

千曲市情報セキュリティポリシー

情報セキュリティ基本方針

目次

序 情報セキュリティポリシーの構成	3
(1) 情報セキュリティ基本方針	3
(2) 情報セキュリティ対策基準	3
第1条 目的	3
第2条 用語の定義	4
第3条 情報セキュリティポリシーの位置付け	5
第4条 情報セキュリティポリシーの対象範囲	5
(1) 適用資産	5
(2) 適用対象者	5
第5条 職員等の義務	5
第6条 情報セキュリティ管理体制	5
第7条 情報資産の分類	5
第8条 情報資産への脅威	6
第9条 情報セキュリティ対策	6
(1) 人的セキュリティ対策	6
(2) 物理的セキュリティ対策	6
(3) 技術的セキュリティ対策	6
(4) 運用	6
第10条 情報セキュリティ対策基準の策定	6
第11条 情報セキュリティ実施手順の策定	7
第12条 情報セキュリティポリシーの情報公開	7
第13条 情報セキュリティ監査の実施	7
第14条 評価及び見直しの実施	7

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、千曲市の情報資産に対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取りまとめた文書を総称する。情報セキュリティポリシーは、千曲市の情報資産に関する業務に携わる職員等、及び外部委託業者に浸透、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、技術の進歩等に伴う情報セキュリティを取り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、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)と情報資産を取り巻く状況の変化に依存する部分(対策基準)の2階層に分けて策定することとした。

(1) 情報セキュリティ基本方針

千曲市としての情報セキュリティ対策に関する取り組み姿勢及び統一的な方針。

(2) 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千曲市におけるすべ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。

第1条 目的

千曲市の情報資産には、市民の個人情報をはじめ行政運営に必要な情報など、部外に漏洩、あるいは滅失した場合には極めて重大な結果を招く情報が多数含まれている。これらの情報資産を人的脅威や災害、事故等から防御することは、市民の財産、プライバシーを守るためにも、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠であり、ひいては、千曲市に対する市民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるIT革命の進展により、電子政府や電子自治体の実現が期待されている中で、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。

このため、千曲市の情報資産の機密性、完全性及び可用性を維持するための対策を整備することを目的として、千曲市情報セキュリティポリシーを定め、情報セキュリティの確保に最大限取り組むものである。

このうち情報セキュリティ基本方針は、千曲市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

第2条 用語の定義

(1) 電子計算機

ハードウェア及びソフトウェアで構成するコンピュータ、及び周辺機器並びに記録媒体(磁気ディスク等並びに入出力帳票及び情報システム仕様書等)をいう。

(2) ネットワーク

電子計算機を相互に接続するための通信網及びその構成機器(ハードウェア及びソフトウェア)で構成され、情報処理を行う仕組みをいう。

(3) 庁内ネットワーク

ネットワークのうち、千曲市役所各庁舎、出先機関、各種委員会、議会事務局、教育機関、福祉施設等の事務室で使用される電子計算機を相互に接続するための通信網及びその構成機器(ハードウェア及びソフトウェア)で構成され、情報処理を行う仕組みをいう。

(4) 情報システム

千曲市の各種電子計算機(ネットワーク、ハードウェア及びソフトウェア)及び記録媒体で構成され、処理を行う仕組みをいう。

(5) 情報資産

ネットワーク及び情報システムの開発と運用に係る全てのデータ並びにネットワーク及び情報システムで取り扱う全てのデータをいう。

(6) 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。

(7) 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ことを確実にすること。

(8) 完全性

情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

(9) 可用性

許可された利用者が必要なときに情報にアクセスできることを確実にすること。

(10) 職員

地方公務員法で規定された特別職、一般職の中で、千曲市に勤務する者の総称をいう。

(11) 関係機関の職員等

各種委員会、議会事務局、福祉施設等に勤務し、千曲市が管理する情報資産を職務で利用する者の総称をいう。

(12) 職員等

千曲市が管理する情報資産を職務で利用する職員及び関係機関の職員等(それぞれ非常勤職員及び臨時職員等を含む)の総称をいう。

(13) 外部委託者

職務委託先社員等、契約に基づいて千曲市の機関で作業する者の総称をいう。

(1 4) 部外者

職員等及び外部委託者以外の千曲市の情報資産に接することが認められていない者の総称をいう。

(1 5) 公共端末

千曲市の情報資産のうち、千曲市の施設等に設置され、職員等及び外部委託者以外の者が操作する端末の総称をいう。

(1 6) 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3条第2項に規定する不正アクセス行為その他の不正な手段により利用者以外の者が行うアクセス又は利用者が行う権限外のアクセスをいう。

第3条 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、千曲市が所掌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取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。

第4条 情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの適用範囲は、次の各項に定めるものとする。

(1) 適用資産

情報セキュリティポリシーの適用対象資産は、千曲市における全ての情報資産とする。

(2) 適用対象者

情報セキュリティポリシーの適用対象者は、千曲市における情報資産に接する全ての職員等とする。

第5条 職員等の義務

千曲市が所掌する情報資産に関する業務に携わる全ての職員等及び外部委託者は、情報セキュリティの重要性について共通の認識をも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。

第6条 情報セキュリティ管理体制

千曲市の情報資産について、適切に情報セキュリティ対策を推進・管理するための体制を確立するものとする。

第7条 情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

第 8 条 情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

- (1) 部外者の侵入による機器又は情報資産の破壊、盗難、故意の不正アクセスまたは不正操作による機器又は情報資産の破壊、盗聴、改ざん、消去等
- (2) 職員等及び外部委託者による機器又は情報資産の持出・誤操作、アクセスのための認証情報又はパスワードの不適切管理、不正アクセス又は不正行為による破壊、盗聴、改ざん、消去、搬送中の事故等による機器又は情報資産の盗難、規定外の端末接続によるデータ漏洩、認証情報等の不適切な管理等
- (3) コンピュータウイルス、地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

第 9 条 情報セキュリティ対策

千曲市の情報資産を第 8 条に示した脅威から保護するために、以下の情報セキュリティ対策を講ずるものとする。

(1) 人的セキュリティ対策

情報資産に接する職員等の情報セキュリティに関する権限や責任等を定めるとともに、全ての職員等及び外部委託者に情報セキュリティポリシーの内容を周知徹底する等、教育、訓練、啓発等を実施する。

(2) 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等、災害による情報資産の破壊・情報システムの停止等から保護するために物理的な対策を講ずる。

(3) 技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理、コンピュータウイルス対策等を実施する。

(4) 運用

情報セキュリティポリシーの実効性を確保するため、また、不正なアクセス等から適切に保護するため、システム開発等の外部委託、システムの管理、庁内ネットワークの監視、情報セキュリティポリシー遵守状況の確認等、運用面における必要な措置を講ずる。

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

第 10 条 情報セキュリティ対策基準の策定

千曲市の様々な情報資産について、第 9 条の情報セキュリティ対策を講ずるに当たっては、職員等が

遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

第 1 1 条 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を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要があることから、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、情報セキュリティ実施手順を策定するものとする。

第 1 2 条 情報セキュリティポリシーの情報公開

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千曲市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

第 1 3 条 情報セキュリティ監査の実施

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、定期的に監査を実施する。

第 1 4 条 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り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。