和歌山県情報セキュリティ基本方針

序文 1
第１章　和歌山県情報セキュリティ基本方針の目的 2
　第１節　和歌山県情報セキュリティ基本方針の目的 2
　第２節　定義 2
　第３節　適用範囲 3
　　第１項　組織 3
　　第２項　ネットワーク 4
　　第３項　情報システム 4
　　第４項　情報資産 4
第２章　基本的な考え方 4
　第１節　情報資産に対する脅威 4
　第２節　情報セキュリティ対策 5
第３章　情報セキュリティポリシー等の取扱い 6
　第１節　基本方針 6
　第２節　対策基準 6
　第３節　実施手順 6
　第４節　点検 6
　第５節　情報セキュリティ監査 6
　第６節　情報セキュリティポリシーの改正 6
第４章　人と組織 7
　第１節　職掌上の役割と責任 7
　　第１項　知事の役割と責任 7
　　第２項　管理職の役割と責任 7
　　第３項　職員の役割と責任 7
　　第４項　部外受託者の役割と責任 7
　第２節　セキュリティの管理体制及び組織 7
　　第１項　管理体制 7
　　第２項　組織 8
　　第３項　情報管理者 10
　第３節　セキュリティに関する教育 10
　第４節　第三者による情報資産使用に関する方針 10
第５章　情報資産の分類 10
　第１節　セキュリティレベルの設定 10
　第２節　情報資産の分類 10
第６章　情報セキュリティ対策 10
　第１節　物理的対策 11
　　第１項　情報資産に対する対策 11
　　第２項　情報システムに対する対策 11
　　第３項　ネットワークに対する対策 11
　第２節　技術的対策 11
　　第１項　情報資産に対する対策 11
　　第２項　情報システムに対する対策 11

第３項　ネットワークに対する対策 11
第３節　運用上の対策 11
第１項　情報資産に対する対策 11
第２項　情報システムに対する対策 11
第３項　ネットワークに対する対策 12
第７章　情報セキュリティ事件・事故対応計画の策定 12
第８章　ポリシーの遵守 12
第１節　法令等の遵守 12
第２節　罰則等 12

序文

和歌山県は、県民生活を豊かにするとともに行政サービスの向上、行政運営の効率化のために「和歌山県 IT 戦略」（平成 14 年 3 月発行）を策定し、電子自治体や電子商取引など情報化を推進しています。しかし、情報活用が期待される一方、和歌山県が取り扱う情報には、県民の個人情報のみならず行政運営上重要な情報などが含まれており、漏洩、損傷等の事故があった場合に極めて重大な結果を招く可能性があります。

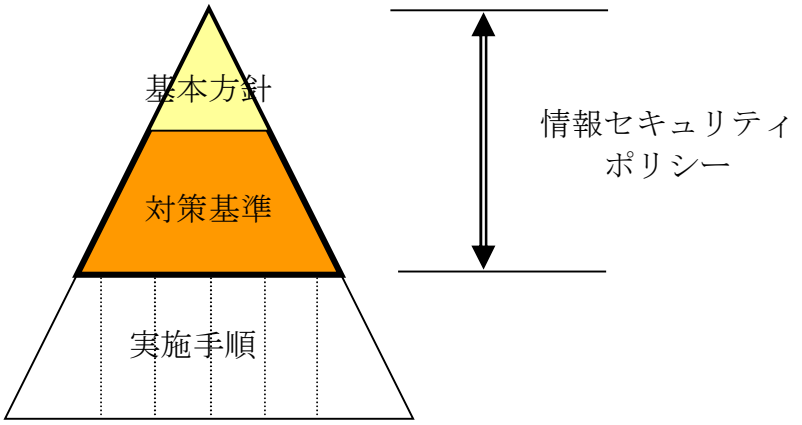
不正アクセス、コンピュータウィルスなどの外部からの脅威も日々増大かつ高度化しており、また内部職員又は業務受託事業者による機密情報又は県民の個人情報の漏洩・悪用の可能性も皆無とはいえず、情報セキュリティ管理の重要性が高まっています。

そこで、和歌山県は、県民が安心・信頼して行政サービスを利用することができるようにするとともに、和歌山県における継続的かつ安定的な行政事務の実施を確保するために、情報セキュリティ管理に関する総合的、体系的かつ具体的な対策を和歌山県情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）として定めます。

情報セキュリティポリシーとは、情報資産の機密性（秘密を守る）、完全性（改ざんされない）、可用性（サービスが停まらない）という３つの情報セキュリティの要素を一定以上に保ち、維持するためのルールです。和歌山県職員は、このルールを理解し、遵守するとともに、情報セキュリティ管理は職員ひとりひとりの責任であることを自覚しなければなりません。

情報セキュリティポリシーは、和歌山県の情報資産をさまざまな脅威から守るための基本的な考え方（基本方針）と基本方針を実現するために何をやらなければならないかという遵守すべき行為及び判断などの基準（対策基準）から構成されます。

また、対策基準に基づいた具体的なセキュリティ対策のため、セキュリティ管理上の役割又は情報システムごとに実施手順を定めます。



情報セキュリティポリシー及び実施手順の構成

第１章　和歌山県情報セキュリティ基本方針の目的

第１節　和歌山県情報セキュリティ基本方針の目的

和歌山県情報セキュリティ基本方針（以下「基本方針」という。）は、情報セキュリティポリシーの構成の一つで、和歌山県（以下「県」という。）の職員（非常勤職員及び臨時職員を含む。）及び部外受託者（県の業務に従事する派遣会社社員、協力会社社員及び業務受託会社社員）など、情報資産を扱う者全員が従うべき、情報セキュリティを確保するための基本的な考え方であり、情報セキュリティポリシーの適用範囲や取扱い、人と組織の役割と責任、情報セキュリティ対策の基本的な方向性等を定めるものである。

第２節　定義

本方針で掲げる用語の意義は、以下に定めるところによる。

(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) 情報通信機器
　ルータ（信号の伝送を中継する装置をいう。）、リピータ（信号を増幅して伝送距離を延長する装置をいう。）等の信号を伝送するための機器をいう。

(3) 情報機器
　ハードウェア及び情報通信機器をいう。

(4) 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。

(5) 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。

(6) 情報セキュリティポリシー
　本基本方針及び和歌山県情報セキュリティ対策基準規程をいう。

(7) 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。

(8) 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。

(9) 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。

(10) マイナンバー利用事務系
行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号）第２条第１０項に規定する個人番号利用事務に係る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。

(11) LGWAN 接続系
LGWAN（地方公共団体を相互に接続する行政専用のネットワークをいう。）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。

(12) 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。

(13) 通信経路の分割
LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(14) 無害化通信
インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

(15) 外部サービス
一般の事業者等の庁外の組織が情報システムの一部又は全部の機能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。

(16) 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等を利用した情報流通といった社会的な要素を含んだメディアの利用を可能とするサービスをいう。

第３節　適用範囲

第１項　組織

情報セキュリティポリシーの適用範囲は、知事部局の全ての部署とする。議会事務局、各種委員会事務局、教育委員会及び警察本部（警察署を含む。）については、知事部局が管理するネットワーク、情報システム及び情報資産を扱う部署を適用範囲とし、適用範囲外となる部署においても、別途、情報セキ

ュリティポリシーに準拠した各組織における情報セキュリティポリシーを策定し、遵守することにより、県全体の情報セキュリティレベルを維持することとする。

第２項　ネットワーク

組織で使用される情報通信機器及び通信回線とする。

第３項　情報システム

組織で使用されるネットワーク、ハードウェア、ソフトウェア及び記憶媒体で構成された情報を処理する仕組みとする。

第４項　情報資産

情報セキュリティポリシーが適用される情報資産は以下のものとする。

(1) 組織で使用されるネットワーク及び情報システムの開発、保守及び運用にかかわる全ての文書、図画、写真、フィルム並びに電磁的記録

(2) 組織で使用されるネットワーク及び情報システムで取り扱う全ての電磁的記録

(3) 組織で使用されるネットワーク及び情報システムの運用時にかかわる文書及び図画。ただし、公文書を除く。

第２章　基本的な考え方

第１節　情報資産に対する脅威

情報資産に対する脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は、以下のとおりとし、情報セキュリティ対策を実施する。

(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

(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) 地震、落雷、火災、風水害等の災害によるサービス及び業務の停止等

(4) 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

(5) 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

第２節　情報セキュリティ対策

前節で示した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ずるものとする。

(1) 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、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③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。

(2) 物理的対策

情報システム及びネットワークを設置する施設への不正な立ち入り、並びに情報システム、ネットワーク及び情報資産への損傷・妨害等から保護するための物理的な対策を講ずる。

(3) 人的対策

情報セキュリティに関する権限及び責任を定め、職員等に基本方針、情報セキュリティに関する法令などの内容を周知徹底する等、十分な教育及び啓発が行われるよう必要な対策を講ずる。

(4) 技術的対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策を講ずる。

また、情報システム及びネットワークの可用性を確保するために、必要な技術面の対策を講ずる。

(5) 運用上の対策

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、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の危機管理対策を講ずる。

(6) 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。

また、外部サービスを利用する場合には、利用にかか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、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

第３章　情報セキュリティポリシー等の取扱い

第１節　基本方針

基本方針は、県民等から預かっている情報の管理方針と位置付け、広く公開するものとする。

第２節　対策基準

基本方針に基づいた情報セキュリティ対策を講じるに当たって、遵守すべき行為、判断などの基準を統一的に定めるために、必要となる基本要件を明記した対策基準を策定する。

対策基準は、県の情報資産を取り扱うすべての職員及び部外受託者に対し、周知徹底する。

第３節　実施手順

情報セキュリティポリシーを遵守して情報セキュリティ対策を実施するため、個々の情報資産の取扱いについて具体的な手順を明記した実施手順を策定するものとする。

実施手順は、当該情報資産を取り扱うすべての職員及び部外受託者に対し、周知徹底する。

第４節　点検

情報セキュリティポリシーに沿った情報セキュリティ対策が実施されているかどうか、定期的に点検を行う。

第５節　情報セキュリティ監査

情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を行う。

第６節　情報セキュリティポリシーの改正

情報セキュリティを取り巻く状況の変化に迅速に対応するため、情報セキュリティ監査の結果なども踏まえ、情報セキュリティポリシーは定期的に見直し、必要に応じて改正する。

第４章　人と組織

第１節　職掌上の役割と責任

第１項　　知事の役割と責任

知事は、セキュリティに関する指針を明らかにし、職員及び部外受託者に対してセキュリティ意識を浸透させ、必要な支援をする役割と責任をもつ。

第２項　　管理職の役割と責任

管理職は、セキュリティ確保の責任を負い、所属部署の職員及び部外受託者が、情報セキュリティポリシー、情報セキュリティポリシーに基づく実施手順等を理解し遵守することを徹底し、かつ管理する。

また、管理職は、所属部署の職員が退職、転出又は業務変更する場合、利用する必要のなくなった全ての情報資産を回収する責任がある。また、部外受託者が契約終了した場合も同様である。

第３項　　職員の役割と責任

職員は、情報セキュリティポリシー、情報セキュリティポリシーに基づく実施手順等及び管理職の指示を遵守し、情報が不正な手段で取得されること又は不正に使用されることを防止する責任がある。

職員は、退職、転出又は業務変更する場合に利用する必要のなくなった全ての情報資産を県に返却しなければならない。

第４項　　部外受託者の役割と責任

部外受託者は、契約に基づき情報セキュリティポリシー、情報セキュリティポリシーに基づく実施手順等及び関係する部署の管理職の指示を遵守し、情報を不正な手段で取得したり、不正に使用してはならない。

部外受託者は、契約終了その他を原因として県の情報資産を取り扱えることができなくなった時点で、全ての情報資産を県に返却しなければならない。

第２節　セキュリティの管理体制及び組織

県の保有する情報資産について、統一的な情報セキュリティを確保するため、全庁的な管理体制を以下のとおりとする。

第１項　　管理体制

(1) 最高情報統括責任者（CIO）

県におけるセキュリティを含む情報管理全般に関する最高責任者であり全ての責任及び権限を有し、副知事がその任に当たる。

(2) 最高情報セキュリティ責任者（CISO）

県における情報セキュリティに関する責任と権限を有し、副知事が任命する者がその任に当たる。

(3) 統括情報セキュリティ責任者
最高情報セキュリティ責任者を補佐し、情報セキュリティ担当課長がその任に当たる。

(4) 情報セキュリティ責任者
各部署における情報セキュリティに関する責任と権限を有し、本庁各部長、各振興局長、議会事務局長、各種委員会事務局長、教育長及び警察本部警務部長がその任に当たる。

(5) 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、各部署における情報セキュリティ活動を行う。
本庁においては、各課室長が、振興局においては、各部長が、地方機関においては、地方機関の長が、各種委員会、教育委員会においては、各課室長が、県警察本部においては、所属長がその任に当たる。

第２項　組織

(1) 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情報セキュリティポリシー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を調査・検討するために情報セキュリティ委員会幹事会を、委員会活動・運営の支援のために委員会事務局を設置する。

(2) 情報セキュリティ委員会幹事会
ｱ　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最高情報統括責任者が指名する。

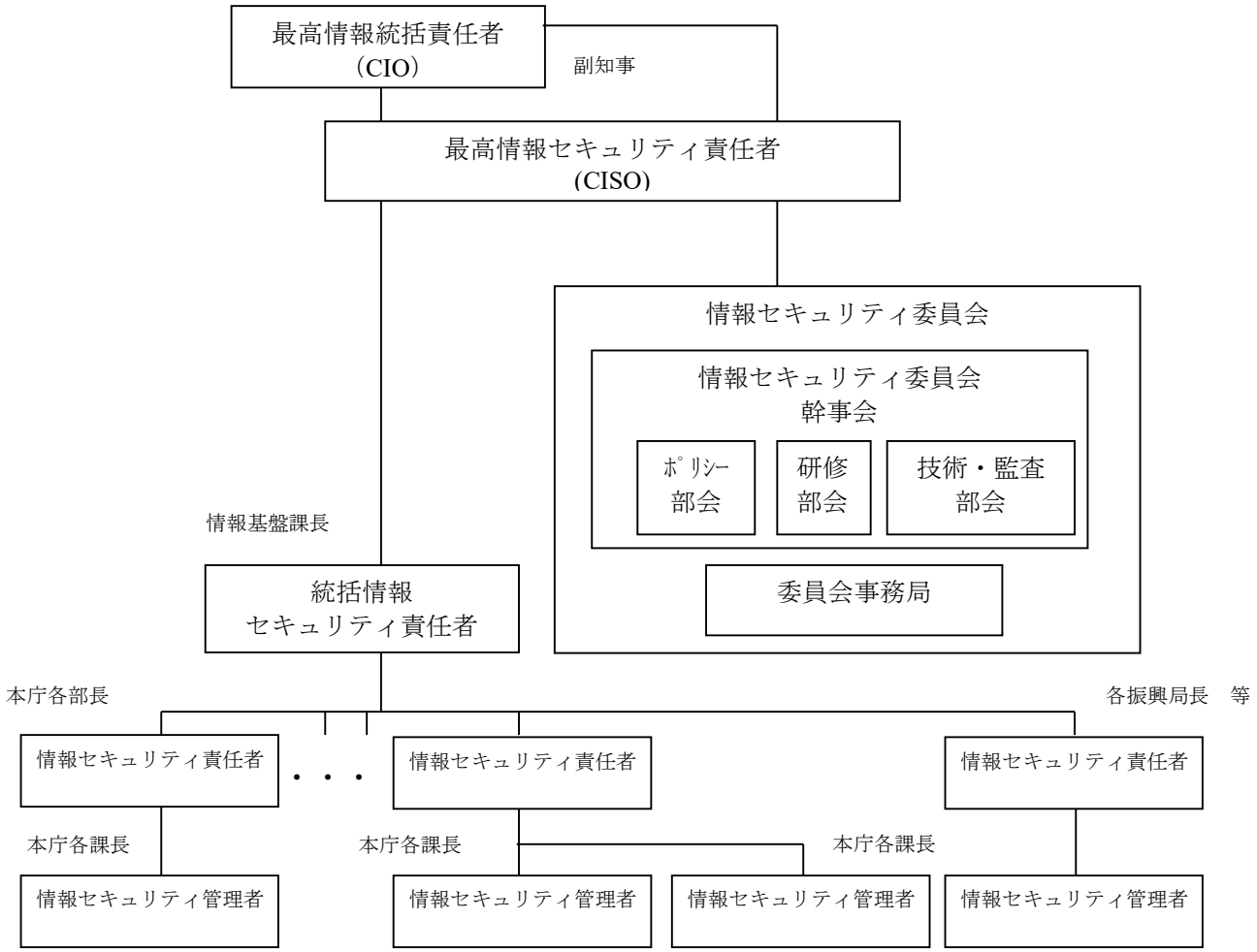
ｲ　情報セキュリティ委員会幹事会幹事長は、ポリシー部会、研修部会及び技術・監査部会を設置する。また、必要に応じて他の部会を設置することができる。

(ｱ) ポリシー部会
情報セキュリティに関する情報を収集し、「情報セキュリティ基本方針」、「情報セキュリティ対策基準」、「情報セキュリティ実施手順」の改定作業を行う。

(ｲ)研修部会
職員及び部外受託者への情報セキュリティに関する教育・研修の検討を行う。

(ｳ)技術・監査部会
情報セキュリティに関する情報を収集し、技術支援を行う。
情報セキュリティに関して、定期的に内部監査を行い、随時外部監査を実施する。

(3) 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、総務部行政企画局情報基盤課内に設置し、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

第３項　情報管理者

主管する業務において、情報収集、作成又は県民等から情報を預託された部署の所属長を情報管理者とする。

情報管理者は、自ら所有する情報資産の保護管理要件を定める。また、情報セキュリティ委員会の委任により、預託された情報の使用者を決定する。

第３節　セキュリティに関する教育

情報セキュリティポリシーの職員等への浸透と情報セキュリティ意識向上のため、情報セキュリティに関する教育プログラムを策定し、それを実施する。

第４節　第三者による情報資産使用に関する方針

県の情報資産を、当該情報を県に預託した本人以外の第三者に使用させる場合は、事前に当該情報の情報管理者の承認を必要とする。また、情報セキュリティ上必要な事項についてその第三者と契約するものとする。

情報管理者は情報資産の使用を承認した場合に、直ちに情報セキュリティ委員会に報告するものとする。

なお、特に個人情報の取扱いについては、個人情報の保護に関する法律の規定を遵守すること。

一般に公開するシステムによる情報使用に対しては、利用者の識別が行われないため、情報が不正な手段で取得されることや、当該システムが不正に使用されることを防止する対策を講じる。

第５章　情報資産の分類

第１節　セキュリティレベルの設定

情報セキュリティ委員会は、情報資産の重要度に応じて、機密性、完全性及び可用性を維持するために、セキュリティレベルを設定する。

セキュリティレベルごとに情報資産の保護管理要件を明確にし、想定されるリスク及びその対策を明確にする。

第２節　情報資産の分類

情報管理者は、自らが所管する情報資産を重要度に応じてセキュリティレベルに分類する。必要な場合は、追加の保護管理要件を設定することができる。

第６章　情報セキュリティ対策

情報セキュリティを確保するため、セキュリティレベルに応じて、情報の機密性、完全性及び可用性を維持するものとし、物理、技術及び運用の面から以下の対策を行う。

第１節　物理的対策

第１項　　情報資産に対する対策

セキュリティレベルに応じ、情報資産の保管、運搬等に関する対策を講じなければならない。

第２項　　情報システムに対する対策

情報システム内で取り扱う情報資産のセキュリティレベルに応じ、情報システムの設置環境、物理的アクセス等に関する対策を講じなければならない。

第３項　　ネットワークに対する対策

ネットワーク内を通過する情報資産のセキュリティレベルに応じ、ネットワークの設置環境等に関する対策を講じなければならない。

第２節　技術的対策

第１項　　情報資産に対する対策

セキュリティレベルに応じ、漏洩や否認防止等に関する対策を講じなければならない。

第２項　　情報システムに対する対策

情報システム内で取り扱う情報資産のセキュリティレベルに応じ、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なければならない。また、システム開発及び保守に関するセキュリティ要件を明確にしなければならない。

第３項　　ネットワークに対する対策

ネットワーク内を通過する情報資産のセキュリティレベルに応じ、ネットワークの経路制御、障害対策等に関する対策を講じなければならない。

第３節　運用上の対策

第１項　　情報資産に対する対策

情報資産は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管理に関する対策を講じなければならない。

第２項　　情報システムに対する対策

情報システムは、情報システム内で取り扱う情報資産のセキュリティレベルに応じて、明確で文書化された運用手順、事故管理手順を作成し、それに基づいて適切に管理運用しなければならない。

情報機器の設置、廃棄、構成の変更などについては、管理手順を定め適切な管理を行わなければならない。

情報システムは、セキュリティレベルに応じて、不正アクセスや障害検知等のための監視を行わなければならない。

情報セキュリティ責任者は、所管する情報システムのセキュリティ情報を収集し、必要な対策をとらなければならない。

第３項　ネットワークに対する対策

ネットワークは、ネットワーク内を通過する情報資産のセキュリティレベルに応じて、明確で文書化された運用手順、事故管理手順を作成し、それに基づいて適切に管理運用しなければならない。

ネットワーク機器の設置、廃棄、構成の変更などについては、管理手順を定め適切な管理を行わなければならない。

ネットワークは、セキュリティレベルに応じて不正アクセスや障害検知等の監視を行わなければならない。

第７章　情報セキュリティ事件・事故対応計画の策定

情報セキュリティ事件又は事故が発生した場合に備えて、被害レベルに基づいた対応体制、対応手順及び県民等への説明等を規定した情報セキュリティ事件・事故対応計画を策定する。

情報セキュリティ事件・事故対応計画は、定期的に訓練を実施し、適宜見直さなければならない。

第８章　ポリシーの遵守

第１節　法令等の遵守

職務を遂行するに当たり、取り扱う情報資産について、関連する法令等を遵守し、これに従わなければならない。

第２節　罰則等

職員が、情報セキュリティポリシー、情報セキュリティポリシーに基づく実施手順等に違反した場合は、その重大性、発生した事案の状況に応じて地方公務員法等の定めにより懲戒処分等の対象となる。

部外受託者が、情報セキュリティポリシー、情報セキュリティポリシーに基づく実施手順等に違反した場合の対応については、予め契約に定めておく。

別表（情報セキュリティ委員会関係）

役　職	
委員長 （最高情報ｾｷｭﾘﾃｨ責任者）	副知事が任命する者
知事室	副知事が任命する者
本庁各部	和歌山県行政組織規則第 9 条第 2 項に定める主管局の長
会計局	副知事が任命する者
教育委員会	副知事が任命する者
警察本部警務部	警務部長