向上を図る。

(4) 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、不正アクセス対策等の技術的対策を講じる。

(5) 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、外部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。また、情報資産への侵害が発生した場合に迅速に対応し、業務の継続及び早期復旧を図るため、緊急時対応体制を整備する。特に対策の実施にあたっては、外部委託事業者との迅速な連絡体制を確立し、構成市や富山県及び専門機関と連携及び協力する。

(6) 外部委託とサービスの利用

ネットワーク構築や保守等の業務を外部委託する際には、適切なセキュリティ水準を満たす事業者を選定し、情報セキュリティ要件を明記した契約を締結する。また、外部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。

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。

(7) 評価及び見直しの実施

情報セキュリティポリシーの遵守状況を検証するため、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。

情報セキュリティポリシー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に定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取巻く状況の変化に対応するために、情報セキュリティポリシーの見直し

を実施する。

9 施行

附 則

この基本方針は、令和8年4月1日から施行する。