和歌山県監査委員情報セキュリティ基本方針

1　目的

和歌山県監査委員情報セキュリティ基本方針（以下「本基本方針」という。）は、和歌山県監査委員（以下「本県委員」という。）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、本県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

⑴　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。

⑵　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。

⑶　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。

⑷　監査委員情報セキュリティポリシー

本基本方針及び和歌山県監査委員情報セキュリティ対策基準規程をいう。

⑸　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。

⑹　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。

⑺　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。

⑻　外部サービス

民間事業者等が情報システムの一部又は全部を提供するクラウドサービス、Web 会議サービス、SNS（ソーシャルネットワーキングサービス）、検索サービス、翻訳サービス、地図サービス、ホスティングサービス等をいう。

⑼　ソーシャルメディアサービス

インターネット上で展開される情報メディアであって、組織又は個人による情報発信、個人間のコミュニケーションの利用を可能とするサービスをいう。

3　対象となる脅威

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　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

⑵　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

4　適用範囲

⑴　対象者の範囲

本方針は、本県委員が保有する情報資産を利用する本県委員及び監査委員事務局職員（以下「利用者」という。）に適用する。

⑵　情報資産の範囲

本方針が対象とする情報資産は以下のものとする。

ア　監査で使用する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

イ　監査で使用する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。）

ウ　監査で使用する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　利用者の遵守義務

利用者は、情報セキュリティの重要性について共通の認識を持ち、監査又は事務局業務の遂行において、監査委員情報セキュリティポリシー及び監査委員情報セキュリティポリシーに基づく実施手順等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。

⑴　組織体制

本方針が対象と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。

⑵　情報資産の分類と管理

代表監査委員は、和歌山県が策定した和歌山県情報セキュリティポリシー（以下「県情報セキュリティポリシー」という。）を準用したセキュリティレベルを設定し、本方針が対象とする情報資産を、その機密性、完全性及び可用性に応じたセキュリティレベルに分類する。

利用者は、当該分類に基づき情報セキュリティ対策を実施する。

⑶　情報システム全体の強靭性の向上

組織における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、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。

⑷　物理的対策

組織で取り扱う情報資産のセキュリティレベルに応じ、情報資産の保管、情報システム又はネットワーク設置環境、物理的アクセス等に関する対策を講じる。

⑸　人的対策

情報セキュリティに関し、利用者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。

⑹　技術的対策

組織で取り扱う情報資産のセキュリティレベルに応じ、漏洩や否認防止、利用者の識別方法、アクセス制御方法、障害対策等に関する対策を講じる。

⑺　運用上の対策

組織で取り扱う情報資産のセキュリティレベルに応じ、データの取扱い、保管、バックアップ等運用上の対策を講じる。また、情報システム及びネットワークに関する運用及び管理手順を定め、不正アクセスや障害検知当の監視を行う。

なお、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は、県情報セキュリティポリシーの「事件・事故対応計画」に準じた対応を行う。

⑻　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。

外部サービス及びソーシャルメディアサービスを利用する場合についても、県情報セキュリティポリシーに準じた対策を講じる。

7　情報セキュリティに関する内部点検の実施

監査委員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に関する内部点検を実施する。

8　情報セキュリティポリシーの見直し

情報セキュリティに係る内部点検の結果、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、リスクを検討した上で、情報セキュリティポリシーを見直す。

9　和歌山県監査委員情報セキュリティ対策基準及び実施手順の策定

本基本方針に基づく情報セキュリティ対策を講じるため、具体的な遵守事項及び判断基準等を定める和歌山県監査委員情報セキュリティ対策基準規程及び個々の情報資産の取扱いに関する具体的な手順を定める実施手順は、代表監査委員が別に定める。