和歌山県人事委員会情報セキュリティ基本方針

1　目的

和歌山県人事委員会情報セキュリティ基本方針（以下「本基本方針」という。）は、和歌山県人事委員会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、和歌山県人事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　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　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。

⑸　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。

⑹　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。

⑺　インターネット接続系

インターネットメール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。

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、ソーシャルメディアサービス、検索サービス、翻訳サービス、地図サービス等をいう。

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（SNS 等）をいう。

3　対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、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、操作・設定ミス、メンテナンス不備、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
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、通信の途絶等のインフラの障害からの波及等

4　適用範囲
⑴　対象者の範囲
本基本方針は、和歌山県人事委員会委員及び同事務局職員（以下「職員等」という。）に適用する。
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。
ア　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　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　情報システムの仕様書等のシステム関連文書

5　職員等の遵守義務
職員等は、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
上記３の脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。
⑴　管理・組織体制
本基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ため、管理・組織体制を別紙のとおりとする。
⑵　情報資産の分類と管理
本基本方針が対象と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　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、インターネット接続系においては、監視等の情報セキュリティ対策を実施する。
⑷　物理的セキュリティ
本基本方針が対象とする情報資産の管理について、物理的な対策を講じる。
⑸　人的セキュリティ
情報セキュリティに関し、職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。
⑹　技術的セキュリティ
アクセス制御、不正アクセス対策等の技術的対策を講じる。
⑺　運用
情報システムの監視、本基本方針の遵守状況の確認、本基本方針の運用面の対策を講じるものとする。
⑻　外部サービスの利用
外部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。
ソーシャルメディアサービスを利用する場合には、和歌山県人事委員会へのなりすましや同委員会であると誤認させる行為への対策を実施する。また、パスワードや認

証のための文字列等の認証情報及びこれを記録した記憶媒体を適正に管理し、不正アクセスへの対策を実施する。

7　情報セキュリティに関する自己点検の実施

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に関する自己点検を実施する。

8　本基本方針の見直し

情報セキュリティに関する自己点検の結果、本基本方針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、本基本方針を見直す。

別紙

和歌山県人事委員会情報セキュリティ管理・組織体制

1　管理体制

⑴　最高情報セキュリティ責任者（CISO）

人事委員会における情報セキュリティに関する責任と権限を有し、人事委員会委員長がその任に当たる。

⑵　情報セキュリティ責任者

人事委員会事務局における情報セキュリティに関する責任と権限を有し、事務局長がその任に当たる。

⑶　情報セキュリティ管理者

情報セキュリティ責任者の指示の下、人事委員会事務局における情報セキュリティ活動を行い、総務課長がその任に当たる。

2　組織体制

⑴　情報セキュリティ委員会

ア　情報セキュリティに関する重要な事項を審議し決定する。
また、業務遂行上やむを得ず本基本方針を適用できない事態についての判断を行う。

イ　情報セキュリティ委員会は、別表第１の者で構成する。
また、必要に応じて関係者及び有識者の参画を求めることができる。

ウ　情報セキュリティ委員会委員長は、最高情報セキュリティ責任者がその任に当たる。

エ　情報セキュリティ委員会委員長は、情報セキュリティに関する事項に関する調査・検討・活動・運営の支援のために、必要に応じて情報セキュリティ委員会幹事会を設置できる。

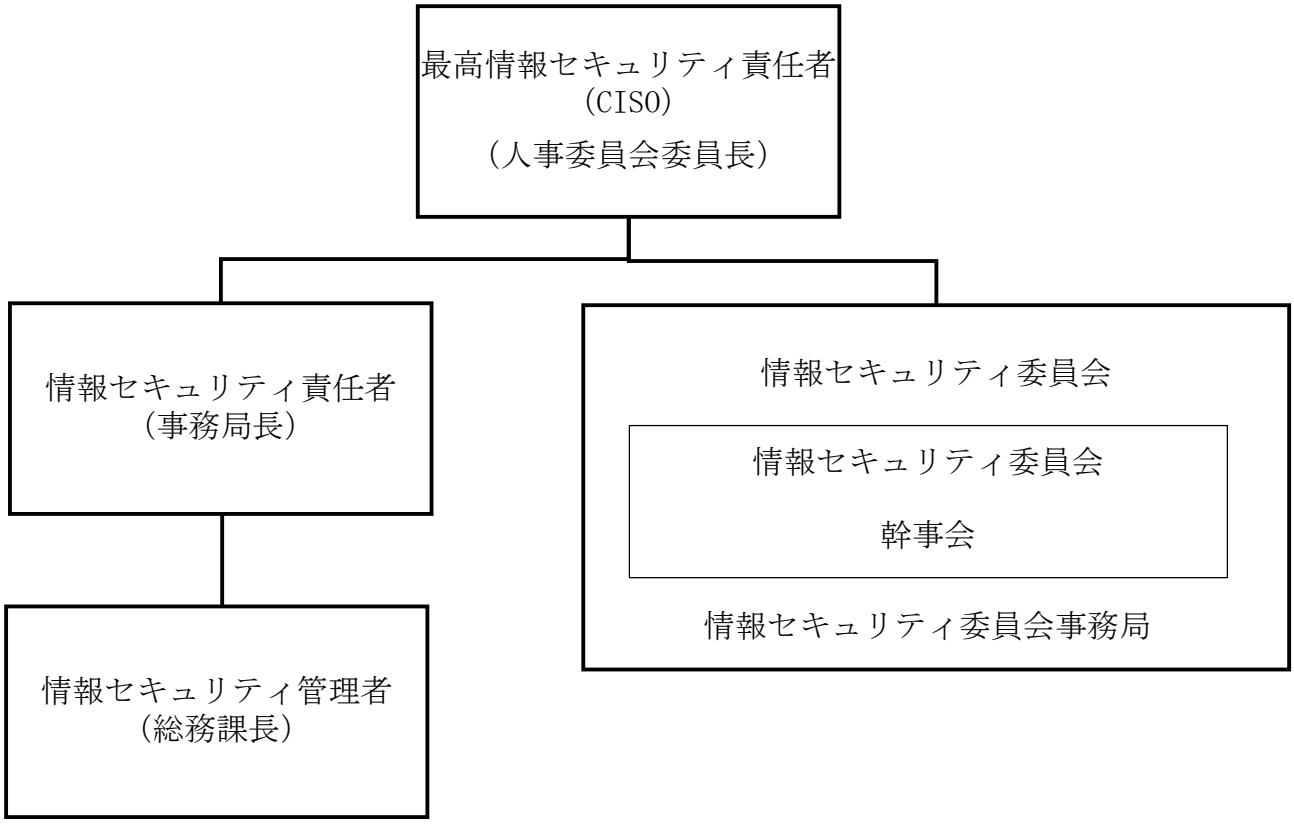
⑵　情報セキュリティ委員会幹事会

ア　情報セキュリティに関する次の事項を行う。
(ｱ)情報セキュリティに関する情報の収集
(ｲ)「情報セキュリティ基本方針」等の改定作業
(ｳ)職員等への情報セキュリティに関する教育・研修の検討
(ｴ)その他幹事長が特に必要と認める事項

イ　情報セキュリティ委員会幹事会の幹事長及びメンバーは、別表第２の者のうち最高情報セキュリティ責任者が指名するもので構成する。

⑶　情報セキュリティ委員会事務局

情報セキュリティ委員会事務局は、人事委員会事務局総務課内に設置し、情報セキュリティ委員会活動・運営の支援を行う。



情報セキュリティ管理組織図

別表第１

情報セキュリティ委員会委員長	人事委員会委員長（最高情報セキュリティ責任者）
情報セキュリティ委員会副委員長	人事委員会事務局長（情報セキュリティ責任者）
情報セキュリティ委員会委員	人事委員会事務局総務課長（情報セキュリティ管理者）
	人事委員会事務局職員課長

別表第２

人事委員会事務局総務課長
人事委員会事務局職員課長
人事委員会事務局総務課副課長
人事委員会総務課課長補佐
人事委員会職員課課長補佐
人事委員会事務局総務課担当