砺波市情報セキュリティ基本方針

平成１６年１１月１日　策定

平成１８年　４月１日　改定

令和　３年　４月１日　改定

令和　５年　４月１日　改定

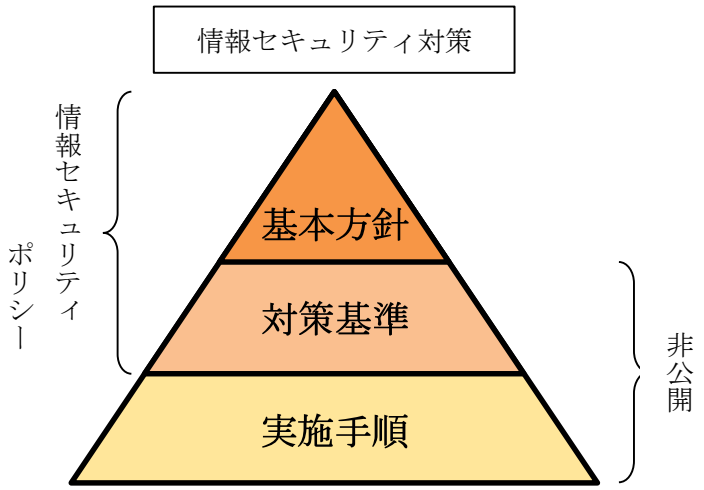
令和　８年　４月１日　改定

序　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、本市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、体系的かつ具体的にとりまとめたものを総称する。情報セキュリティポリシーは、本市が所管する情報資産に関する業務に携わる全職員、(任期付職員、会計年度任用職員、臨時的任用職員を含む。(以下「職員等」という。)及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、ＩＣＴの進歩等に伴う情報セキュリティを取巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、「砺波市電子計算組織に係る個人情報の保護に関する規則」の定めにより情報セキュリティポリシーを一定の普遍性を備えた部分(基本方針)と情報資産を取巻く状況の変化に依存する部分(対策基準)に分けて策定することとする。なお情報セキュリティ対策基準および情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼす恐れがあることから非公開とする。

情報セキュリティポリシーの構成



文　書　名		内　　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順。

１　目的

本市の情報システムには、市民の個人情報や行政運営上の重要情報など、漏洩時に重大な影響を及ぼす情報が多数含まれている。これらの情報資産を様々な脅威から守ることは、市民の財産やプライバシーの保護、安定的な行政運営に不可欠であり、本市に対する市民からの信頼維持・向上に直結するものである。

また、ＩＣＴの進展に伴う電子自治体の構築においては、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件となる。

これらを踏まえ、本市の情報セキュリティ対策を整備するため、「情報セキュリティポリシー（情報セキュリティ基本方針、情報セキュリティ対策基準)」を定める。

このうち、本「情報セキュリティ基本方針」は、対策の基本的な方針として、ポリシーの位置付けや対象、対策の概要等を定めるものとする。

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「個人情報の保護に関する法律」（平成１５年法律第５７号)、「砺波市電子計算組織に係る個人情報の保護に関する規則」（平成１６年砺波市規則第１４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

本市における市長部局、議会事務局、教育委員会事務局（各教育機関を含む）及びその他行政委員会をいう。

（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、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が認可された者だけがアクセスできる状態を確保すること。

（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。

（６）　可用性

許可された利用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。

（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、本市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

本市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、「砺波市電子計算組織に係る個人情報の保護に関する規則」に定める「砺波市電子計算組織運営管理協議会」（以下「協議会」という。）を中心とした全庁的な管理体制を確立する。

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、本市における部局等とする。ただし、総合病院および各小中学校の教育ネットワークは別にセキュリティポリシーを定めるため、範囲外とする。

（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

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）　情報セキュリティ対策の実施

機密性、完全性、可用性の各脅威から情報資産を保護するために、物理的、人的、技術的及び運用におけるセキュリティ対策を講ずる。

（２）　物理的セキュリティ

サーバ、サーバ室をはじめとする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の管理について、物理的な対策を講じる。

（３）　人的セキュリティ

情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するためには、その手順を具体的に定めていく必要がある。そのため、電子計算組織又は情報資産の特色に応じたセキュリティ対策を明記した、情報セキュリティ実施手順を策定し、この手順に関し十分な教育及び啓発を行う等の人的な対策を講じる。

（４）　技術的セキュリティ

電子計算組織の管理、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。

また、情報セキュリティの強化を目的とし、電子計算組織全体に対し、次の対策を実施する。

ア　電子計算組織をインターネット接続系、ＬＧＷＡＮ系、個人番号利用事務系の三つのネットワークに分離し、それぞれ他のネットワークとの通信をできないようにする。

イ　全ての端末に資産管理システムを導入し、「砺波市電子計算組織に係る個人情報の保護に関する規則」第１０条に定めるもののほか外部記録媒体による情報の持ち出しを原則禁止する。

ウ　インターネット接続系においては、富山県自治体情報セキュリティクラウドに参加したうえで不正通信の監視などの高度なセキュリティ対策を実施することとし、インターネットの通信回線は集約する。

エ　個人番号利用事務系については生体認証とＩＣカードの２要素認証を実施する。インターネット接続系、ＬＧＷＡＮ系については、２要素認証またはＩＣカードによる認証を実施する。

（５）　リスク分析の実施

情報資産ごとに、機密性、完全性、可用性に応じて分類し、当該分類に基づきセキュリティ対策を実施するとともに脅威と情報セキュリティが損なわれた場合の影響及び脆弱性の検証を行う。

（６） 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と同時に、情報セキュリティ実施手順を策定し詳細な運用ルールの確立を行う。また、電子計算組織及び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、対策基準において本市ＣＳＩＲＴ設置に関し必要な事項を定める。

（７） 外部サービス（クラウドサービス）の利用

業務委託する際には、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、利用に係る規定を整備し対策を講じる。

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。

（８） 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーが遵守されていることを検証するため、「砺波市電子計算組織に係る個人情報の保護に関する規則」に定める定期的な監査及び自己点検を実施する。

（９） 評価及び見直しの実施

情報セキュリティ監査の結果等により、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、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、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、平成１６年６月１日から施行する。

附 則

この基本方針は、平成１８年４月１日から施行する。

附 則

この基本方針は、令和　３年４月１日から施行する。

附 則

この基本方針は、令和　５年４月１日から施行する。

附 則

この基本方針は、令和　８年４月１日から施行する。