島根県情報セキュリティポリシー

令和５年４月
島根県

目次

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、会計年度任用職員、非常勤職員及び臨時的任用職員）(以下、「職員等」という。）並びに業務委託事業者に浸透、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。

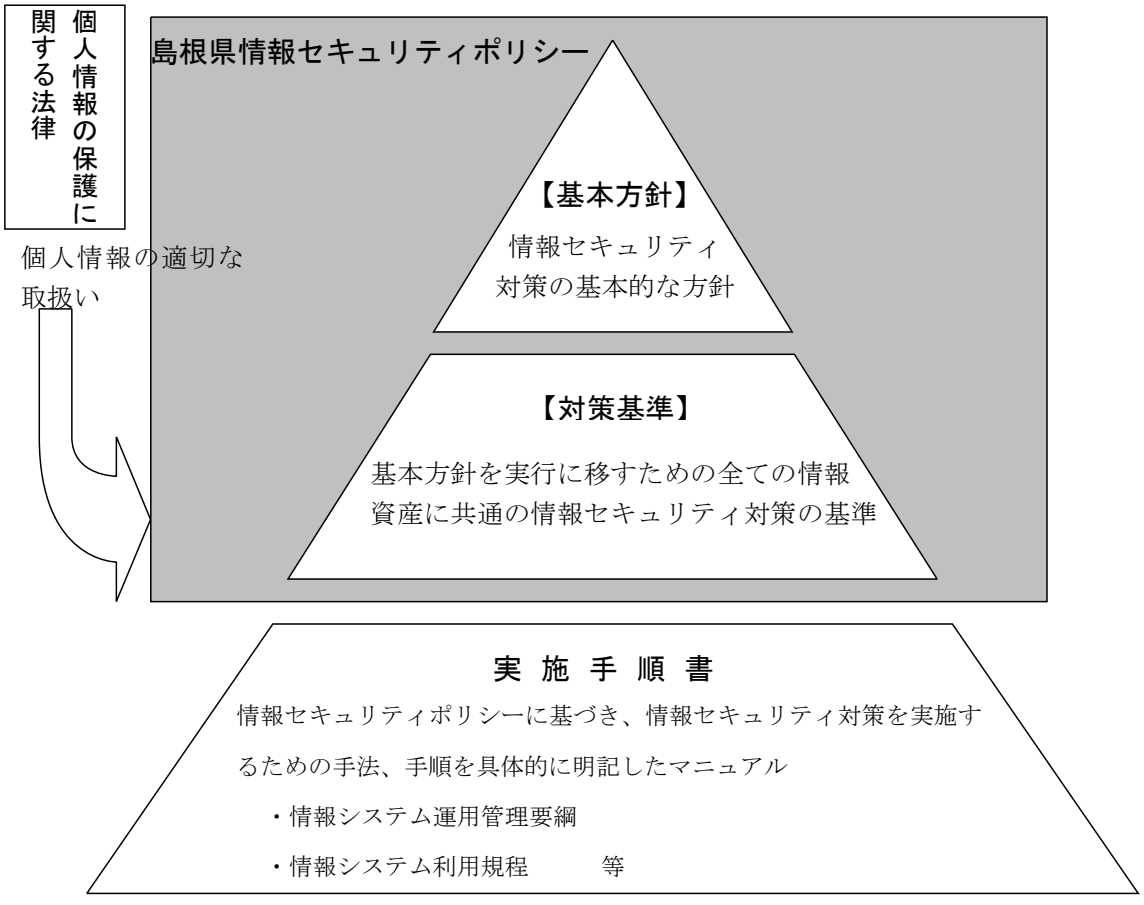
このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（セキュリティ基準）で構成する。

「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

１　目　的

この基本方針は、県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、県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　情報資産

情報及び情報システムをいう。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　情報セキュリティポリシー

情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。

⑺　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。

⑻　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。

⑼　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。

⑽　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」に規定された個人番号利用事務に関わる情報システムをいう。

⑾　行政系

職員等が一般行政事務に使用することを目的とし、総合行政ネットワーク（以下、「ＬＧＷＡＮ」という。）に接続された情報システムをいう（マイナンバー利用事務系を除く。）。

⑿　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をいう。

⒀　通信経路の分割

行政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。

⒁　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ない等、安全が確保された通信をいう。

⒂　情報セキュリティインシデント

単独もしくは一連の望まないあるいは予期しない情報セキュリティに関する事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。具体的にはサイバー攻撃、意図的な要因による情報漏えい、破壊、改ざん、機器故障等の非意図的な要因による情報漏えい、破壊、改ざん等をいう。

３　対象とする脅威

情報資産に対する脅威として、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

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、水道供給の途絶等のインフラの障害からの波及等

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。

５　職員等の義務

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

県の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

⑵　情報資産の分類と管理

県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、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、重要情報の流出を防ぐ。

② 行政系においては、行政系の情報システムと、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。高度な情報セキュリティ対策として、県及び市町村のインターネットとの通信を集約した上で、しまねセキュリティクラウドの導入等を実施する。

⑷　物理的セキュリティ

サーバー、情報システム室、通信回線及び職員等のパソコンやモバイル端末の管理について、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

コンピュータ等の管理、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。

⑺　運用

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、緊急時対応計画を策定する。

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（再委託事業者等も含む）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。

外部サービスを利用する場合には、利用にかかる規程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。

７　情報セキュリティ監査及び自己点検の実施

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監査及び自己点検を実施する。

８　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、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には、情報セキュリティポリシーを見直す。

９　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより県の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

第２章　情報セキュリティ対策基準

１　情報セキュリティの管理体制

１．１．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。

⑴　最高情報セキュリティ責任者（CISO:Chief Information Security Officer、以下「ＣＩＳＯ」という。）

①　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。

②　ＣＩＳＯは、副知事をもって充てる。

③　ＣＩＳＯは、情報セキュリティ委員会を招集し、主宰する。

④　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。

⑤　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、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。

⑵　統括情報セキュリティ責任者

①　ＣＩＳＯを補佐する者として、統括情報セキュリティ責任者を置く。

②　統括情報セキュリティ責任者は、総務部長をもって充てる。

③　統括情報セキュリティ責任者は、ＣＩＳＯが不在の場合及び前項⑤に基づきＣＩＳＯの代行を命じられた場合に、その任にあたる。

④　統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じてＣＩＳＯにその内容を報告しなければならない。

⑶　情報セキュリティ委員会

①　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。

②　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。

③　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。

④　情報セキュリティ委員会は、全庁共通の情報セキュリティ実施手順書を作成する。

⑤　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。

⑷　島根県ＣＳＩＲＴ（シーサート）

①　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及び統括情報セキュリティ責任者の指揮のもと、島根県ＣＳＩＲＴを置く。

②　島根県ＣＳＩＲＴの構成員は、統括情報セキュリティ責任者が情報セキュリティ委員、総務部情報システム推進課職員及び委託事業者等の中から指名する。

　なお、ＣＳＩＲＴの責任者を置き、ＣＳＩＲＴ内の業務統括、外部との連携等を行う職員などを定めることとし、体制図のとおりとする。

③　島根県ＣＳＩＲＴは、初動対応を迅速かつ機動的に遂行するために必要となる権限をＣＩＳＯ及び統括情報セキュリティ責任者から付与されるものとし、情報セキュリティインシデントが発生した場合は、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を始め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。

④　島根県ＣＳＩＲＴは、ＣＩＳＯによる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等へ提供する。

⑤　島根県ＣＳＩＲＴは、情報セキュリティインシデントを認知した場合には、ＣＩＳＯ、総務省等へ報告するとともに、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行う。

⑥　全ての実施機関は、島根県ＣＳＩＲＴ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。

⑦　島根県ＣＳＩＲＴは、情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行う。

⑸　情報セキュリティ推進班

①　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ことができる。

②　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。

③　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。

④　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。

⑤　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。

⑹　情報セキュリティ委員会事務局

①　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、総務部情報システム推進課が所掌する。

②　情報システム推進課長は、情報セキュリティ推進班を招集し、主宰する。

⑺　システム管理者

①　各情報システムにおいて、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。

②　システム管理者は、各情報システムの運用管理を行う所属の長をもって充てる。

③　システム管理者は、所管する情報システムにおける開発、設定の変更、運用、更新等を行う権限及び責任を有する。

④　システム管理者は、所管する情報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。

⑤　新たな情報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。

⑥　システム管理者は、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必要と認める時は、その任を代行させる者を指定することができる。

⑻　ネットワーク管理者

システム管理者のうち、もっぱらネットワークの適正な運用管理を行うため、ネットワーク管理者を置く。

⑼　運用（開発）担当者

①　システム管理者を補助し、情報システムの適切な利用を推進するため、各情報システムに運用（開発）担当者を置く。

②　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。

③　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システム推進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。

⑽　所属長

①　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。

②　所属内で情報セキュリティに関する研修及び啓発を定期的に行う。

⑾　セキュリティ担当者

①　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。

②　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。

③　所属長は、毎年度、セキュリティ担当者の職指名を情報システム推進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。

④　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。

(ｱ)　コンピュータウイルス対策の徹底

(ｲ)　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

⑤　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。

⑿　職員等

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。

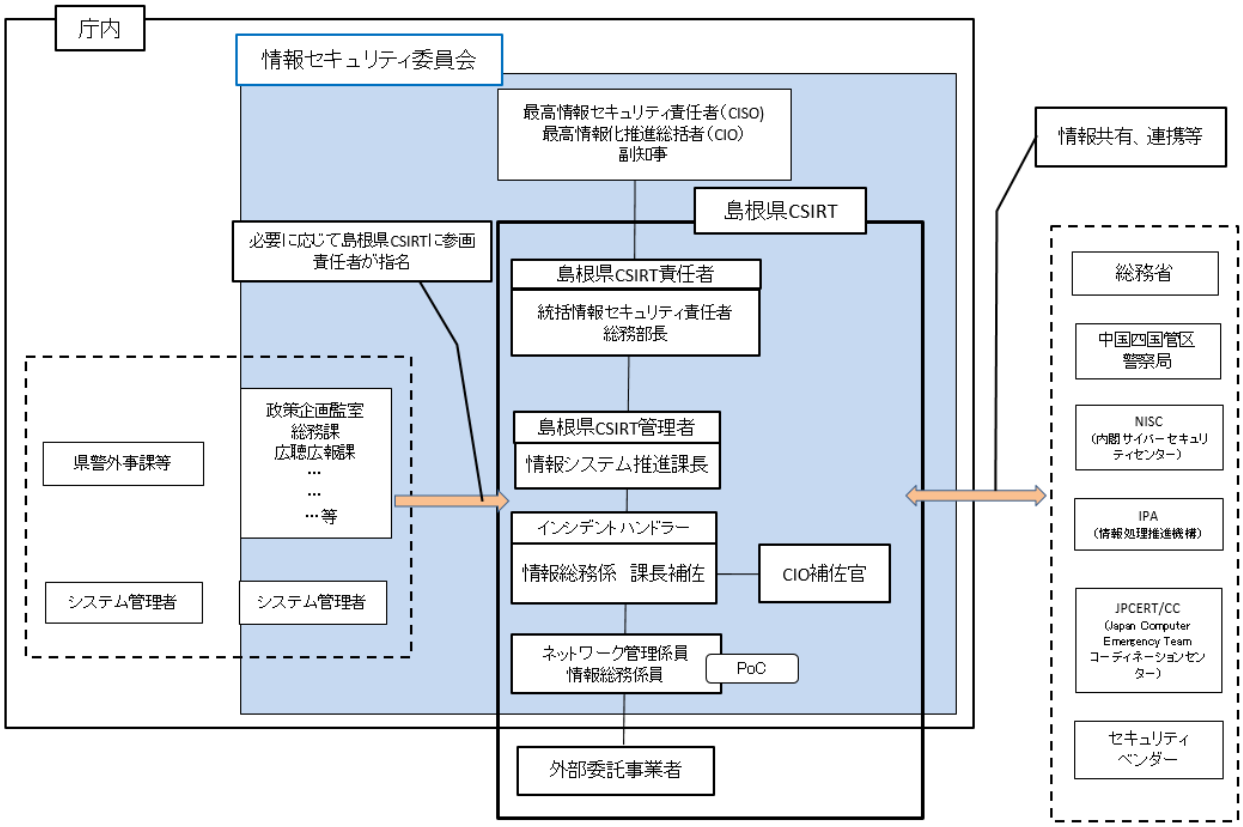
１．２．兼務の禁止

⑴　情報セキュリティ対策の実施において、止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。

⑵　情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、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

委員長		最高情報セキュリティ責任者（ＣＩＳＯ）
委員長代理		統括情報セキュリティ責任者
委員	政策企画局	政策企画監、広聴広報課長
	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、情報システム推進課長
	防災部	消防総務課長
	地域振興部	地域政策課長、デジタル戦略室長、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



参考　島根県 CSIRT 体制図

２　情報の分類と管理

２．１．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。

⑴　重要情報

①　個人情報の保護に関する法律（平成 15 年法律第 57 号）に規定する個人情報及び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）に規定する特定個人情報

②　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

③　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

⑵　一般情報

重要情報以外の全ての情報

２．２．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、職員等、運用（開発）担当者及び業務委託事業者等に適切に取り扱うよう指示する。

２．３．情報の分類の表示

職員等は、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。

２．４．情報の作成

⑴　職員等は、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。

２．５．情報の入手

⑴　職員等は、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　職員等は、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等は、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。

２．６．情報の利用

⑴　職員等は、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等は、情報の分類に応じ、適切に取り扱う。

２．７．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。

２．８．情報の伝送・送付

⑴　職員等は、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パスワード等による暗号化などの適切な措置を講ずる。

⑵　職員等は、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。

２．９．情報の搬送

職員等は、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パスワード等による暗号化などの措置を講ずる。

２．10．情報の提供・公開

⑴　職員等は、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　職員等は、県機関以外の者に重要情報を提供する場合は、所属長の許可を得る。

⑶　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。

２．11．情報の消去・廃棄

⑴　職員等は、不要となった情報は確実に消去する。

⑵　職員等は、情報が記録された電磁的記録媒体を廃棄やリース返却等する場合は、所属長の許可を得た上で、記録されている情報の重要性に応じ、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。その際に、行った処理について、日時、担当者及び処理内容を記録する。

なお、重要情報のうち、特定個人情報を含むものは、廃棄する。

⑶　職員等は、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。

3　情報システム全体の強靭性の向上

⑴　マイナンバー利用事務系

①　マイナンバー利用事務系と他のネットワークとの分離

マイナンバー利用事務系と他のネットワークを通信できないようにしなければならない。マイナンバー利用事務ネットワークと外部との通信をする必要がある場合は、通信経路等を限定しなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、ＬＧＷＡＮを経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送は可能とする。

②　情報のアクセス及び持ち出しにおける対策

(ｱ)　情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する多要素認証を利用しなければならない。また、原則、業務毎に専用端末を設置する。

(ｲ)　情報の持ち出し不可設定

原則として、ＵＳＢメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

⑵　行政系

①　行政系とインターネット接続系の分割

行政系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを行政系ネットワークに取り込む場合は、次の方法等により、無害化通信を図らなければならない。

(ｱ)　インターネット環境で受信したインターネットメールの本文のみを行政系に転送するメールテキスト化方式

(ｲ)　インターネット接続系の端末から、行政ネットワークの端末へ画面を転送する方式

(ｳ)　危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

⑶　インターネット接続系

①　インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及びＬＧＷＡＮへの不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

②　県及び市町村のインターネットとの通信を集約するしまねセキュリティクラウドに参加するとともに、総務省等と連携しながら、情報セキュリティ対策を推

進しなければならない。

４　物理的セキュリティ

所属長及びシステム管理者は、所管する情報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。

４．１．サーバ等の管理

⑴　機器等の管理

所属長及びシステム管理者は、所属又はそれぞれのシステムで管理する機器及びソフトウェアの台帳等を作成し、作動要件、使用許諾契約内容、ライセンス証書等を適切に管理する。

⑵　機器の取付け

システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じ、定期的に当該機器の設置状況を確認する。

⑶　サーバの冗長化

①　システム管理者は、重要情報を格納しているサーバ等を冗長化し、同一データを保持するよう努める。

②　システム管理者は、サーバに障害が発生した場合には、情報システムの運用停止時間を最小限にするよう努める。

⑷　機器の電源

①　システム管理者は、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源等を備え付ける。

②　システム管理者は、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じる。

⑸　通信ケーブル等の配線

①　システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じる。

②　システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応する。

③　システム管理者は、ネットワークの接続口を関係者以外が容易に接続できない場所に設置する等適正に管理する。

④　システム管理者は、自ら又は運用（開発）担当者及び契約により操作を認められた委託事業者以外の者が配線を変更、追加できないように必要な措置を講じ

る。

⑹ 機器の保守及び修理

① システム管理者は、サーバ等の機器に対し必要に応じて保守を実施する。

② システム管理者は、電磁的記録媒体を内蔵する機器を委託事業者に修理させる場合、内容を消去した状態で行わせる。内容を消去できない場合、システム管理者は、修理を委託する事業者と守秘義務契約を締結するほか、秘密保持体制の確認等を行う。

⑺ 庁外への機器の設置

システム管理者は、庁外にサーバ等の機器を設置する場合、定期的に当該機器への情報セキュリティ対策状況について確認する。

⑻ 機器の廃棄等

システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じる。

４．２．施設の管理

⑴ 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。

① 事務室において所属の職員等以外の者が立ち入ることのできる範囲を明確にする。

② 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等を明確にする。

③ 職員等が不在となる場合は、事務室を施錠する。

⑵ 管理区域の構造等

① 管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいい、場所は庁舎内外を問わない。

② システム管理者は、管理区域の担当者を決め、実施体制と管理責任を明確化する。

③ システム管理者は、管理区域の存在を示す案内板や標識等は設置しない。

④ システム管理者は、管理区域に鍵、監視機能又は警報装置等を設置して、外部から容易に侵入できないようにする。また、管理区域を囲む外壁等の床下開口部を塞ぐように努める。

⑤ システム管理者は、情報システムの安定稼働のために空調設備を導入する。

⑥ システム管理者は、管理区域内の情報システムに停電、火災及び自然災害等による被害発生を防止するための措置を講じる

⑦　システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにする。

⑶　管理区域の入退室管理等

①　システム管理者は、管理区域への入退室は許可された者のみに制限し、生体認証や入退室管理簿、ＩＣカードの記載による入退室管理を行い、定期的に認証内容を確認する。

②　職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示する。

③　システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じる。

④　システム管理者は、管理区域に入室する者について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体及び一般通念上危険物と認められる物を持ち込ませないようにする。

⑤　職員等は、管理区域内で撮影、録音、喫煙、飲食を行ってはならない。

⑷　機器等の搬入出

①　システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ確認する。

②　システム管理者は、情報システム室の機器等の搬入出について、職員あるいは委託事業者を立ち会わせる。

４．３．通信回線及び通信回線装置の管理

⑴　システム管理者は、庁内の通信回線及び通信回線装置を、適正に管理する。また、通信回線及び通信回線装置に関連する文書を適正に保管する。

⑵　システム管理者は、外部へのネットワーク接続を必要最低限に限定する。

⑶　システム管理者は、情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択する。また、必要に応じ、送受信される情報の暗号化を行う。

⑷　システム管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施する。

⑸　システム管理者は、情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択し、必要に応じて回線を冗長構成にする等の措置を講じる。

４．４．職員等の利用する端末や電磁的記録媒体等の管理

⑴　所属長は、各端末等の管理規程により適切に管理する。執務室内では、盗難防止のため、執務室の施錠、ワイヤーによる固定、使用時以外の施錠管理等の物理的措

置を講じる。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去する。

⑵　システム管理者は、情報システムへのログインに際し、パスワード、スマートカード、あるいは生体認証等の認証情報の入力を必要とするように設定する。

⑶　システム管理者は、端末の電源起動時のパスワード等の併用を検討する。

⑷　システム管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する多要素認証を行うよう設定する。

⑸　システム管理者は、パソコンやモバイル端末等にセキュリティチップが搭載されている場合、その機能を有効に活用する。同様に、電磁的記録媒体についてもデータ暗号化機能を備える場合には有効に使用する。

⑹　システム管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、必要に応じて遠隔消去機能等の措置を講じる。

⑺　システム管理者は、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限する。

５　人的セキュリティ

職員等は、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。

５．１．職員等の遵守事項

⑴　職員等の遵守事項

①　情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守する。また、情報セキュリティ対策について不明な点、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相談し、指示を仰がなければならない。

②　業務以外の目的での使用等の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレス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　モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

(ｱ)　所属長は、重要情報を外部で処理する場合における安全管理措置を定める。

(ｲ)　職員等は、モバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部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。

(ｳ)　職員等は、外部で情報処理業務を行う場合には、所属長の許可を得る。所属長は、端末等の持ち出し及び持ち込みについて、記録を作成する。なお、外部における情報処理業務は、情報セキュリティへの脅威が増すので、業務遂行にあたり、本ポリシーや実施手順書、実施要領等の規定を遵守し、関係機関の示すガイドラインを参考に、細心の注意を払って行わなければならない。

④　支給以外のパソコン、モバイル端末及び電磁的記録媒体等の使用禁止

(ｱ)　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断をＣＩＳＯが行った後に、災害時等業務上必要かつやむを得ない場合は、統括情報セキュリティ責任者の定める手順に従い、所属長の許可を得て利用することができる。

(ｲ)　職員等は、(ｱ)に従って支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、外部で情報処理作業を行う場合にも安全管理措置に関する規定を遵守する。

⑤　セキュリティ設定変更及び機器構成の変更の禁止

(ｱ)　職員等は、セキュリティ機能の設定をシステム管理者の許可なく変更してはならない。

(ｲ)　パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

(ｳ)　職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行

ってはならない。ただし、業務上必要がある場合には、システム管理者の許可を得る。

⑥　業務外ネットワークへの接続の禁止

職員等は、パソコンやモバイル端末を、有線・無線を問わず、その端末を接続して利用するようシステム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

⑦　机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じる。

⑧　無許可ソフトウェアの導入等の禁止

(ｱ)　職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

(ｲ)　職員等は、業務上の必要がある場合は、システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、ソフトウェアのライセンスを適切に管理する。

(ｳ)　職員等は、不正にコピーしたソフトウェアを利用してはならない。

⑨　電子メール及びＦＡＸの利用

(ｱ)　職員等は、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。

(ｲ)　職員等は、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。

⑩　電子メールの利用制限

(ｱ)　職員等は、自動転送機能を用いて、電子メールを転送してはならない。

(ｲ)　職員等は、業務上必要のない送信先に電子メールを送信してはならない。

(ｳ)　職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにする。

(ｴ)　職員等は、重要情報を送信する場合等必要に応じて、パスワード等による添付ファイルの暗号化等、セキュリティを考慮する。

(ｵ)　職員等は、電子メールを誤送信した場合、所属長に報告しなければならない。

(ｶ)　職員等は、プロバイダーが提供するサービスである電子メールやオンラインストレージサービス等をネットワーク管理者の許可なく使用してはならない。

⑪　不正プログラム対策

(ｱ)　行政系に外部からデータを取り入れる場合には、原則として無害化処理を行う。

(ｲ)　差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除する。

(ｳ)　システム管理者が提供するウイルス情報を、常に確認しなければならない。
(ｴ)　インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、県が管理している媒体以外を利用してはならない。
(ｵ)　コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、システム管理者が定める手順により適切に対応する。
(ｶ)　外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
(ｷ)　パソコンやモバイル端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。
(ｸ)　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

⑫　文書の管理

職員等は、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。

(ｱ)　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。
(ｲ)　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。
(ｳ)　複合機、コピー機、ＦＡＸ、プリンタ等には、入出力した文書を放置してはならない。

⑬　名札等

(ｱ)　職員等は、名札を着用し、所属を明らかにする。
(ｲ)　職員等は、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。

⑭　退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を、返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

⑵　情報セキュリティポリシー等の掲示

統括情報セキュリティ責任者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるようにする。

⑶　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、情報システムの開発・保守等を事業者に発注する場合、委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項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（再委託事業者を含む）

が行う情報セキュリティ対策の実施状況を管理する。

５．２．研修・訓練

⑴　情報セキュリティに関する研修・訓練

情報セキュリティ委員会は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

⑵　研修計画の策定及び実施

①　情報セキュリティ委員会は、全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行う。

②　研修計画において、職員等は定期的に情報セキュリティ研修を受講できるようにする。

③　所属長は、所属の職員等に対して、情報セキュリティに関する研修を毎年度実施する。

④　システム管理者は、所管する情報システムの運用（開発）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。

⑤　所属長は、会計年度任用職員等に対し、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。

⑥　所属長は、研修の実施状況を記録し、統括情報セキュリティ責任者に報告しなければならない。

⑦　統括情報セキュリティ責任者は、研修の実施状況を分析、評価し、ＣＩＳＯに情報セキュリティ対策に関する教育の実施状況について報告しなければならない。

⑶　緊急時対応計画の策定及び訓練

システム管理者は、緊急時対応計画を策定し、緊急時を想定した対応訓練を定期的に実施する。緊急時対応計画は必要に応じて見直す。

⑷　研修・訓練への参加

全ての職員等は、定められた研修・訓練に参加する。

５．３．情報セキュリティインシデントの報告

⑴ 情報セキュリティインシデントの報告

① 職員等は、情報セキュリティインシデントに関して認知あるいは通報を受けた場合、速やかに所属長、セキュリティ担当者及びシステム管理者に報告する。

② 前号により報告を受けた所属長及びシステム管理者は、島根県ＣＳＩＲＴに概要を報告する。

⑵ 窓口の設置等

住民等の外部の者が利用する情報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。

⑶ 情報セキュリティインシデント原因の究明・記録、再発防止等

① 島根県ＣＳＩＲＴは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行う。

② 島根県ＣＳＩＲＴは、情報セキュリティインシデントであると評価した場合、ＣＩＳＯに速やかに報告する。

③ 島根県ＣＳＩＲＴは、情報セキュリティインシデントに関係するシステム管理者等に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行う。

④ 島根県ＣＳＩＲＴは、情報セキュリティインシデント原因を究明し、記録する。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、ＣＩＳＯ に報告する。

⑤ ＣＩＳＯは、島根県ＣＳＩＲＴから、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示する。

５．４．ＩＤ及びパスワード等の管理

⑴ ＩＤの取扱い

職員等は、自己の管理するＩＤに関し、次の事項を遵守する。

① 自己が利用しているＩＤは、他人に利用させてはならない。

② 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。

⑵ パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守する。

① パスワードは、他者に知られないように管理する。

② 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。

③ 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。

④ パスワードが流出したおそれがある場合には、システム管理者に速やかに報告し、パスワードを速やかに変更する。

⑤　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
⑥　仮のパスワード（初期パスワード含む）は、最初のログイン時に変更する。
⑦　サーバ、ネットワーク機器及びパソコンやモバイル端末に原則としてパスワードを記憶させてはならない。
⑧　職員等間でパスワードを共有してはならない。ただし、共用ＩＤに対するパスワードは除く。

⑶　ＩＣカード等の取扱い

①　職員等は、自己の管理するＩＣカード等に関し、次の事項を遵守する。
　(ｱ)　認証に用いるＩＣカード等を、職員等間で共有してはならない。
　(ｲ)　業務上必要のないときは、ＩＣカード等をカードリーダ又はパソコンやモバイル端末のスロット等から抜いておく。
　(ｳ)　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通報し、指示に従う。
②　システム管理者は、ＩＣカード等の紛失等の通報があり次第、当該ＩＣカード等を使用したアクセス等を速やかに停止する。
③　システム管理者は、ＩＣカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄する。

６　技術的セキュリティ

６．１．コンピュータ及びネットワークの管理

システム管理者は、情報セキュリティインシデントの発生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。

⑴　ファイルサーバーの設定等

①　システム管理者は、職員等が使用できるファイルサーバーの容量を設定し、職員等に周知する。

②　システム管理者は、ファイルサーバーを所属単位で構成し、職員等が他所属のフォルダ及びファイルを閲覧及び使用できないように、設定する。

③　システム管理者は、重要情報等、特定の職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一所属であっても、担当職員以外の職員等が閲覧及び使用できないようする。

⑵　バックアップの実施

①　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。

②　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。

③　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。

④　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。

⑶　他団体との情報システムに関する情報等の交換

システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定める。

⑷　システム管理記録及び作業の確認

①　システム管理者は、所管する情報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。

②　システム管理者は、所管する情報システムにおいて、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正に管理する。

③　システム管理者又は運用（開発）担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認する。

⑸　情報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、情報システム仕様書、設計書及びマニ

ュアル等について、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、適正に管理する。

⑹　ログの取得等

①　システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存する。

②　システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理する。

③　システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施する。

⑺　障害記録

システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録する。

⑻　ネットワークの接続制御、経路制御等

①　ネットワーク管理者は、経路制御等について、不整合が発生しないように、ファイアウォール、ルータ等を設定する。

②　ネットワーク管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施す。

⑼　ファイアウォール

①　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。

②　重要情報を取り扱う情報システムのシステム管理者は、当該情報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。

③　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、職員等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。

⑽　外部の者が利用できるシステムの分離等

システム管理者は、電子申請受付システム等、外部の者が利用できる情報システムについて、必要に応じて他のネットワーク及び情報システムと物理的、あるいは論理的に分離する等の措置を講じる。

⑾　外部ネットワークとの接続制限等

①　ネットワーク管理者は、所管するネットワークを外部ネットワークと接続しよ

うとする場合には、ＣＩＳＯ及び統括情報セキュリティ責任者の許可を得なければならない。

② ネットワーク管理者は、接続しようとする外部ネットワークに係るネットワーク構成等を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認する。

③ システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保する。

④ 統括情報セキュリティ責任者及びシステム管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続する。

⑤ ネットワーク管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断する。

⑿ 複合機のセキュリティ管理

① 所属長は、複合機を調達する場合、当該複合機が備える機能及び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、適正なセキュリティ要件を策定する。

② 所属長は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じる。

③ 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する又は再利用できないようにする対策を講じる。

⒀ ＩｏＴ機器を含む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講じる。

⒁ 無線ＬＡＮ及びネットワークの盗聴対策

① ネットワーク管理者は、無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付ける。

② ネットワーク管理者は、重要情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、必要に応じて暗号化等の措置を講じる。

⒂ 電子メールのセキュリティ管理

① システム管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバを設定する。

② システム管理者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止する。
③ システム管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にする。
④ システム管理者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知する。
⑤ システム管理者は、システム開発や運用、保守等のため庁舎内に常駐している委託事業者による電子メールアドレス利用について、委託事業者との間で利用方法を取り決める。

⑯ Ｗｅｂ会議サービスの利用時の対策

① 統括情報セキュリティ責任者は、Ｗｅｂ会議を適切に利用するための利用手順を定めなければならない。
② 職員等は、利用手順に従い、Ｗｅｂ会議の参加者や取り扱う状況に応じた情報セキュリティ対策を実施する。
③ 職員等は、Ｗｅｂ会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずる。
④ 職員等は、外部からＷｅｂ会議に招待される場合は、利用手順に従い、必要に応じた対応をしなければならない。

⑰ ソーシャルメディアサービスの利用

① 所属長は、県が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。
(ｱ) 県のアカウントによる情報発信が、実際の所属のものであることを明らかにするために、県管理Ｗｅｂサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。
(ｲ) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、ＵＳＢ、メモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。
(ｳ) 「島根県ソーシャルメディア利用指針」記載の必要事項。
② 重要情報は、ソーシャルメディアサービスで発信してはならない。
③ 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なければならない。
④ アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。
⑤ 住民の権利が侵害される又は行政事務の安定的な遂行に支障を及ぼすおそれのある情報の提供にソーシャルメディアサービスを用いる場合は県管理Ｗｅｂサイトに当該情報を掲載して参照可能とする。

６．２．アクセス制御

⑴ アクセス制御等

① アクセス制御

システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限する。

② 利用者ＩＤの取扱い

(ｱ) システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定める。

(ｲ) 職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、システム管理者に報告する。

(ｳ) システム管理者は、利用されていないＩＤが放置されないよう点検する。

③ 特権を付与された利用者ＩＤの取扱い

(ｱ) システム管理者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理する。

(ｲ) システム管理者は、特権を付与されたＩＤ及びパスワードについて、職員等の端末等のパスワードよりもセキュリティ機能を強化する。

(ｳ) システム管理者は、特権を付与されたＩＤを初期設定以外のものに変更する。

⑵ 職員等による外部からのアクセス等の制限

① 職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、ネットワーク管理者及び当該情報システムを管理するシステム管理者の許可を得る。

② 内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止する。やむを得ず、内部のネットワーク又は情報システムに外部からアクセスする場合は、ネットワーク管理者及び当該情報システムを管理するシステム管理者は、アクセスが必要な合理的理由を有する必要最小限の者に限定する。

③ ネットワーク管理者及びシステム管理者は、外部からのアクセスを認める場合、外部環境での使用時における危険性を排除するための職員等及び端末の認証手段の強化等の対策を施すと共に、通信途上の盗聴を防御するために暗号化等の措置を講じる。

④ ネットワーク管理者及び当該情報システムを管理するシステム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講ずる。

⑤ 職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末等を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、修正プログラムの適用状況等を確認し、所属長の許可を得るか、もしくは事前に定義されたポリシーに従って接続しなければならない。

６．３．システム開発、導入、運用、保守等

⑴ 情報システムの調達

① システム管理者は、情報システム開発、導入、運用、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。

② 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。

⑵ 情報システムの開発

① システム開発における責任者及び作業者の特定

システム管理者は、システム開発の責任者及び作業者を特定する。また、システム開発のための規定を定める。

② システム開発における責任者、作業者のＩＤの管理

(ｱ) システム管理者は、システム開発の責任者及び作業者が使用する開発用ＩＤを管理し、開発完了後、開発用ＩＤ を削除する。

(ｲ) システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定する。

③ システム開発に用いるハードウェア及びソフトウェアの管理

(ｱ) システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定する。

(ｲ) システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除する。

⑶ 情報システムの導入

① 開発環境と運用環境の分離及び移行手順の明確化

(ｱ) システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離する。

(ｲ) システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にする。

(ｳ) システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮する。

② テスト

(ｱ) システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行う。

(ｲ) システム管理者は、原則として重要情報をテストデータに使用してはならない。やむを得ず重要情報を含むデータをテストに利用する場合には、システム運用環境と同様の機密性が保たれるよう対策を講じた上で、所属長の承認を得る。

(ｳ) システム管理者は、テスト時において運用環境の情報を誤って書き換えて

しまうことがないよう対策を行う。

(ｴ)　システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行う。

⑷　システム開発、運用、保守に関連する資料等の整備・保管

①　システム管理者は、システム開発、運用、保守に関連する資料及びシステム関連文書を適正に整備保管する。

②　システム管理者は、テスト結果及びテストデータを一定期間保管する。

③　システム管理者は、情報システムに係るソースコードを適正な方法で保管する。

⑸　情報システムにおける入出力データの正確性の確保

①　システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計する。

②　システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計する。

③　システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計する。

⑹　情報システムの変更管理

システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成する。

⑺　開発、運用、保守用のソフトウェアの更新等

システム管理者は、開発、運用、保守用のソフトウェア等を更新又は修正プログラムを適用する場合、他の情報システムとの整合性を確認する。

⑻　システム更新又は統合時の検証等

システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行う。

６．４．不正プログラム対策

⑴　システム管理者の措置事項

システム管理者は、不正プログラム対策として、次の事項を措置しなければならない。

①　外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止する。

②　外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止する。

③　添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行う。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを行政系に取込む場合は無害化する。

④　コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起する。

⑤　所掌するサーバ及びパソコンやモバイル端末に、コンピュータウイルス等の不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入して常駐させ、定期的に当該ソフトウェア及びパターンファイルの更新を実施する。

⑥　不正プログラム対策ソフトウェア及びパターンファイルは、常に最新の状態に保つ。

⑦　不正プログラム対策ソフトウェアによるフルチェックを定期的に実施する。

⑧　業務で利用するソフトウェアは、修正ファイルやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

⑨　不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、システム管理者が許可した職員を除く職員等に当該権限を付与してならない。

⑵　専門家の支援体制

ＣＩＳＯは、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておく。

６．５．不正アクセス対策

⑴　システム管理者の措置事項

システム管理者は、不正アクセス対策として、以下の事項を措置する。

①　使用されていないポートを閉鎖する。

②　不要なサービスについて、機能を削除又は停止する。

⑵　攻撃への対処

ＣＩＳＯ及びシステム管理者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じる。また、総務省等と連絡を密にして情報の収集に努める。

⑶　記録の保存

ＣＩＳＯ及びシステム管理者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努める。

⑷　サービス不能攻撃

統括情報セキュリティ責任者及びシステム管理者は、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、情報システムの可用性を確保する対策を講じる。

⑸　内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、職員等及び委託事業者が使用しているパソコンやモバイル端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

⑹　職員等による不正アクセス

統括情報セキュリティ責任者及びシステム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する所属長に通知し、適正な処置を求めなければならない。

⑺　標的型攻撃

統括情報セキュリティ責任者及びシステム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

６．６．セキュリティ情報の収集

⑴　セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有する。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施する。

⑵　不正プログラム等のセキュリティ情報の収集・周知

システム管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知する。

⑶　情報セキュリティに関する情報の収集及び共有

システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有する。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じる。

7　運用

7．1．情報システムの監視

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、情報システムを常時監視する。

② システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ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。

④ 暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。

7．2．情報セキュリティポリシーの遵守状況の確認

⑴ 遵守状況の確認及び対処

① 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等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。

② 所属長は、所属で利用している情報システムの実施手順書の職員等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。

③ 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。

⑵ 情報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、不正プログラム等の調査のために、職員等が使用している情報システム機器、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。

⑶ 職員等の報告義務

① 職員等は、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。

② 所属長又はシステム管理者は、職員等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。

③ 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。

７．３．緊急時の対応等

⑴　緊急時対応計画の策定

ＣＩＳＯ又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定め、セキュリティ侵害時には当該計画に従って適正に対処する。

⑵　緊急時対応計画に盛り込む内容

緊急時対応計画には、以下の内容を定める。

①　関係者の連絡先
②　発生した事案に係る報告すべき事項
③　発生した事案への対応措置
④　再発防止措置の策定

⑶　業務継続計画との整合性確保

大規模災害、津波災害、原子力災害及び大規模・広範囲にわたる疾病等に備えて策定された島根県の各業務継続計画と情報セキュリティポリシーの整合性を確保する。

⑷　緊急時対応計画の見直し

ＣＩＳＯ及び情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直す。

７．４．例外措置

⑴　例外措置の許可

システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用する又は遵守事項を実施しないことについて合理的な理由がある場合には、ＣＩＳＯの許可を得て、例外措置を講じることができる。

⑵　緊急時の例外措置

システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかにＣＩＳＯに報告する。

７．５．法令遵守

職員等は、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、これに従わなければならない。

⑴　地方公務員法(昭和 25 年法律第 261 号)
⑵　著作権法（昭和 45 年法律第 48 号）
⑶　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）
⑷　個人情報の保護に関する法律（平成 15 年法律第 57 号）
⑸　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）
⑹　サイバーセキュリティ基本法（平成 28 年法律第 31 号）
⑺　島根県情報公開条例（平成 12 年島根県条例第 52 号）

７．６．義務違反者に対する措置

⑴　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。
⑵　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には、当該職員による情報システムの利用を停止する。
⑶　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。

８　業務委託と外部サービスの利用

８．１．業務委託

情報システムの業務委託を行う際は、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しなければならない。

⑴　委託事業者の選定基準

①　所属長及びシステム管理者は、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。

②　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、委託事業者を選定する。

⑵　契約項目

情報システムの運用、保守等を業務委託する場合には、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　委託事業者の責任者、委託内容、作業者の所属、作業場所の特定（再委託事業者も含む）

③　提供されるサービスレベルの保証

④　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（再委託事業者も含む）

⑤　委託事業者の従業員に対する教育の実施（再委託事業者も含む）

⑥　提供された情報の目的外利用及び委託事業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　県による情報セキュリティインシデント発生時の公表

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)

⑶　確認・措置等

①　システム管理者は、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、⑵の契約に基づき措置を実施する。

②　管理区域の管理を外部事業者に委託する場合には、システム管理者は、定期的に、情報セキュリティマネジメントシステム（ＩＳＭＳ）適合性評価制度やプライバシーマーク制度の認証状況、あるはこれらと同等の情報セキュリティシステムの確立状況を確認する。

８．２．外部サービスの利用（重要情報を取り扱う場合）

⑴　外部サービスの利用に係る規程の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（重要情報を取り扱う場合）の利用に関する規程を整備する。また、当該サービスの利用において、情報資産の内容により適切な措置を講じるように規定する。

①　外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下８．２節において「外部サービス利用判断基準」という。）

②　外部サービス提供者の選定基準

③　外部サービスの利用申請の許可権限者と利用手続

④　外部サービス管理者の指名と外部サービスの利用状況の管理

⑵　外部サービスの選定

①　所属長及びシステム管理者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討する。

②　所属長及びシステム管理者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定する。

また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含める。

(ｱ)　外部サービスの利用を通じて県が取り扱う情報の外部サービス提供者における目的外利用の禁止

(ｲ)　外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

(ｳ)　外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、県の意図しない変更が加えられないための管理体制

(ｴ)　外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

(ｵ)　情報セキュリティインシデントへの対処方法

(ｶ)　情報セキュリティ対策その他の契約の履行状況の確認方法

(ｷ)　情報セキュリティ対策の履行が不十分な場合の対処方法

③　所属長及びシステム管理者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含める。

④　所属長及びシステム管理者は、外部サービスの利用を通じて県が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含める。

(ｱ)　情報セキュリティ監査の受入れ

(ｲ)　サービスレベルの保証

⑤　所属長及びシステム管理者は、外部サービスの利用を通じて県が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて県の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含める。

⑥　所属長及びシステム管理者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を県に提供し、県の承認を受けるよう、外部サービス提供者の選定条件に含める。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断する。

⑦　所属長及びシステム管理者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定する。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求める。

⑧　所属長及びシステム管理者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定める。

⑨　統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断する。

⑶　外部サービスの利用に係る調達・契約

①　所属長及びシステム管理者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含める。

②　所属長及びシステム管理者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含める。

⑷　外部サービスの利用承認

①　所属長及びシステム管理者は、外部サービスを利用する場合には、統括情報セキュリティ責任者へ外部サービスの利用申請を行う。

②　統括情報セキュリティ責任者は、外部サービスの利用申請を審査し、利用の可否を決定する。

③　統括情報セキュリティ責任者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、所属長及びシステム管理者を外部サービス管理者に指名する。

⑸　外部サービスを利用した情報システムの導入・構築時の対策

①　統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際の

セキュリティ対策の原則を規定する。

(ｱ)　不正なアクセスを防止するためのアクセス制御

(ｲ)　取り扱う情報の機密性保護のための暗号化

(ｳ)　開発時におけるセキュリティ対策

(ｴ)　設計・設定時の誤りの防止

②　外部サービス管理者は、前号において定める規定に対し、構築時に実施状況を確認・記録する。

⑹　外部サービスを利用した情報システムの運用・保守時の対策

①　統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策の原則を規定する。

(ｱ)　外部サービス利用方針の規定

(ｲ)　外部サービス利用に必要な教育

(ｳ)　取り扱う資産の管理

(ｴ)　不正アクセスを防止するためのアクセス制御

(ｵ)　取り扱う情報の機密性保護のための暗号化

(ｶ)　外部サービス内の通信の制御

(ｷ)　設計・設定時の誤りの防止

(ｸ)　外部サービスを利用した情報システムの事業継続

②　所属長及びシステム管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備する。

③　外部サービス管理者は、前２号において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録する。

⑺　外部サービスを利用した情報システムの更改・廃棄時の対策

①　統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策の原則を規定する。

(ｱ)　外部サービスの利用終了時における対策

(ｲ)　外部サービスで取り扱った情報の廃棄

(ｳ)　外部サービスの利用のために作成したアカウントの廃棄

②　外部サービス管理者は、前号において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録する。

８．３．外部サービスの利用（重要情報を取り扱わない場合）

⑴　外部サービスの利用に係る規程の整備

所属長及びシステム管理者は、以下を含む外部サービス（重要情報を取り扱わない場合）の利用に関する規程を整備する。

(ｱ)　外部サービスを利用可能な業務の範囲

(ｲ)　外部サービスの利用申請の許可権限者と利用手続

(ｳ)　外部サービス管理者の指名と外部サービスの利用状況の管理

(ｴ)　外部サービスの利用の運用手順

⑵　外部サービスの利用における対策の実施

①　職員等は、利用するサービスの約款、その他の提供条件等から、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重要情報を取り扱わない場合の外部サービスの利用を所属長等へ申請する。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずる。

②　所属長及びシステム管理者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定する。また、承認した外部サービスを記録する。

９　評価・見直し

９．１．情報セキュリティ監査

⑴　実施方法

①　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。

②　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。

③　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。

⑵　監査人の要件

①　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。

②　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。

⑶　監査実施計画の立案及び実施への協力

①　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。

②　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。

③　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。

④　被監査部門は、監査の実施に協力する。

⑷　委託事業者に対する監査

事業者に委託している場合、委託事業者から再委託を受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を必要に応じて実施する。

⑸　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。

⑹　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。

⑺　監査結果への対応

①　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。

②　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。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者が、当該事項の対処を指示する。

⑻ 改善の実施及び監査結果の活用

① 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。

② 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。

９．２．自己点検

⑴ 実施方法

① 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。

② システム管理者は、所管する情報システムの情報セキュリティ対策の実施状況について、毎年度自己点検を実施する。

③ 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。

⑵ 改善の実施及び点検結果の活用

① 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。

② 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。

９．３．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。

10　用語の定義

ポリシーに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。

【あ】

●「遠隔消去機能」

「遠隔消去機能」とは、携帯電話などに記録してあるデータを、当該端末から操作するのではなく離れた場所から、遠隔操作（リモート）で、消去、無効化する機能をいう。携帯電話を紛失したり盗難にあった場合の、情報漏えいを防ぐ目的で利用される。

●「Ｗｅｂ（ウエブ）会議サービス」

「Ｗｅｂ（ウエブ）会議サービス」とは、専用のアプリケーションやＷｅｂブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。

【か】

●業務継続計画（ＢＣＰ：Busisness Continuity Plan）」

「業務継続計画（ＢＣＰ）」とは、組織において特定する業務の継続に支障をきたすと想定される自然災害、人的災害・事故、機器の障害等の事態に組織が適正に対応し目標とする業務継続性の確保を図るために当該組織において策定する、事態の予防及び事態発生後の業務の維持並びに復旧に係る計画をいう。

●「外部サービス」

「外部サービス」とは、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ものをいう。ただし、当該機能において自組織の情報が取り扱われる場合に限る。

●「外部サービス管理者」

「外部サービス管理者」とは、外部サービスの利用における利用申請の許可権者から利用承認時に指名された当該外部サービスに係る管理者をいう。

●　「外部サービス提供者」

「外部サービス提供者」とは、外部サービスを提供する事業者をいう。外部サービスを利用して自組織に向けて独自のサービスを提供する事業者は含まれない。

【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。

●「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。

●「スパムメール」

「スパムメール」とは、不特定多数に対して多量に送られてきた広告メールなどの迷惑メールのことをいう。攻撃者がこの方法を用いてマルウェア感染などを狙う攻撃をしたり、詐欺サイトに誘導するメールなどに利用することもある。

●「セキュリティホール」

「セキュリティホール」とは、システム上、攻撃者が不正な侵入などを行える状態になっている「穴」のことをいう。

●「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。

●「情報の格付」

情報の重要性に基づき「重要情報」又は「一般情報」と区分すること（情報の分類）をいう。

【た】

●「多要素認証」

「多要素認証」とは、システムが正規の利用者かどうかを判断する際の信頼性を高めるために、複数の認証手段を組み合わせて認証する方式をいう。認証方式は大きく分けて「知識」、「所持」及び「存在」を利用する方式がある。それぞれの認証手段には各々異なった利点と欠点があり、複数の認証方式を組み合わせることが利用者認

証の信頼性を高める意味でも有効である。

●「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。

●「端末への画面転送」

「端末への画面転送」とは、サーバ側に仮想的なクライアント環境を設けた上で、当該クライアント環境にパソコンやモバイル端末が専用のアプリケーションを使用してアクセスし、パソコンやモバイル端末にデータを保存せずに、データの閲覧や編集を行うことを可能とする機能をいう。

●「庁内ネットワーク」

「庁内ネットワーク」とは、地方公共団体の庁舎・出先機関を含めた団体が管理主体となるネットワーク及び同ネットワークを委託しているデータセンターに設置している情報システムをいう。

●「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。

●「特権を付与されたＩＤ」

「特権を付与されたＩＤ」とは、サーバの起動や停止、アプリケーションのインストールやシステム設定の変更、全データへのアクセスなど、通常のＩＤよりもシステムに対するより高いレベルでの操作が可能なＩＤ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。

●「ポート」

「ポート」とは、パソコンやモバイル端末がインターネットを通じて相手とデータを送受信するための窓口のことをいう。それぞれに数字が振られ、これを「ポート番号」という。また送信するものを「送信ポート」、受信するものを「受信ポート」と呼ぶ。

【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。

【ら】

●「ログ」

「ログ」とは、その機器で行われた活動を記録したデータ。通信に関するものは「通信ログ」という。

【Ａ～Ｚ】

●「ＣＳＩＲＴ（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。

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。
本情報セキュリティポリシーは平成 31 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令和３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令和４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令和５年 4 月 1 日から施行する。