

茅野市情報セキュリティ基本方針

1 目的

この基本方針は、本市が保有する電子情報資産（以下「情報資産」という。）の機密性（情報資産に許可された者だけがアクセスできる状態をいう。以下同じ。）、完全性（情報資産及び処理の方法が正確かつ完全である状態をいう。以下同じ。）及び可用性（情報資産に対し必要なときにアクセスできる状態をいう。以下同じ。）を維持するため、本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。

2 適用範囲

(1) 行政機関の範囲

この基本方針が適用される行政機関（以下「行政機関」という。）は、市長部局、行政委員会、議会事務局及び地方公営企業とする。

なお、行政機関が、この基本方針に沿って、関連団体（広域連合、一部事務組合、茅野市土地開発公社、社会福祉法人茅野市社会福祉協議会、茅野市総合サービス株式会社及び公の施設の管理を行わせる指定管理者をいう。以下同じ。）との間で協定書等を締結した場合は、その関連団体も適用範囲とする。

(2) 情報資産の範囲

この基本方針が適用される情報資産は、次のとおりとする。

- 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電子情報
- ③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

3 定義

次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(1) ネットワーク

ハードウェア（コンピュータを構成している電子回路、周辺機器等の物理的実体をいう。）を相互に接続する通信網をいう。

(2) 情報システム

ハードウェア、ソフトウェア（コンピュータを動作させる手順・命令をコンピュータが理解できる形式で記述したものをいう。）及びネットワークに

より業務処理を行う仕組みをいう。

(3) 情報セキュリティ

情報資産の機密性及び完全性を維持し、並びに可用性を確保することをいう。

(4) 職員等

情報資産を取り扱う職員（嘱託職員、非常勤職員及び臨時職員並びに協定又は覚書に基づく派遣職員を含む。）をいう。

4 情報資産の分類と管理

行政機関は、所管する情報資産について機密性、完全性及び可用性を踏まえ分類し、その重要性に応じて適正な管理を行うものとする。

5 情報資産への脅威

情報資産に対する特に認識すべき脅威は、次に掲げるものとする。

(1) サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウィルス攻撃、サービス不能攻撃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な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障害による影響等

6 情報セキュリティ対策

行政機関は、情報資産への脅威から情報資産を保護するために、次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

情報セキュリティに関する権限及び責任並びに遵守すべき事項を明確に定め、職員等に対する周知及び徹底を図るとともに、十分な教育、啓発が行われるよう必要な対策を講ずるものとする。

(2) 物理的セキュリティ対策

コンピュータ及びネットワーク機器を設置する施設への不正な立入り、情報資産への改変、損傷、破壊、盗難等から保護するための物理的な対策を講ずるものとする。

(3) 技術的セキュリティ対策

情報資産を不正アクセス等から保護するため、情報資産へのアクセス制御、ネットワーク管理等の対策を講ずるものとする。

(4) 運用セキュリティ対策

情報システムの監視、情報セキュリティ対策の遵守状況の確認、外部委託を行う際のセキュリティ確保等運用面のセキュリティ対策を講ずるものとする。また、緊急事態が発生した場合に、迅速かつ適切な対応が可能となるような危機管理体制の整備等による対策を講ずるものとする。

7 情報セキュリティ対策基準の策定

行政機関は、情報セキュリティ対策を実施するに当たって遵守すべき事項及び判断の統一的な基準として、情報セキュリティ対策基準を定めるものとする。

8 情報セキュリティ実施手順の策定

行政機関は、情報セキュリティ対策を具体的に実施するために、情報セキュリティ実施手順（以下「実施手順」という。）を定めるものとする。

9 実施手順の扱い

実施手順は、公にすることにより市が行う情報セキュリティに関する対策に重大な支障を及ぼす恐れのある情報を含むことから、非公開とする。

10 職員等の義務

職員等は、情報セキュリティの重要性を認識するとともに、業務の遂行にあたっては、この基本方針及び情報セキュリティ対策基準（以下「情報セキュリティポリシー」という。）並びに実施手順を遵守する義務を負うものとする。

また、職員等は、情報資産の利用及び管理にあたり、茅野市個人情報保護条例（平成10年茅野市条例第25号）等の関連する法令等を遵守しなければならない。

11 協定等を締結した関連団体の義務

協定等を締結した関連団体は、情報システムを使用する者に対して、この基本方針を遵守するための必要な措置を講ずるものとする。

12 情報セキュリティに関する違反への対応

行政機関は、情報セキュリティポリシー及び実施手順に違反した者に対して、当該違反により発生した事案の重大性、状況等に応じて、懲戒処分等の必要な措置を講ずるものとする。

13 情報セキュリティ実施状況の検証

行政機関は、情報セキュリティポリシー及び実施手順が遵守されていることを確認するため、定期的実施状況の検証を行うものとする。

14 評価及び見直し

行政機関は、情報セキュリティの実施状況の検証結果及び情報セキュリティを取り巻く状況の変化に対応し、必要に応じて情報セキュリティポリシー及び実施手順の見直しを適宜行うものとする。