# 高山市監査委員サイバーセキュリティを確保するための方針

（目的）

第１　この方針は、監査委員（以下「委員」という。）が保有する情報資産（第４第３項に規定する情報資産をいう。以下同じ。）の機密性、完全性及び可用性を維持するため、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。

（定義）

第２　この方針において、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　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。

⑵　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。

⑶　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。

⑷　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。

⑸　情報システム　コンピュータ、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及びその構成機器（ソフトウェアを含む。）をいう。）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。

⑹　情報セキュリティポリシー　この方針をいう。

（対象とする脅威）

第３　情報資産に対する情報セキュリティ対策の実施に当たり、対象とする脅威は、次の各号に掲げるとおりとする。

⑴　サイバー攻撃（不正アクセス、ウイルス攻撃、サービス不能攻撃等をいう。）、内部不正（職員等及び委託事業者による情報資産の無断持出し等をいう。）、部外者の侵入その他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

⑵　無許可ソフトウェアの使用等、設計・開発の不備、プログラム上の欠陥、誤操作、設定の不備、保守・管理の不備、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、機器故障その他非意図的要因による情報資産の漏えい、破壊、消去等

⑶　地震、落雷、火災その他災害によるサービス及び業務の停止等

⑷　大規模かつ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　通信、電力供給及び水道供給の途絶等のインフラの障害からの波及等

⑹　その他情報セキュリティを脅かす事案

（適用範囲）

第４　この方針の適用を受ける行政機関は、委員とする。

２　この方針の適用を受ける者は、委員、監査委員事務局の常勤職員（以下「委員等」という。）とする。

３　この方針が対象とする情報資産は、次のとおりとする。

⑴　情報システム

⑵　情報システムで取り扱う情報（印刷した文書を含む。）

（委員等の遵守義務）

第５　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。

（委託等に伴う措置）

第６　委託等により、業務において委員が保有する情報資産を委員等以外の者に利用させる場合は、情報セキュリティポリシーと同等以上の水準での情報セキュリティを確保できるよう、契約等において必要な措置を講じるものとする。

２　委託等により、業務において委員が保有する情報資産を利用する委員等以外の者は、当該業務の範囲において情報セキュリティポリシーを遵守するものとする。

（情報セキュリティ対策）

第７　第３に規定する脅威から情報資産を保護するために講じる情報セキュリティ対策は、次の各号に掲げる区分に応じ、当該各号に定めるとおりとする。

⑴　組織体制　委員の保有する情報資産について、情報セキュリティ対策を推進する組織体制を確立するものとする。

⑵　情報資産の分類及び管理　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行うものとする。

⑶　物理的セキュリティ対策　サーバ、サーバ室、通信回線、端末等の管理について、物理的な対策を講じるものとする。

⑷　人的セキュリティ対策　情報セキュリティに関し、委員等が遵守すべき事項を別に定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じるものとする。

⑸　技術的セキュリティ対策　情報システムの管理、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ものとする。

⑹　運用面の対策　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、外部委託を行う際のセキュリティ確保その他情報セキュリティポリシーの運用面の対策を講じるとと

もに、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切に対応するため、緊急時対応体制を整備するものとする。

（自己点検等の実施）

第８　情報セキュリティポリシーの遵守状況を検証するため、必要に応じて自己点検又は情報セキュリティ監査を実施するものとする。

（情報セキュリティポリシーの見直し）

第９　自己点検又は情報セキュリティ監査の結果、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は、情報セキュリティポリシーを見直すものとする。

（監査委員事務局の特例）

第１０　監査委員事務局職員（監査委員事務局の常勤職員をいう。）が、高山市の情報システムを利用する場合は、この方針に関わらず高山市情報セキュリティポリシーを遵守するものとする。

附　則

この方針は、令和８年４月１日から施行する。