鳥取市固定資産評価審査委員会
情報セキュリティ基本方針

制定　令和８年４月

改定履歴

版	改定日	施行日	改定箇所	改定内容
初	令和８年４月１日	令和８年４月１日	全章	初版発行

目　次

１　目的

鳥取市固定資産評価審査委員会（以下「委員会」という。）は、市民の個人情報や行政運営情報など、外部への漏えいやデータの改ざん等の被害を受けた場合に極めて重大な結果を招く情報資産を多数保有している。

したがって、委員会が取り扱うこれらの情報資産を盗難や不正アクセスなどの様々な脅威から守ることは、市民の財産やプライバシーを保護するとともに、行政サービスの安定的な運営を図るために必要不可欠である。

本基本方針は、委員会が保有する情報資産の機密性・完全性・可用性を維持する対策として、委員会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　用語の定義

この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

⑴　委員等　委員会が保有する情報資産に関する業務に携わる全ての委員や職員をいう。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

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。

⑴　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・消去等、重要情報の詐取、内部不正等

⑵　情報資産の無断持ち出し、監査機能の不備、マネジメントの欠陥

⑶　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

⑷　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

⑸　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

⑴　行政機関の範囲

本基本方針が適用される行政機関は、鳥取市固定資産評価審査委員会とする。

⑵　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。ただし、市長部局が管理するネットワーク及び情報システム等の情報資産については、市長部局が定める方針の対象とする。

①　委員会が保有し又は作成する情報資産（市長部局が管理する情報システム等により作成され又は保存された記録及び情報を印刷した文書を含む。）

５　委員等の遵守義務

委員等は、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本基本方針を遵守しなければならない。

６　情報セキュリティ対策

対象とする脅威から情報資産を保護するため、本方針で対象とする情報資産を管理する行政機関において、以下のセキュリティ対策を実施するものとする。

⑴　組織体制

情報セキュリティにおける責任者を明確にし、その責任者に情報セキュリティに関する全ての権限を与える。また、情報セキュリティ責任者を補佐し、情報資産を利用する委員及び書記に対して指導及び監督を行うため、情報セキュリティ担当者を置き、情報資産を取り扱う委員及び書記への教育やセキュリティ事故発生時の対応等の情報セキュリティ対策を円滑に推進する。

⑵　情報資産の分類と管理

委員会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。

⑶　物理的セキュリティ

情報資産の管理について、物理的な対策を講じる。

⑷　人的セキュリティ

情報セキュリティに関し、委員等が遵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。

⑸　運用

本基本方針の遵守状況の確認等、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、緊急時対応計画を策定する。

⑹　評価・見直し

本基本方針の遵守状況を検証するため、定期的又は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し、運用改善を行い、情報セキュリティの向上を図る。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

要になった場合など、本基本方針の見直しが必要な場合は見直しを行う。

７　情報セキュリティ監査及び自己点検の実施

本基本方針の遵守状況を検証するため、定期的又は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　本基本方針の見直し

情報セキュリティ監査及び自己点検の結果、の見直しが必要となった場合及び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場合には、保有する情報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、本基本方針を見直す。