

茨木市情報セキュリティ基本方針

1 目的

本基本方針は、議会及び各執行機関の共同策定のもと、地方自治法（昭和22年法律第67号）第244条の6第1項に規定するサイバーセキュリティを確保するための方針として、本市が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、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。

なお、各執行機関による策定については、茨木市高度情報化の推進に関する規則（平成28年茨木市規則第52号。2 定義において「規則」という。）第10条に基づくものとする。

2 定義

本基本方針における用語の意義は、以下に定めるもののほか、規則の例による。

(1) 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

(2) 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。

(3) 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。

(4) 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。

(5) 情報セキュリティインシデント

望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

(6) 情報セキュリティ侵害

機密性、完全性又は可用性のいずれかが損なわれた状態をいう。

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、監査機能の不備、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インフラの障害からの波及等

4 適用範囲

本基本方針は、本市が保有する全ての情報資産に適用する。

5 順守義務

本基本方針適用対象となる情報資産を扱う者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシーを順守しなければならない。

6 情報セキュリティ対策

上記3の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制

本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組織体制を確立する。

(2) 情報資産の分類と管理

本市の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、当該分類に基づき情報セキュリティ対策を実施する。

(3) 物理的セキュリティ

サーバ、情報システム室、通信回線及び情報資産を扱う者のパソコン等の管理について、物理的な対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関し、情報資産を扱う者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。

(5) 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。

(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順守状況の確認、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、情報資産に対する情報セキュリティ侵害が発生した場合等に迅速かつ適切に対応するため、情報セキュリティインシデント対応手順を策定する。

(7) 業務委託と外部サービスの利用

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。

外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

7 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の順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。

8 情報セキュリティポリシーの見直し

情報セキュリティ監査又は自己点検の結果、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又は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ときは、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、情報セキュリティポリシーを見直す。

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ため、具体的な順守事項、判断基準等を定める情報セキュリティ対策基準を策定する。ただし、市長部局が整備するネットワークと論理的または物理的に分離されているネットワークについては、当該ネットワークを所管する行政機関が個別に対策基準を必要に応じて策定するものとする。

なお、情報セキュリティ対策基準は、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おそれがあることから非公開とする。

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基づき、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。ただし、市長部局が整備するネットワークと論理的又は物理的に分離されているネットワークについては、当該ネットワークを所管する行政機関が個別に実施手順を必要に応じて策定するものとする。

なお、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おそれがあることから非公開とする。