# 神戸市監査委員
# 情報セキュリティポリシー

令和８年３月 25 日　制定

令和８年４月１日　施行

神戸市監査委員

## 目次


1. 目的 3
2. 定義 3
2.1. ネットワーク 3
2.2. 情報システム 3
2.3. 情報セキュリティ 3
2.4. 機密性 3
2.5. 完全性 3
2.6. 可用性 3
2.7. インターネット接続系 3
3. 対象とする脅威 3
4. 適用範囲 3
4.1. 適用範囲 3
4.2. 情報資産の範囲 3
5. 監査委員の遵守義務 4
6. 情報セキュリティ対策 4
6.1. 組織体制 4
6.2. 情報資産の分類と管理 4
6.3. 情報システム全体の強靭性の向上 4
6.4. 物理的セキュリティ 4
6.5. 人的セキュリティ 4
6.6. 技術的セキュリティ 4
6.7. 運用 4
6.8. 業務委託と外部サービス（クラウドサービス）の利用 5
6.9. 評価・見直し 5
6.10. 情報資産の提供について 5
6.11. 貸与端末について 5
6.12. 自己所有端末について 5
7. 情報セキュリティ監査及び自己点検の実施 6
8. 情報セキュリティポリシーの見直し 6

## 1. 目的

本情報セキュリティポリシーは、監査委員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、監査委員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. 定義

### 2.1. ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

### 2.2. 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

### 2.3. 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。

### 2.4. 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。

### 2.5. 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をいう。

### 2.6. 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。

### 2.7. インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

## 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。

3.1. 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

3.2. 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、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

3.3. 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

3.4. 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

### 4.1. 適用範囲

本情報セキュリティポリシーの適用対象者は、監査委員とする。また、監査事務局職員に対して、本ポリシーの 6.10.及び神戸市セキュリティポリシーを適用する。

### 4.2. 情報資産の範囲

本情報セキュリティポリシーが対象とする情報資産は、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情報（これらを印刷した文書を含む。）
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

## 5. 監査委員の遵守義務

監査委員は、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遵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。

### 6.1. 組織体制

監査委員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。

最高情報セキュリティ責任者（CISO）として代表監査委員を置き、監査委員の情報セキュリティ対策に関する最終的な責任を負う 。ただし、代表監査委員が常勤ではない場合は、常勤監査委員がその責を担う。

CISO を補佐する統括情報セキュリティ責任者として監査事務局長を置き、情報セキュリティ管理者として監査事務局第１課長を置く。

### 6.2. 情報資産の分類と管理

監査委員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。情報資産の分類については、『地方公共団体における情報セキュリティポリシーに関するガイドライン』に準ずる。

### 6.3. 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じる。

インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

### 6.4. 物理的セキュリティ

サーバ、情報システム室、通信回線及びパソコン等の管理について、物理的な対策を講じる。

### 6.5. 人的セキュリティ

情報セキュリティに関し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。

① 業務目的外での情報資産の利用や持ち出しを禁止する。

② 情報セキュリティインシデントを発見した場合は、速やかに情報セキュリティ管理者である第１課長へ報告する義務を負う。

### 6.6. 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。

### 6.7. 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、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、緊急時対応計画を以下のとおりとする。

① 関係者の連絡先（神戸市監査委員情報セキュリティインシデント・セキュリティ侵害発生時連絡先のとおり）

② セキュリティ侵害を発見した場合は、統括情報セキュリティ責任者である監査事務局長へ報告し、監査事務局長は最高情報セキュリティ責任者と対応を協議することとする。

### 6.8. 業務委託と外部サービス（クラウドサービス）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（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。

### 6.9. 評価・見直し

情報セキュリティポリシー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。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

### 6.10. 情報資産の提供について

監査委員と監査事務局との間で自治体機密性２以上の情報資産の提供を行う場合は、次の事項を遵守する。

① 取り扱うデータは監査委員業務をおこなうにあたり必要な情報とする。
② 情報を取り扱う監査委員業務は、他者へ情報漏洩することのない環境の整った自宅又は執務室等で行うこととする。
③ 情報提供は、原則監査事務局が指定するファイル共有サービス（以下「ファイル共有サービス」という。）、E メール又は紙とする。なお、インターネット回線を利用してデータのダウンロード、アップロードを行う際には、ファイル共有サービスを介してのみ行うこととする。
④ 印刷をする場合は、②の環境下のみとし、印刷した資料はシュレッダー等による廃棄処理まで管理を行うこととする。
⑤ 端末内にデータをダウンロードする場合は原則監査事務局執務室内のみ可能とする。ただし、ダウンロード後は端末内にデータを保存したままにせず、ファイル共有サービス内に最終的に保存することとする。

### 6.11. 貸与端末について

情報資産取扱いのため、監査事務局より端末の貸与を受けることとする。本端末については以下の通り取り扱うこととする。

① 上記 6.10.の業務の用途でのみ使用可とする。
② 貸与端末は市から提供する LTE 回線のみ接続可とし、Wi-Fi 接続は不可とする。
③ 通常使用による端末故障は監査事務局が修理を行うこととする。

### 6.12. 自己所有端末について

情報資産取扱いのため、以下の要件を満たす場合にのみ自己所有端末の利用を認めることとする。

① 事前に使用する端末の登録を行うこと。
② ウイルス定義の定期的な更新等安全性を保つこと。
③ 安全性の確認できている回線・Wi-Fi のみに接続すること
④ 監査委員が本ポリシーに違反し、もしくはそのおそれがあることを発見した場合、情報管理者が強制的に個人端末等のデータの削除等の必要な措置を行える権限を有するものとする 。
⑤ 前項のデータの削除等の必要な措置を行う際に、個人端末等に保存されていた私有の情報が削除されてしまった場合、それにより発生した損害については、市は一切の責任を負わないものとする。

## 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. 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及び自己点検の結果、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。