島根県情報セキュリティポリシー

平成２９年４月
島根県

序　情報セキュリティポリシーの構成

島根県情報セキュリティポリシーは、島根県（以下「県」という）が管理する情報資産を適切に保護するため、県が行う情報セキュリティ対策について、総合的、体系的に取りまとめたものである。

情報セキュリティポリシーは、全ての県職員（常勤職員、臨時的任用職員及び非常勤職員）並びに外部委託事業者に浸透、定着させるものであり、安定的な規範であることが要請される。

しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

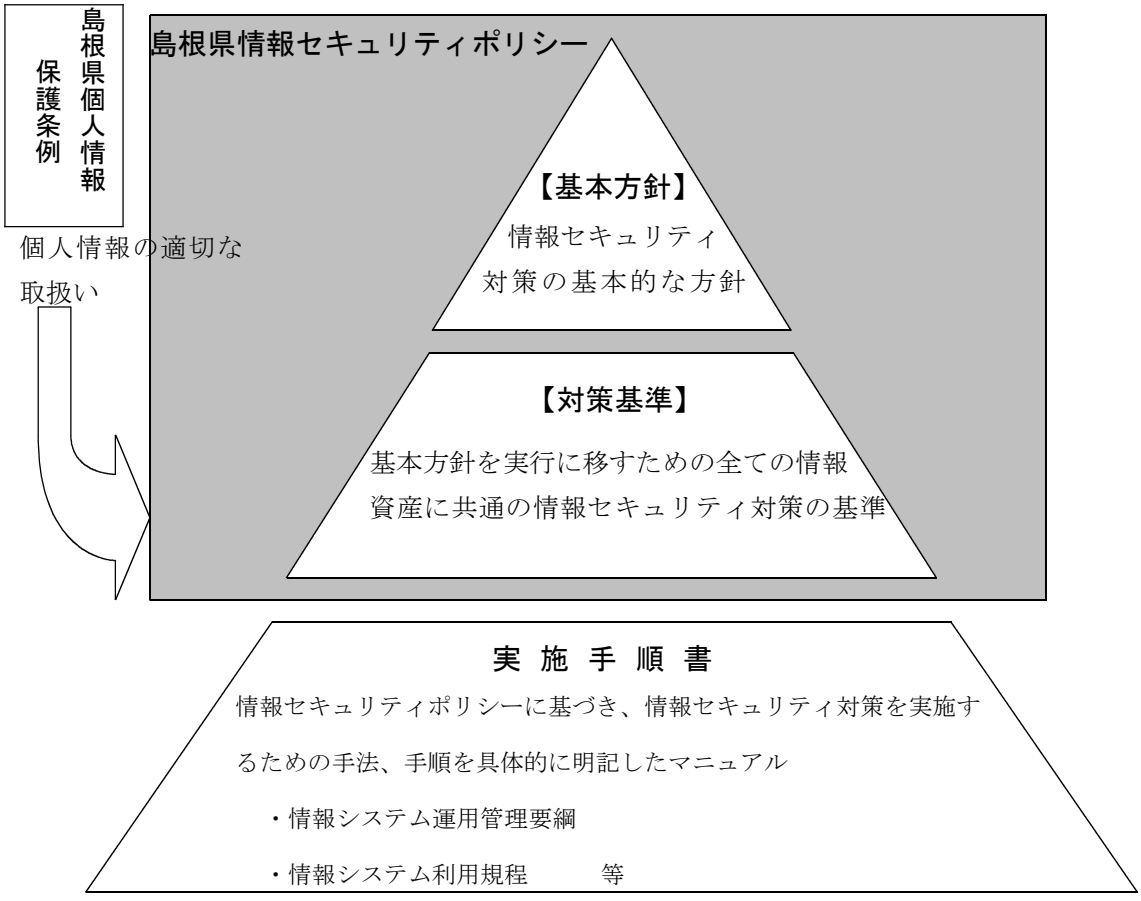
このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（セキュリティ基準）で構成する。

「情報セキュリティ基本方針」・・・情報セキュリティ対策の基本的な方針

「情報セキュリティ対策基準」・・・基本方針を実行に移すための全ての情報資産に共通の情報セキュリティ対策の基準

また、情報セキュリティポリシーに基づき、具体的な情報セキュリティ対策を実施するため情報セキュリティ実施手順を策定することとする。

島根県の情報セキュリティ対策文書の体系図



第１章 情報セキュリティ基本方針

第１　目　的

島根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）は、県が管理する情報資産を適切に保護するための情報セキュリティについての基本的な考え方及び方策を定める。

第２　定　義

１　情報資産

情報及び情報通信システムをいう。

２　情報

職務の遂行に伴って取り扱う全ての情報（紙及び電磁的記録媒体に記録されたもの、会話等を含む）をいう。

３ 情報システム

コンピューター及びそれを制御するソフトウェアを利用し、情報を適切に保存し、管理（集計等の処理を含む。）し、流通（ネットワークを利用した伝達のほか、用紙に出力することによる流通も含む。）させるための仕組みをいう。国等の県以外の者が管理運営する情報システムを利用する場合を含む。

４ ネットワーク

伝送路及び通信を制御する機器により構成され、情報の送受信を行う仕組みをいう。

５ 情報通信システム

情報システム及びネットワークをいう。

６ 情報セキュリティ

情報資産を脅威から保護し、情報資産の「機密性」、「完全性」及び「可用性」を確保することをいう。

- 機密性：権限のない者への重要な情報の漏えいを防止すること
- 完全性：情報の改ざん、破壊による被害を防止すること
- 可用性：権限のある者に対し、いつでも情報の利用を可能とすること

７ 脆弱性

脅威による情報資産の損失を起こりやすく、かつ、拡大させる要因をいう。

第３　対象となる脅威

自然的脅威（地震、火災、風水害等）、人的脅威（不正行為、誤操作等）及び技術的脅威（情報通信システムの故障、誤動作等）、外的脅威（不正アクセス、不正プログラム、サイバー攻撃等）など情報資産に損失を生じさせる直接の要因をいう。

第４　対象機関

情報セキュリティポリシーの対象となる機関（以下「実施機関」という。）は、知事部局、企業局、病院局、議会事務局、各行政委員会及び警察本部（警察署を含む。）とする。なお、知事部局及び企業局以外の機関については、知事が管理運用する情報資産を利用する場合に限る。ただし、知事部局及び企業局以外の機関が知事が管理運用する以外の情報資産を利用する場合に、この情報セキュリティポリシーを準用することは妨げない。

第５　職員の義務

職員（臨時的任用職員及び非常勤職員を含む。以下において同じ。）は、情報セキュリティの重要性について共通の認識を持つとともに、関係する法令、情報セキュリティポリシー及び関係規定を遵守する義務を負う。

第６　情報セキュリティ管理体制

統一的な情報セキュリティを確保するため、全庁的な組織体制を整備する。

第７　情報の分類

情報は、その重要度により区分し、適切な保護対策を講ずる。

第８　情報セキュリティ対策

情報資産を脅威から保護するために、次の各号に定める情報セキュリティ対策を講ずる。

１　物理的対策

情報資産を取り扱う施設への不正な立ち入りや災害等から情報資産を保護するための、入退室管理、震災対策等の物理的な対策

２　人的対策

職員及び委託事業者に対して情報セキュリティの重要性を認識させるために有効と考えられる研修や啓発活動などの対策

３　技術的対策

情報通信システムの故障、情報通信システムへの不正アクセス、誤操作等から情報資産を保護するための、アクセス制御等の技術的な対策

４　情報通信システム運用上の対策

情報通信システムの故障、情報通信システムへの不正アクセス、誤操作及びコンピューターウイルス等から情報資産を保護するための、運用、保守、監視等の対策

５　情報通信システム開発時における対策

情報通信システムの開発及び変更時における開発環境の管理対策や品質の確保対策

６　緊急時における対策

情報の安全性を侵害する事故の発生に備え、迅速かつ適切な対応を可能とするための危機管理対策

第９　実施手順書

情報セキュリティポリシーに基づき、情報セキュリティ対策を実施するための具体的な手法、手順を明記した実施手順書を策定する。

第10　委託に伴う措置

委託契約を締結し、委託事業者を情報資産の取扱いに従事させる場合は、契約に基づき、情報セキュリティポリシーを遵守させるための必要な措置を講ずる。

第11　情報セキュリティ対策実施状況の点検及び監査

情報セキュリティポリシーが遵守されていることを確認するため、定期的に情報セキュリティ対策の実施状況の点検及び監査を行う。

第12　義務違反者に対する措置

１　情報セキュリティポリシー及び実施手順書に違反した職員に対しては、改善を求める等の措置を行う。

２　発生した事案の状況及び重大性により、地方公務員法等による懲戒処分を含め、厳格に対応する。

第13　評価及び見直し

情報セキュリティをとりまく状況の変化等を踏まえ、適宜、情報セキュリティポリシー及び実施手順書を見直す。

第２章　情報セキュリティ対策基準

第１節　情報セキュリティの管理体制

第１　管理体制

情報セキュリティポリシーに定める情報セキュリティ対策は、以下の管理体制により、体系的に実施する。

１　最高情報セキュリティ責任者（ＣＩＳＯ：Chief Information Security Officer、以下「ＣＩＳＯ」という。）

⑴　県の情報セキュリティを統括する最高責任者として、ＣＩＳＯを置く。

⑵　ＣＩＳＯは、副知事をもって充てる。

⑶　ＣＩＳＯは、情報セキュリティ委員会を招集し、主宰する。

⑷　ＣＩＳＯは、情報セキュリティの実施状況及び情報セキュリティ委員会の活動状況等について、必要に応じて知事に報告する。

⑸　ＣＩＳＯは、情報セキュリティに係るリスク管理上の初動対応を迅速かつ機動的に進める場合など必要と認める時は、ＣＩＯ（統括情報セキュリティ責任者）にその任を代行させることができる。

２　統括情報セキュリティ責任者

⑴　ＣＩＳＯを補佐する者として、ＣＩＯ（統括情報セキュリティ責任者）を置く。

⑵　ＣＩＯは、行政情報化推進総括者（地域振興部長）をもって充てる。

⑶　ＣＩＯは、ＣＩＳＯが不在の場合及び前項１の⑸に基づきＣＩＳＯの代行を命じられた場合に、その任にあたる。

３　情報セキュリティ委員会

⑴　情報セキュリティ対策を推進し、適正な運用及び管理を総合的に審議するため、情報セキュリティ委員会を置く。

⑵　情報セキュリティ委員は、別表に掲げる職にある者をもって充てる。

⑶　情報セキュリティ委員会は、情報セキュリティポリシーについて必要に応じて検討・見直しを行う。

⑷　情報セキュリティ委員会は、情報セキュリティに関する統一的な窓口の機能を有し、情報の安全性を侵害する重大な事故が発生した場合は、その対応策を検討する。

４　島根県ＣＳＩＲＴ（シーサート）

⑴　情報セキュリティに係るリスク管理上の初動対応を迅速かつ機動的に進めるため、ＣＩＳＯ及びＣＩＯの指揮のもとに、島根県ＣＳＩＲＴを置く。

⑵　島根県ＣＳＩＲＴの構成員は、ＣＩＯが情報セキュリティ委員、地域振興部情報政策課職員及び委託事業者等の中から指名する。

⑶　島根県ＣＳＩＲＴは、⑴の任務を遂行するために必要となる権限をＣＩＳＯ及びＣＩＯから付与されるものとし、全ての実施機関に対し、指示・指導・助言を行うことができる。

⑷　全ての実施機関は、⑶の指示・指導・助言を受けた時は、速やかに対処しなければならない。

５　情報セキュリティ推進班

⑴　情報セキュリティ委員会を補佐し、情報セキュリティ対策を効果的に進めるため、情報セキュリティ推進班を置く。

⑵　情報セキュリティ推進班の構成員は、情報セキュリティ委員が所属のグループリーダー級以上の職員を指名する。

⑶　情報の安全性を侵害する事故が発生した場合は、事故対応の状況を確認し、必要に応じてシステム管理者及び関係する所属に助言・指示を行う。

⑷　情報セキュリティに関する情報収集及び関係する所属への情報の周知を行う。

⑸　情報セキュリティ推進班に、必要に応じて特定のテーマごとに専門部会を置くことができる。

⑹　専門部会の構成及び運営に関し必要な事項は、情報セキュリティ推進班で定める。

６　情報セキュリティ委員会事務局

⑴　情報セキュリティ委員会及び情報セキュリティ推進班の運営に関する事務は、地域振興部情報政策課が所掌する。

⑵　情報政策課長は、情報セキュリティ推進班を招集し、主宰する。

７　システム管理者

⑴　各情報通信システムにおいて、この基準に基づき情報セキュリティ対策を実施し、安定的な運用を図るため、システム管理者を置く。

⑵　システム管理者は、各情報通信システムの運用管理を行う所属の長をもって充てる。

⑶　システム管理者は、所管する情報通信システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

⑷　システム管理者は、所管する情報通信システムにおける情報セキュリティに関する権限及び責任を有する。

⑸　新たな情報通信システムを開発する場合は、開発を担当する所属の長をシステム管理者とする。

８　ネットワーク管理者

システム管理者のうち、専らネットワークの運用管理を行うため、ネットワーク管理者を置く。

９　運用（開発）担当者

⑴　システム管理者を補助し、情報通信システムの適切な利用を推進するため、各情報通信システムに運用（開発）担当者を置く。

⑵　運用（開発）担当者は、システム管理者が指定する者をもって充てる。

⑶　システム管理者は、毎年度、運用（開発）担当者の職指名を情報政策課長に報告するものとする。年度途中において運用（開発）担当者を変更した場合も同様とする。

10　所属長

⑴　所属で保有する情報資産（システム管理者が管理するものを除く）を管理し、情報セキュリティ委員会及びシステム管理者が定める実施手順書に基づき、情報セキュリティ対策の適切な運用を図る。

⑵　所属内で情報セキュリティに関する研修及び啓発を行う。

11　セキュリティ担当者

⑴　所属長を補助し、情報資産の適切な利用を推進するため、所属にセキュリティ担当者を置く。

⑵　セキュリティ担当者は、総括担当のグループリーダー又は所属長が指定する者（地方機関にあっては、所属長が適当と認める課長等）をもって充てる。

⑶　所属長は、毎年度、セキュリティ担当者の職指名を情報政策課長に報告するものとする。年度途中においてセキュリティ担当者を変更した場合も同様とする。

⑷　セキュリティ担当者は、情報セキュリティ対策に関する次の各号に掲げる業務を行う。

①　コンピューターウイルス対策の徹底

②　ＩＤ、パスワード及び情報システムの設定情報の適切な運用の徹底

⑸　セキュリティ担当者は、必要に応じて所属の職員に前項に掲げる業務の遂行を補助させることができる。

12　職員

所属長及びシステム管理者の指示に従い、情報資産を適切に取り扱う。

第２　兼務の禁止

１　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

２　監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

別表　情報セキュリティ委員名簿

部局名	情報セキュリティ委員
政策企画局	政策企画監
総務部	総務課長、人事課長、税務課長、管財課長、総務事務センター長
広報部	広報室長
防災部	消防総務課長
地域振興部	地域政策課長、情報政策課長、市町村課長
環境生活部	環境生活総務課長
健康福祉部	健康福祉総務課長
農林水産部	農林水産総務課長
商工労働部	商工政策課長
土木部	土木総務課長
出納局	会計課長
企業局	総務課長
病院局	県立病院課長
県議会事務局	総務課長
教育委員会事務局	総務課長、学校企画課長
人事委員会事務局	企画課長
監査委員事務局	監査第一課長
労働委員会事務局	審査調整課長
警察本部	情報管理課長

第２節　情報の分類と管理

第１ 情報の分類

本県における情報は重要性に基づき次のとおり分類する。

１　重要情報

⑴　島根県個人情報保護条例（平成14年島根県条例第７号）に規定する個人情報
⑵　島根県情報公開条例（平成12年島根県条例第52号）に規定する非公開情報
⑶　所属長、システム管理者及びネットワーク管理者が重要情報と同等の取扱いが必要と認めた情報

２　一般情報

重要情報以外の全ての情報

第２　情報の管理

１　情報の管理基準

所属長及びシステム管理者は、アクセス制御等により情報を管理・保護する対策を講じるとともに、職員並びに運用（開発）担当者及び一般利用者に適切に取り扱うよう指示する。

２　情報の分類の表示

職員は、重要情報について、ファイル（ファイル名等)、格納する電磁的記録媒体のラベル、文書の隅等に、分類を表示し、必要に応じて取扱制限について明示する。

３　情報の作成

⑴　職員は、業務上必要のない情報を作成してはならない。
⑵　情報を作成する者は、情報の作成時に情報の分類に応じ当該情報を区分し、適切に管理する。
⑶　情報が複製または伝送された場合には、複製等された情報を情報の分類に応じ当該情報を区分し、適切に管理する。
⑷　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止する。また、情報の作成途上で不要になった場合は、当該情報を消去する。

４　情報資産の入手

⑴　職員は、他の職員が作成した情報を入手したときは、作成者が定めた情報の分類により当該情報を取り扱う。
⑵　職員は、県機関以外の者が作成した情報を入手したときは、情報の分類に応じ当該情報を区分し、適切に管理する。
⑶　情報を入手した職員は、入手した情報の分類が不明な場合又は区分することが

困難な場合は、所属長又はシステム管理者に報告し、指示に従う。

５　情報の利用

⑴　職員は、業務以外の目的に情報資産を利用してはならない。

⑵　情報を利用する職員は、情報の分類に応じ、適切に取り扱う。

６　情報の保管

所属長及びシステム管理者は、情報資産の分類及び保存期間に応じ、当該情報資産を適切に保管する。

７　情報の伝送・送付

⑴　職員は、重要情報を電子メール及びＦＡＸ等の通信手段を利用して送信してはならない。やむを得ず送信する必要がある場合は、所属長の許可を得た上で適切な措置を講ずる。

⑵　職員は、重要情報が記録又は記載された記録媒体及び文書を郵送等の手段により送付する場合は、所属長の許可を得た上で適切な措置を講ずる。

８　情報の搬送

職員は、車両等の手段を利用して情報を搬送する場合は、情報の分類に応じ、情報の不正利用を防止するための必要な措置を講ずる。

９　情報の提供・公開

⑴　職員は、県機関以外の者に重要情報を提供する場合は、契約書等により提供先に適切な管理を保証させる。

⑵　所属長及びシステム管理者は、住民に公開する情報については完全性を確保する。

10　情報の消去・廃棄

⑴　職員は、不要となった情報は確実に消去する。

⑵　職員は、情報が記録された記録媒体を廃棄又は再利用する場合は、所属長の許可を得た上で、記録された情報が復元されないよう適切な措置を講ずる。

⑶　職員は、重要情報が記載された文書を廃棄するときは、シュレッダー等により裁断する。

第３節　実施手順書

第１　実施手順書の作成

実施手順書とは情報セキュリティポリシーに基づき、情報セキュリティ対策を実施するための手法、手順を具体的に明記したマニュアルである。

１　共通の実施手順書

全庁共通の実施手順書は情報セキュリティ委員会が作成する。

２　情報通信システム毎の実施手順書

情報通信システム毎の実施手順書はシステム管理者が作成する。手順書の内容により、運用担当者用と一般利用者用を分けて作成し、それぞれの利用範囲は明確に区分する。

なお、国等が管理する情報通信システムを利用する場合や民間事業者の提供するサービスを利用する場合は、情報通信システムを運用管理する者又はサービス提供事業者が定める実施手順書によることし、必要に応じて当該情報通信システムの利用方法を定めた利用手順書を定めることとする。ただし、情報通信システムを運用管理する者又はサービス提供事業者が定める実施手順書の内容が、情報セキュリティポリシー又は共通の実施手順書に適合しない場合は、情報セキュリティ委員会に協議したうえで利用方法を決定する。

３　組織毎の実施手順書

所属長は、共通の実施手順書及び情報通信システム毎の実施手順書（国等が管理する情報通信システムを利用する場合や民間事業者の提供するサービスを利用する場合の利用手順書を含む。以下において同じ。）に加えて、所属毎に実施手順を定める必要がある場合は、その適用範囲を明確にしたうえで実施手順書を作成する。

定めようとする実施手順書の内容が、情報セキュリティポリシー又は共通の実施手順書の規定に適合しない場合は、情報セキュリティ委員会に協議する。

定めようとする実施手順書の内容が、情報通信システム毎の実施手順書の規定に適合しない場合は、該当する情報通信システムのシステム管理者に協議する。

４　関係規定の整理

所属長は、所掌事務に関して、情報セキュリティポリシー及び各手順書に基づき、必要に応じて関係諸規程の作成または見直しを行う。

第２ 実施手順書の取扱い

情報セキュリティ委員会、システム管理者及び所属長は、実施手順書を策定または改定した時は、速やかに関係する職員に周知する。

実施手順書に重要情報が含まれる場合は、情報セキュリティポリシーに基づき適正な管理を行う。

第３ 実施手順書の改定

１　情報セキュリティ委員会、システム管理者及び所属長は、実施手順書の内容について毎年点検を行う。

２　情報セキュリティ委員会、システム管理者及び所属長は、情報通信システムの変更及び環境の変化にあわせて実施手順書を改定する。

第４節　物理的セキュリティ対策

所属長及びシステム管理者は、所管する情報通信システム機器等について以下の管理策を実施しなければならない。

第１　サーバー等の管理

１　機器の取り付け

⑴　サーバーやネットワーク機器などの重要な情報通信システム機器は、施錠が可能なラック等に設置し、適切に管理する。

⑵　情報通信システム機器の盗難を防ぐため、必要に応じて機器を設置場所に固定する物理的対策を講ずる。

２　サーバーの冗長化

重要情報を格納しているサーバー等を冗長化し、同一データを保持する。

３　機器の電源

⑴　連続的な電力の供給を必要とする情報通信システム機器には、無停電電源装置や電源の多重供給等の対策を講ずる。

⑵　落雷等による過電流に対して、サーバー等の機器を保護するための措置を講ずる。

４　電源及び通信ケーブルの配線

電源及びネットワーク等の配線を不正傍受及び損傷から保護する対策を講ずる。

５　機器の搬送

修理等のために情報通信システム機器を搬送する場合には、物理的な破損や衝撃から保護する梱包を行う。

６　機器の処分

情報通信システム機器を処分（廃棄、リース返却、再利用等）する場合は、記録された情報を消去プログラム等により完全に消去する。

第２　施設の管理

１　各事務室の管理

所属長は、事務室においては島根県庁舎等管理規則（昭和52年島根県規則第20号）及び関係規定による定めのほか、以下の管理策を実施する。

⑴　事務室において所属の職員以外の者が立ち入ることのできる範囲を明確にする。

⑵　セキュリティの重要度により事務室内を区分する必要がある場合は、それぞれの区分の範囲及び立ち入ることができる職員を明確にする。
⑶　職員が不在となる場合は、事務室を施錠する。

２　情報通信システム機器を庁舎外に設置する場合

システム管理者は、重要情報を格納する情報通信システム機器を庁舎外に設置する場合は、以下の対策を実施する。

⑴　建物及びマシン室（情報通信システム機器を設置する室）の担当者を定め、実施体制と管理責任を明確にする。
⑵　県の情報通信システム機器の存在を示す案内板や標識等は、建物の内外を問わず表示しない。
⑶　外部からの侵入や盗難を防ぐ防犯設備を導入する。
⑷　情報通信システムの安定稼働のため、空調設備を導入する。
⑸　停電、火災、自然災害等の被害を防ぐために、以下の対策を講ずる。
　①　停電に備えるため、補助電源設備を導入
　②　火災に備えるため、火災検知、消火・保護装置を導入
　③　地震に備えるため、固定器具装置等による情報通信システム機器の転倒防止策を導入
　④　設置する情報通信システム機器の重要度に応じ、落雷、津波、高潮等の自然災害に加え、漏水、ほこり、振動、化学作用、漏電、電磁波、静電気等の脅威に対する装置・設備等の導入
⑹　マシン室内への入退室の際は認証を行う。
⑺　マシン室内への入退室を記録し、定期的に確認する。
⑻　マシン室内においては、管理担当者が許可した場合を除き、以下の行為を禁止する。
　①　一般常識上、危険物と認められる物の持ち込み
　②　複写機及びＦＡＸの設置
　③　撮影及び録音
　④　喫煙及び飲食
　⑤　情報通信システム機器及び記録媒体の持ち込み
⑼　十分なセキュリティ対策がなされているか職員により定期的に確認する。
⑽　建物及びマシン室の管理を外部事業者に委託する場合は、職員が定期的に以下の項目を確認する。
　①　情報セキュリティマネジメントシステム（ＩＳＭＳ）適合性評価制度の認証を受けていること。
　②　プライバシーマーク制度の認証を受けていること。
　③　①又は②と同等の情報セキュリティシステムを確立していること。

第３　利用する端末や電磁的記録媒体の管理

所属長及びシステム管理者は、所管するモバイル端末及び電磁的記録媒体につい

て以下の対策を実施する。

1　モバイル端末及び電磁的記録媒体の管理体制及び管理責任を明確にする。

2　重要情報が格納されたモバイル端末及び電磁的記録媒体は、台帳を作成の上、施錠されたキャビネット等に保管する。

第５節　人的セキュリティ対策

職員は、情報セキュリティに関する適正な行動がとれるよう、以下のとおり対応しなければならない。

第１　職員の遵守事項

１　情報セキュリティポリシー等の遵守

⑴　職員は、情報セキュリティポリシー及び実施手順書に定められている事項を遵守する。

⑵　情報セキュリティ対策を実施するにあたって、不明な点、遵守することが困難な点等がある場合は、速やかに所属長又はセキュリティ担当者に報告し、指示に従う。

２　業務以外の目的での使用の禁止

職員は、業務以外の目的で情報通信システムへのアクセス、電子メールの使用及びインターネットへのアクセスを行ってはならない。

３　情報通信システム機器の持ち出し制限

⑴　職員は、情報通信システム機器を庁外に持ち出してはならない。ただし、所属長の許可を得た場合を除く。

⑵　職員は、電磁的記録媒体を持ち込み又は持ち出してはならない。ただし、システム管理者又は所属長の指示があった場合を除く。

４　私用の情報通信システム機器の使用禁止

職員は、私用の情報通信システム機器を庁内で情報を扱う目的で使用してはならない。

５　セキュリティ設定変更の禁止

職員は、情報通信システム機器のセキュリティ機能の設定を変更してはならない。ただし、システム管理者又は所属長の指示があった場合を除く。

６　外部ネットワークとの接続禁止

職員は、情報通信システム機器を外部ネットワークに接続してはならない。ただし、ネットワーク管理者又は所属長の許可を得た場合を除く。

７　机上の管理

⑴　職員は、情報通信システム機器を他人に使用されることがないよう、離席時のロック等の適切な措置を行う。

⑵　職員は、情報通信システム機器を使用しないときはシステムからログオフする。

⑶　職員は、勤務時間内外を問わず、記録媒体を放置してはならない。

８　退職時等の遵守事項

職員は、異動、退職等により業務を離れる場合には、業務上知り得た情報を秘匿にする。

９　ソフトウェアの利用

⑴　職員は、ソフトウェアの使用許諾条件を遵守し、不正にコピーしたソフトウェアを利用してはならない。

⑵　職員は、情報通信システム機器に新たなソフトウェアをインストールしてはならない。ただし、システム管理者又は所属長の許可を得た場合を除く。

10　電子メール及びＦＡＸの利用

⑴　職員は、電子メール又はＦＡＸにより情報を送信する前に、宛先設定及び内容が適正かどうかを再確認する。

⑵　職員は、電子メールを自動転送機能を使って転送してはならない。

⑶　職員は、不審なメールを受信したときは、開かずに直ちに削除する。

11　文書の管理

⑴　職員は、文書の管理について島根県公文書等の管理に関する条例（平成23年島根県条例第３号）及び関係規定による定めのほか、以下の事項を実施する。

①　重要情報が記載された文書の取扱いについては、所属長の指示により適切に管理する。

②　実施手順書等の情報セキュリティに関する文書は、公開する範囲を明確にする。

③　コピー機、ＦＡＸ、プリンター等には、入出力した文書を放置してはならない。

12　名札等

⑴　職員は、名札を着用し、所属を明らかにする。

⑵　職員は、電話や立ち話及び会議の発言について、盗み聞きを防止するよう配慮する。

第２　外部委託事業者に対する説明

１　所属長及びシステム管理者は、事業者等に委託して業務を実施する場合は、委託事業者（再委託を受ける事業者も含む）の守秘義務、情報セキュリティポリシー及び実施手順書に定められている事項のうち委託事業者が遵守すべき内容を契約により明確化する。

２　所属長及びシステム管理者は、契約により委託事業者（再委託を受ける事業者も含む）が行う情報セキュリティ対策の実施状況を管理する。

第３　情報セキュリティに関する研修・訓練

１　情報セキュリティ委員会は、全ての職員に対して情報セキュリティポリシーに基づく情報セキュリティ対策について啓発を行う。

２　所属長は、所属の職員に対して、情報セキュリティに関する研修を実施する。

３　システム管理者は、所管する情報通信システムの運用担当者、一般利用者及び委託事業者に対して、情報セキュリティに関する研修を実施する。

４　所属長は、臨時的任用職員及び非常勤職員に対し、採用時に情報セキュリティポリシー及び実施手順書に定めている事項を理解させる。また、必要に応じて情報セキュリティポリシー及び実施手順書に定めている事項を遵守する旨の同意書を提出させる。

５　所属長及びシステム管理者は、緊急時対応を想定した訓練を定期的に実施する。訓練計画は、情報通信システムの規模等を考慮し、訓練の実施の体制、範囲等を定め、効果的に実施できるようにする。

第４　事故等の報告

１　事故等の報告

⑴　職員は、情報セキュリティに関する事故、情報通信システムの欠陥又は誤作動を発見したとき又は住民等の外部の者から通報を受けたときは、速やかに所属長に報告する。

⑵　所属長は、報告を受けた事故等が情報通信システムに関連する場合は、速やかに当該情報通信システムのシステム管理者に報告する。

⑶　所属長又はシステム管理者は、報告を受けた事故等について、必要に応じて情報セキュリティ委員会に報告する。

２　窓口の設置等

住民等の外部の者が利用する情報通信システムのシステム管理者は、情報セキュリティに関する事故及び情報通信システムの欠陥について外部から報告を受けるための窓口を設置し、当該窓口への通信手段を公表する。

３　情報セキュリティに関する事故の原因の究明・再発防止等

情報セキュリティ委員会は、情報セキュリティに関する事故が発生した所属長又

は情報システム管理者等と連携し、事故原因を究明し、再発防止のための必要な措置を指示する。

第５　ＩＣカード、ＩＤ及びパスワード等の管理

１　ＩＣカード等の取扱い

職員は、情報通信システムの認証のためＩＣカード等の媒体を利用する場合は、次の事項を遵守する。

⑴　認証に用いるＩＣカード等を、職員間で共有してはならない。

⑵　業務上必要ないときは、ＩＣカード等をカードリーダーライター等からはずしておく。

⑶　ＩＣカード等を紛失した場合には、速やかに所属長及びシステム管理者に報告し、指示に従う。

２　ＩＤの取扱い

職員は、情報通信システムのＩＤに関し、次の事項を遵守する。

⑴　自己が利用しているＩＤは、他人に利用させてはならない。

⑵　共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

３　パスワードの取扱い

職員は、自己の管理するパスワードに関し、次の事項を遵守する。

⑴　パスワードは、他人に知られないように管理する。

⑵　パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

⑶　パスワードは、十分な長さとし、文字列は想像しにくいものにする。

⑷　パスワードを流出したおそれがある場合は、速やかにシステム管理者に報告し、パスワードを速やかに変更する。

⑸　パスワードは定期的に又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。

⑹　複数の情報通信システムを利用する職員は、同一のパスワードを情報通信システム間で用いてはならない。

⑺　仮のパスワードは、最初のログイン時点で変更する。

⑻　パソコン等の端末にパスワードを記憶させてはならない。

⑼　職員間でパスワードを共有してはならない。

第６節　技術的セキュリティ対策

システム管理者は、情報セキュリティに関する事故等の発生の防止ができるように、以下のとおり対応しなければならない。

第１　コンピューター等の管理

１　ファイルサーバーの設定等

⑴　システム管理者は、職員が使用できるファイルサーバーの容量を設定し、職員に周知する。

⑵　システム管理者は、ファイルサーバーを所属の単位で構成し、職員が他の所属のフォルダー及びファイルを閲覧及び使用できないように設定する。

⑶　システム管理者及び所属長は、重要情報を含む文書については、同一所属であっても担当者以外の職員が閲覧及び使用できないようにする。

２　データのバックアップ

⑴　システム管理者は、周期を明確に定めて、データをバックアップする。

⑵　システム管理者は、バックアップデータの完全性を確保するため、定期的にバックアップデータ及びその復元方法について確認する。

⑶　システム管理者は、重要情報をバックアップした記録媒体を、施錠されたキャビネット等で保管する。

⑷　システム管理者は、バックアップデータの世代管理を行い、データを一定期間保管する。

３　情報通信システム管理記録及び作業の確認

⑴　システム管理者は、所管する情報通信システムの運用において実施した作業について作業記録を作成する。

⑵　システム管理者は、所管する情報通信システムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理する。

⑶　システム管理者は、システム変更等の作業を行う場合は、２名以上で作業を実施し、互いにその作業を確認する。

４　情報通信システム仕様書等の管理

システム管理者は、ネットワーク構成図、情報通信システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理する。

５　情報通信システムの設定管理

⑴　システム管理者は、情報通信システムの脆弱性や脅威に関する最新の情報を常に収集し、提供元により安定稼働が保証された最新の修正プログラムを適用する。

⑵　システム管理者は、適切な性能管理を実施することにより情報通信システムの可用性を維持する。
⑶　システム管理者は、WWWサーバー等に必要に応じて改ざん検出の仕組みを設ける。
⑷　システム管理者は、メールサーバーに不正中継を防ぐ設定を行うとともに、迷惑メールへの対策を実施する。

６　ネットワークの管理

⑴　ネットワーク管理者は、情報通信機器を庁内のネットワークに接続する際の申請手順を明確にする。
⑵　ネットワーク管理者は、ネットワークの通信速度を制御し、ネットワークの性能を維持する。
⑶　インターネットに接続するネットワークのネットワーク管理者は、インターネット接続を提供している通信事業者に対して、契約書等により、適切な管理を保証させる。

７　ログの取得等

⑴　システム管理者は、情報通信システムの日常的な監視のため、情報通信システムの利用状況を監査ログに記録し、定期的に点検する。
⑵　システム管理者は、監査ログをシステム管理者及び運用担当者のみがアクセスできる領域に保存する。
⑶　運用担当者は、運用に関する作業記録を作成する。
⑷　システム管理者は、情報通信システムに問題が発生した場合には、作業記録と各種ログ情報を比較して、点検又は分析を実施する。この場合には、悪意ある第三者等からの不正アクセス、不正操作等の有無についても留意する。

８　障害記録

システム管理者は、障害の発生、調査結果、回復手段及び再発防止策についての記録を作成する。また、情報通信システムが廃止された後もその記録を一定期間保管する。

９　ファイアウォール

⑴　インターネットに接続するネットワークのネットワーク管理者は、インターネットへの接続箇所にファイアウォールを設置し、通過させるサービスは、必要最小限とする。
⑵　重要情報を取り扱う情報通信システムのシステム管理者は、当該情報通信システムが利用するネットワークを他のネットワークとは独立したネットワーク、又はそれに準ずる構成とする。また、他のネットワークと接続する場合には、厳密なアクセス制御を行う。
⑶　インターネットに接続するネットワークのネットワーク管理者は、職員による

インターネット上の有害サイトへのアクセスを制限する。

10　複合機のセキュリティ管理

⑴　所属長は、所属で独自に複合機を調達する場合、当該複合機が備える機能、設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定する。

⑵　所属長は、複合機の機能について適切な設定等を行うことにより、複合機の運用中に情報セキュリティに関する事故を防止策を講じる。

⑶　所属長は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする。

11　特定用途機器のセキュリティ管理

システム管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施する。

12　無線ＬＡＮ及びネットワークの盗聴対策

⑴　所属長及びシステム管理者は無線ＬＡＮにより庁内ネットワークへ接続してはならない。ただし、ネットワーク管理者の許可を得た場合を除く。

⑵　ネットワーク管理者は、無線ＬＡＮの利用を認める場合には、所属長及びシステム管理者に対し暗号化及びアクセス制御技術の使用を義務付ける。

13　データの暗号化

データの重要性に応じて、暗号化又はパスワード設定等を実施する。

14　ソフトウェアの管理

⑴　所属長及びシステム管理者は、それぞれのシステム又は所属で管理するソフトウェアの管理台帳を作成し、使用許諾契約書及び媒体を適切に管理する。

⑵　システム管理者は、ソフトウェアを導入する前に既存システムへの適合性等について検証を行う。

第２　アクセス制御

１　情報通信システムへのアクセス制御等

⑴　システム管理者は、情報通信システムに利用者の利用制限を認証する機能を備える。

⑵　システム管理者は、情報システムに関係する者を、システム管理者及び運用担当者、一般利用者である職員、それ以外の利用者に分類し、それぞれに必要な利用権限のみをあたえる。

⑶　システム管理者は、前項⑵に占める分類ごとに割り当てられている権限の正当

性を、定期的に確認する。

⑷　システム管理者又は運用担当者であっても、通常の用途で情報通信システムを使用する場合は、一般利用者の利用権限で使用する。

２　職員による外部からのアクセス等の制限

所属長及びシステム管理者は、リモートアクセスシステムにより庁内のネットワークに接続してはならない。ただし、業務の遂行上必要な場合で、外部環境での使用時における危険性を排除するための認証手段の強化等の対策を施し、導入についてネットワーク管理者の許可を得た場合を除く。

第３　システム開発、導入、保守等

１　情報システムの調達

⑴　システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記する。

⑵　システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認する。

２　情報システムの開発

システム管理者は、開発する情報通信システムに対して、適切なアクセス制御を行う。

３　情報システムの導入

⑴　システム管理者は、稼働中の情報通信システム等と開発する情報通信システムを分離することにより、権限のないアクセスを相互に防止する。

⑵　システム管理者は、情報通信システムの安全な導入、稼働を確認するための導入手順書を作成する。

⑶　システム管理者は、開発用に使用したソフトウェア、ＩＤ、パスワード及びＩＣカード等のデータを、本番稼働前に削除する。システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

４　システム開発・保守に関連する資料等の整備・保管

⑴　システム管理者は、開発する情報通信システムを構成する管理対象物（プログラムソース、オブジェクトコード、設計ドキュメント、障害レポート、開発記録等）を定義し、管理対象物の版数管理等を適切に管理する。

⑵　テスト結果及び使用したデータ（実際の業務データを除く）を厳重に保管する。

５　情報システムの変更管理

⑴　システム管理者は、情報通信システムの変更箇所を記録し、変更に伴う情報通信システム機器やソフトウェア等の版数管理を行う。

⑵　システム管理者は、緊急時の復旧のため、変更前の状態に戻せるようにしておく。

６　開発・保守用のソフトウェアの更新等

システム管理者は、ソフトウェアを導入する前に既存システムへの適合性等について検証を行う。

第４　不正プログラム対策

１　システム管理者は、コンピューターウイルス等の不正プログラムを検出・駆除する対策プログラムを導入し、不正プログラムによる被害の発生を予防する。

２　システム管理者は、情報通信システムに含まれる不要なプログラムを削除する。

第５　不正アクセス対策

１　システム管理者は、情報通信システムの利用者に対し、必要なサービスを必要な時間のみ提供する。

２　システム管理者は、使用されていないポートを閉鎖する。

３　システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するための対策を講じる。

４　システム管理者は、情報通信システムにおいて、標的型攻撃による内部への侵入を防止するために、攻撃を早期に検知するための対策を講じる。

第６　セキュリティ情報の収集等

１　システム管理者は、情報通信システムの脆弱性や脅威に関する最新の情報を常に収集し、開発元により安定稼働が保証された最新の修正プログラムを適用する。

２　所属長及びシステム管理者は、修正プログラムの提供やバージョンアップなど開発元のサポートが終了したソフトウェアを業務に利用してはならない。

３　情報セキュリティ委員会及びシステム管理者は、コンピューターウイルス等の情報セキュリティに関連する情報を常に収集し、職員に周知する。

第７節　運用

第１　情報通信システムの監視

１　システム管理者は、セキュリティに関する事案を検知するために、情報通信システムを常時監視する。

２　システム管理者は、情報通信システム処理結果の証拠性、信頼性を確保するために、重要なログ等を取得するサーバー等の正確な時刻設定及びサーバー間の時刻同期ができる措置を講じる。

３　システム管理者は、外部と常時接続するシステムを常時監視する。

第２　情報セキュリティポリシーの遵守状況の確認

１　遵守状況の確認及び対処

⑴　所属長又はセキュリティ担当者は、情報セキュリティポリシー及び共通の実施手順書の職員の遵守事項について必要に応じて確認を行い、違反があったときは、速やかに違反行為に対する改善を指導する。

⑵　所属長は、所属で利用している情報通信システムの実施手順書の職員の遵守状況について必要に応じて確認を行い、違反があったときは、速やかに違反行為に対する改善を指導する。

⑶　所属長又はシステム管理者は、違反行為がセキュリティ上重大な影響を及ぼす可能性があると判断した場合は、情報セキュリティ委員会に報告する。

２　情報通信システム機器等の利用状況調査

所属長又はシステム管理者は、不正アクセス、不正ソフトウエアプログラム等の調査のために、職員が使用している情報通信システム機器、記録媒体のアクセス記録、電子メールの送受信記録及びインターネットのアクセス記録等の利用状況を調査することができる。

３　職員等の報告義務

⑴　職員は、情報セキュリティポリシー及び実施手順書に対する違反行為を発見した場合、直ちに所属長又はシステム管理者に報告する。

⑵　所属長又はシステム管理者は、職員から違反行為の報告があったときは、速やかに違反行為に対する改善を指導する。

⑶　所属長又はシステム管理者は、報告を受けた違反行為がセキュリティ上重大な影響を及ぼす可能性があると判断した場合は、情報セキュリティ委員会に報告する。

第３　緊急時における情報セキュリティ対策

１　情報の安全性を侵害する事故に対する事前準備

⑴　情報セキュリティ委員会及びシステム管理者は、情報の安全性を侵害する事故の発生に備え、事故に対応する体制及び対応手順を定め、利用者に周知する。

⑵　情報セキュリティ委員会及びシステム管理者は、必要に応じて、事故対応手順に沿ってテスト及び訓練を実施する。また、訓練の結果を検証して改善点がある場合には手順を改定する。

２　情報の安全性を侵害する事故発生時の対応

⑴　所属長及びシステム管理者は情報の安全性を侵害する事故が発生した場合、事故対応手順により適切に対応するとともに情報セキュリティ委員会に報告する。

⑵　所属長及びシステム管理者は情報の安全性を侵害する事故の発生、調査結果、復旧手段について記録し、保存する。

第４　例外措置

所属長は、業務を遂行する上で、やむを得ない事情により情報セキュリティポリシーに定められている情報セキュリティ対策を実施することが困難な場合は、情報セキュリティ委員会に協議する。

第５　法令遵守

職員は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従う。

①　地方公務員法(昭和25年12月13日法律第261号)
②　著作権法（昭和45年法律第48号）
③　刑法（明治44年法律第45号）
④　不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
⑤　個人情報の保護に関する法律（平成15年５月30日法律第57号）
⑥　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）
⑦　島根県個人情報保護条例（平成14年島根県条例第７号）
⑧　島根県情報公開条例（平成12年島根県条例第52号）

第６　義務違反者に対する措置

１　情報セキュリティ委員会及びシステム管理者は、情報セキュリティポリシー及び実施手順書に違反した職員に対しその所属長を通じて改善を求める。

２　システム管理者は、所属長の指導による改善が認められない場合は、当該職員に

よる情報通信システムの利用を停止する。

3　違反した職員は、違反行為により発生した事案の状況及び重大性により、地方公務員法等による懲戒処分を含め処罰の対象となる。

第８節　外部サービスの利用

第１　外部委託

情報通信システムの外部委託を行う際は、外部委託事業者からの情報漏洩等の事故を防止するために、以下のとおり適切に対応する。

１　外部委託事業者の選定基準

⑴　所属長及びシステム管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認する。

⑵　所属長及びシステム管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者を選定する。

⑶　所属長及びシステム管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用する。

２　契約項目

情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結する。

①　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
②　外部委託事業者の責任者、委託内容、作業者、作業場所の特定
③　提供されるサービスレベルの保証
④　外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
⑤　外部委託事業者の従業員に対する教育の実施
⑥　提供された情報の目的外利用及び受託者以外の者への提供の禁止
⑦　業務上知り得た情報の守秘義務
⑧　再委託に関する制限事項の遵守
⑨　委託業務終了時の情報資産の返還、廃棄等
⑩　委託業務の定期報告及び緊急時報告義務
⑪　県による監査、検査
⑫　県による事故時等の公表
⑬　情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

３　確認・措置等

所属長は、外部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定期的に確認し、必要に応じ、２の契約に基づき措置する。

第２　約款による外部サービスの利用

１　約款による外部サービスの利用に係る規定の整備

⑴　所属長は、以下を含む約款による外部サービスの利用に関する規定を整備する。

① 約款によるサービスを利用してよい範囲
② 業務により利用する約款による外部サービス
③ 利用手続及び運用手順

２ 約款による外部サービスの利用における対策の実施

職員は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用する。

第３ ソーシャルメディアサービスの利用

所属長は、県が管理するアカウントによるソーシャルメディアサービスを適切な措置を講じた上で利用する。

第９節　情報セキュリティ対策の評価・見直し

第１　情報セキュリティ監査

１　実施方法

⑴　情報セキュリティ委員会は、内部監査を定期的又は必要に応じて実施する。
⑵　情報セキュリティ委員会は、外部監査組織による監査を必要に応じて実施する。
⑶　情報セキュリティ委員会は、監査の実施に関する責任者（以下「監査責任者」という。）を指名し、実施体制及び管理責任を明確にする。

２　監査人の要件

⑴　監査責任者は、被監査部門から独立した者を監査を行う者（以下「監査人」という。）に指名する。
⑵　監査人は、情報セキュリティ及び監査に関する専門知識を有する者とする。

３　監査実施計画の立案及び実施への協力

⑴　監査責任者は、監査計画を作成し、情報セキュリティ委員会の承認を得る。
⑵　監査責任者及び監査人は、監査計画に従い、適正に監査を実施する。
⑶　監査責任者及び監査人は、監査の過程で知り得た情報を監査以外の目的で利用しない。
⑷　被監査部門は、監査の実施に協力する。

４　報告

監査責任者は、監査結果を取りまとめた監査実施報告書を作成し、情報セキュリティ委員会に報告する。

５　保管

監査責任者は、情報セキュリティ監査の実施を通じて収集した監査証拠、監査報告書の作成のための監査調書を、適切に保管する。

６　監査結果への対応

⑴　情報セキュリティ委員会は、監査結果を踏まえ、改善事項があった情報通信システムのシステム管理者に対し、当該事項への対処を指示する。
⑵　改善の指示を受けたシステム管理者は、改善事項に対する改善計画書を作成し、情報セキュリティ委員会に提出する。

７　改善の実施及び監査結果の活用

⑴　システム管理者は、改善計画書に基づき、速やかに改善を行う。
⑵　情報セキュリティ委員会は、監査結果を情報セキュリティ対策の充実や情報セキュリティポリシー及び実施手順書の見直し、その他情報セキュリティ対策の見

直し等に活用する。

第２　自己点検

１　実施方法

⑴　所属長は、情報セキュリティポリシー及び実施手順書に基づき、情報セキュリティ対策の実施状況を毎年度自己点検する。

⑵　システム管理者は、所管する情報通信システムの情報セキュリティ対策の実施状況について、毎年自己点検を実施する。

⑶　所属長及びシステム管理者は、点検結果と改善策を取りまとめ、情報セキュリティ委員会に報告する。

２　改善の実施及び点検結果の活用

⑴　所属長及びシステム管理者は、改善策に基づき、速やかに改善を行う。

⑵　情報セキュリティ委員会は、この点検結果を情報セキュリティ対策の充実や、情報セキュリティポリシー及び実施手順書の見直し、その他情報セキュリティ対策の見直し時に活用する。

第３　情報セキュリティポリシーの見直し

情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシーの見直し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。

第10節 用語の定義

情報セキュリティポリシーおいて次の各号に掲げる用語の定義は、当該各号に定めるところによる。

【さ】

●「サイバー攻撃」

「サイバー攻撃」とは、コンピュータシステムやインターネットなどを利用して、標的のコンピューターやネットワークに不正に侵入してデータの詐取や破壊、改ざんなどを行なったり、標的のシステムを機能不全に陥らせることをいう。

●「サービス不能攻撃」

「サービス不能攻撃」とは、通信ネットワークを通じてコンピューターや通信機器などに行われる攻撃手法の一つで、大量のデータや不正なデータを送りつけて相手方のシステムを正常に稼働できない状態に追い込むことをいう。

●「ＣＳＩＲＴ（シーサート、Computer Security Incident Response Team)」

「ＣＳＩＲＴ」とは、コンピュータやネットワーク（特にインターネット）上で何らかの問題（主にセキュリティ上の問題）が起きていないかどうかを監視すると共に、万が一問題が発生した場合にその原因解析や影響範囲の調査を行ったりする組織の総称をいう。

●「情報セキュリティマネジメントシステム（ＩＳＭＳ)」

「情報セキュリティマネジメントシステム（ＩＳＭＳ)」とは、個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用することをいう。

●「ソーシャルメディアサービス」

「ソーシャルメディアサービス」とは、インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持ったＷｅｂサイトやネットサービスなどを総称する用語で、電子掲示板(ＢＢＳ)やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄などを含む。

【た】

●「端末」

「端末」とは、情報システムの構成要素である機器のうち、職員が情報処理を行

うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りが無い限り、地方公共団体が調達又は開発するものをいう。

●「特定用途機器」

「特定用途機器」とは、テレビ会議システム、ＩＰ電話システム、ネットワークカメラシステム等の特定用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵しているものをいう。

【は】

●「パソコン」

「パソコン」とは、端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいい、端末の形態は問わない。

●「標的型攻撃」

「標的型攻撃」とは、明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。

●「ファイアウォール」

「ファイアウォール」とは、あるコンピューターやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システムなどのことをいう。

●「複合機」

「複合機」とは、プリンター、ＦＡＸ、イメージスキャナー、コピー機等の機能が一つにまとめられている機器のことをいう。

●「プライバシーマーク」

「プライバシーマーク」とは、個人情報保護に関して一定の要件を満たした事業者に対し、一般財団法人日本情報経済社会推進協会（ＪＩＰＤＥＣ）により使用を認められる登録商標の事をいう。

【ま】

●「モバイル端末」

「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

【や】

●「約款による外部サービス」

「約款による外部サービス」とは、民間事業者等の庁外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバー装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。

附　則

本情報セキュリティポリシーは平成19年4月1日から施行する。
本情報セキュリティポリシーは平成24年4月1日から施行する。
本情報セキュリティポリシーは平成25年4月1日から施行する。
本情報セキュリティポリシーは平成26年4月1日から施行する。
本情報セキュリティポリシーは平成27年9月1日から施行する。
本情報セキュリティポリシーは平成29年4月1日から施行する。