山口県情報セキュリティポリシー

令和６年４月１日

山口県

目　次

はじめに

近年、政府における「クラウド・バイ・デフォルト原則」などを受けたクラウド化、デジタル手続法の成立による行政手続のオンライン化、働き方改革や業務継続のためのテレワークなど、地方自治体においても新たな時代の要請が日々増大している。

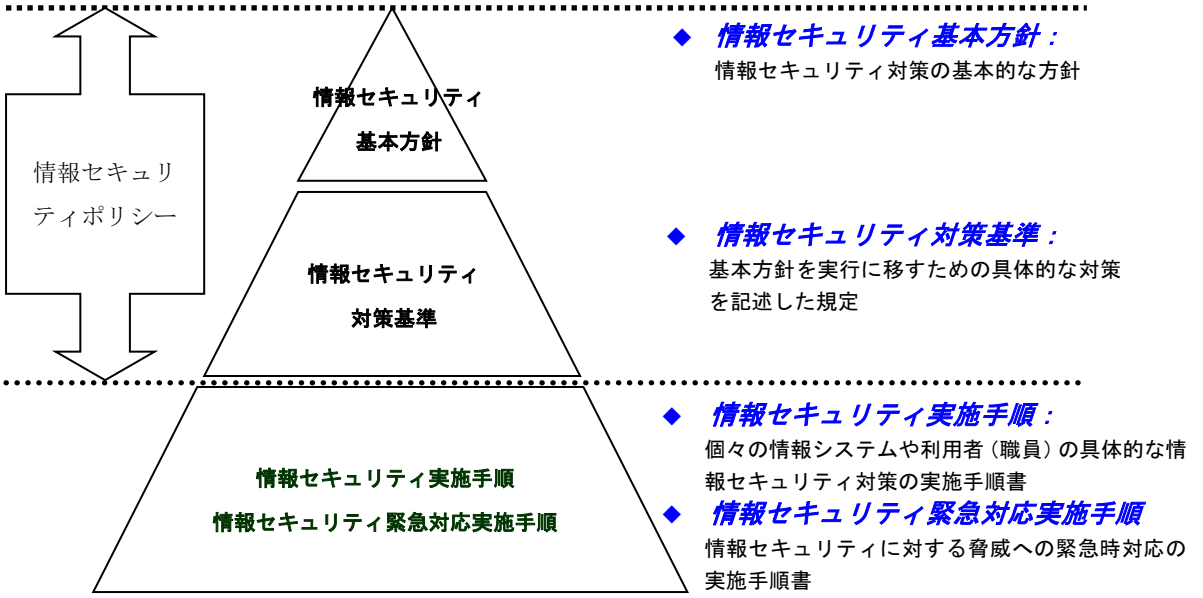
本県においても、令和２年12月に閣議決定された国の「デジタル社会の実現に向けた改革の基本方針」及びデジタル庁において策定された「デジタル社会の実現に向けた重点計画」や総務省において策定された「自治体ＤＸ推進計画」等を踏まえながら、令和３年３月に「やまぐちデジタル改革基本方針」を策定し、①『やまぐちＤＸ』の創出、②『デジタル・ガバメントやまぐち』の構築、③『デジタル・エリアやまぐち』の形成の３つの柱を掲げ、社会全体のデジタル化に向けた取組を進めているところである。

一方、サイバー攻撃の増加やサイバー犯罪における手口の巧妙化などセキュリティ上の新たな脅威や、他自治体におけるリース契約満了により返却したハードディスクの盗難による情報流出、地方公共団体向けクラウドサービスの大規模システム障害等のインシデントが発生しており、情報資産の取扱いを誤ると、県民の生活や県政の運営に重大な影響を及ぼすこととなる。

こうした脅威やインシデントから情報資産を守り、デジタル化をはじめ県民から信頼される県政運営を実施するため、情報資産の利活用における体系的かつ総合的なセキュリティ対策を定めた山口県情報セキュリティポリシーを定め、県の保有する情報資産を適切に管理することとする。

＜情報セキュリティポリシーの構成＞

情報セキュリティポリシーは「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」から構成される。また、情報セキュリティポリシーの下位に位置付けされるものに、情報セキュリティ実施手順、情報セキュリティ緊急対応実施手順がある。



第１章　山口県情報セキュリティ基本方針

第１　目的

山口県情報セキュリティ基本方針（以下「基本方針」という。）は、情報資産の利活用において、「個人情報の保護」及び「組織活動を安全に維持すること」を確保するための基本的な考え方及び方策を定める。

第２　定義

（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（ハードウエア及びソフトウエア）をいう。

（２）　情報システム

コンピュータ、ネットワーク及び記憶媒体で構成され、情報処理を行う仕組みをいう（単体のコンピュータで情報処理するものを含む。）。

（３）　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。

（４）　情報セキュリティポリシー

情報セキュリティ対策について総合的かつ体系的にとりまとめたもので「基本方針」及び「山口県情報セキュリティ対策基準（以下「対策基準」という。）」のことをいう。

（５）　行政情報

職務遂行のためコンピュータ及び記憶媒体に収集又は作成されたデータをいう。

（６）　機密性

行政情報にアクセスすることを認められた者だけが、行政情報にアクセスできる状態を確保することをいう。

（７）　完全性

行政情報が破壊、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。

（８）　可用性

行政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、行政情報にアクセスできる状態を確保することをいう。

（９）　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及び行政情報をいう。

（１０）LGWAN 接続系

LGWAN に接続された情報システム及びその情報システムで取扱う行政情報をいう（マイナンバー利用事務系を除く）。

（１１）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扱う行政情報をいう。

（１２）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。

（１３）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。

第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。

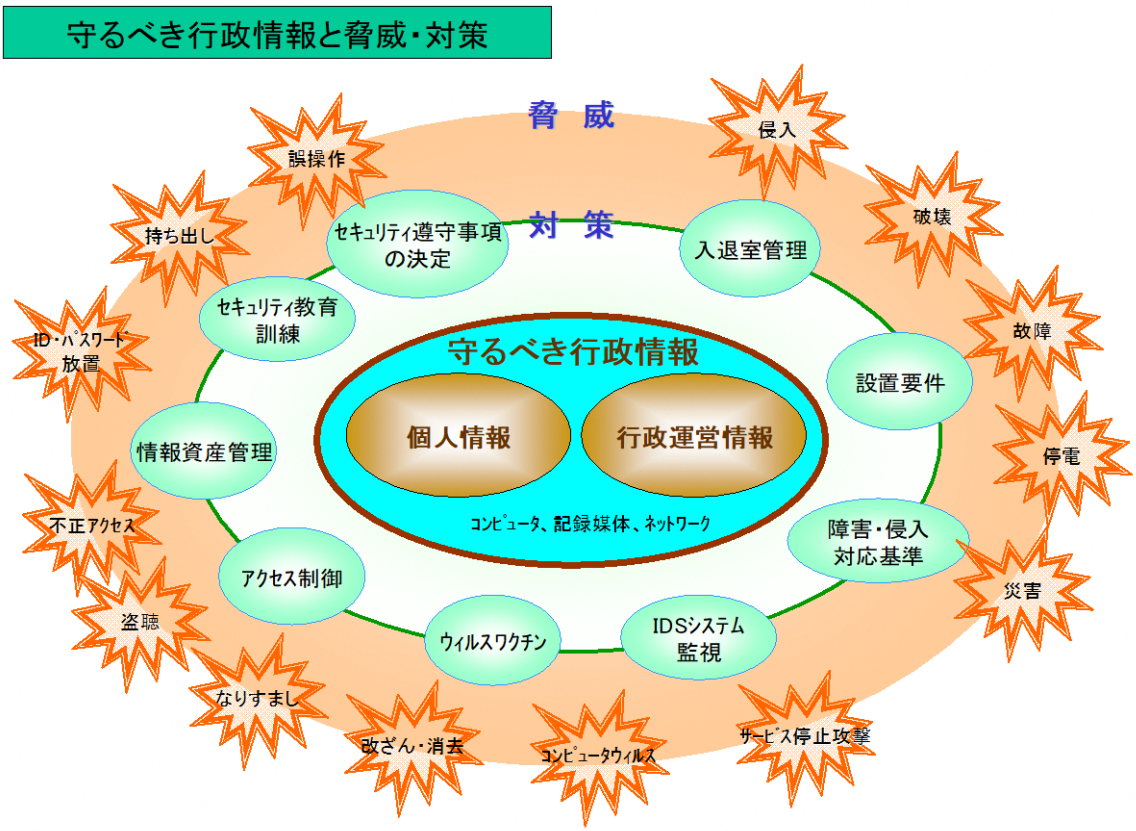
（１）　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（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４　適用範囲

（１）　行政機関の範囲

情報セキュリティポリシーの対象範囲は、県の機関とする。ただし、知事以外の執行機関等については知事の運用管理する情報システムを利用する場合に限る。

（２）　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。

① コンピュータ（ソフトウェアを含む。）、ネットワーク及び記憶媒体
② 行政情報
③ 情報システムにより印刷された文書（以下、「出力帳票」という。）
④ 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

第５　職員等の遵守義務

職員、会計年度任用職員等（以下「職員等」という。）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。

第６　情報セキュリティ対策

第３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じる。

（１）　組織体制

本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。

（２）　情報資産の分類と管理

本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行う。

（３）　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、県民情報の流出を防ぐ。
② LGWAN 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、無害化通信を行う。
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、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４）　物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

（５）　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。

（６）　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。

（７）　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切に対応するため、緊急対応実施手順を策定する。

（８）　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。

外部サービスを利用する場合には、取扱う情報の機密性に留意する。

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。

（９）　評価・見直し

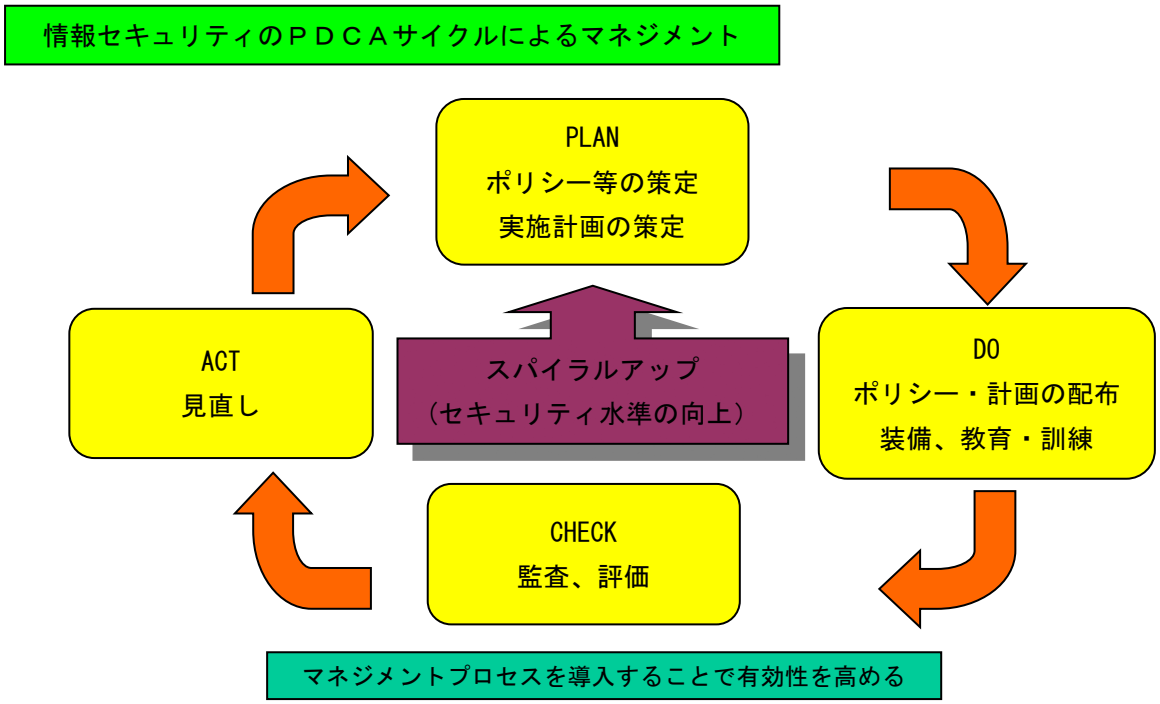
情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

第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。

第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。



第９　情報セキュリティ対策基準の策定

第６、第７及び第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。

第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。

第１１　取扱い

実施手順は、公開することにより行政運営に重大な支障を及ぼす恐れがあることから非公開とする。

第２章　山口県情報セキュリティ対策基準

山口県情報セキュリティ基本方針を適切に実施し、本県が有する情報資産を守るための具体的な情報セキュリティ対策基準を定める。

第１　組織体制

（１）　最高情報セキュリティ責任者

① デジタル推進局長を最高情報セキュリティ責任者（以下「CISO」という。）とする。

② 知事の保有する情報資産に係る情報セキュリティ対策の実施及び監視を統括する。

③ 知事が運営管理する情報システムにおける開発（「山口県情報セキュリティ基本方針 4 (1) 対象範囲」に該当する情報システムを新たに開発する場合を含む)、設定の変更、運用、見直し等を統括する責任及び権限を有する。

④ CISO が不在の時は情報セキュリティ運営管理者（以下「運営管理者」という。）が代理する。

（２）　情報セキュリティ運営管理者

① デジタル・ガバメント推進課長を運営管理者とする。

② CISO を補佐し、知事の保有する情報資産に係る情報セキュリティに関する総合的な対策を行う。

③ CISO の指示の下で、知事の保有する県の共通的なネットワーク、情報システム等の情報資産についての情報セキュリティ対策の実施に関する責任及び権限を有する。

④ 運営管理者は、情報セキュリティインシデントに対処するための体制（山口県 CSIRT：Computer Security Incident Response Team）（以下、「緊急対応チーム」という。）を整備し、役割を明確化する。

（３）　部局情報セキュリティ統括管理者

① 各部局主管課長を部局情報セキュリティ統括管理者（以下「統括管理者」という。）とする。

② 部局内の情報セキュリティ対策（情報システムに関する事項を除く。）の実施及び監視を統括する。

（４）　部局情報セキュリティ統括担当者

① 統括管理者は、部局情報セキュリティ統括担当者（以下「統括担当者」という。）を指名する。

② 統括担当者は、統括管理者を補佐し、部局における情報セキュリティの連絡調整に関する事務を行う。

（５）　情報セキュリティ管理者

① 各所属長を情報セキュリティ管理者とする。

② 所属における情報セキュリティに関する責任及び権限を有する。

（６） 外部サービス管理者

① 情報セキュリティ管理者は、外部サービス利用を開始する場合、外部サービス管理者を指名する。

② 外部サービスの利用状況の管理として、導入・構築・運用・保守・更改・廃棄といった利用のライフサイクルにおいて実施状況の確認や記録に関する責任及び権限を有する。

（７） 情報システム管理者

① 所属長のうち、情報システム（開発段階にあるものも含む。）を所管する者を情報システム管理者とする。

② 所管する情報システムの開発、運用及び保守に関する責任及び権限を有する。

（８） 情報セキュリティ担当者

① 情報セキュリティ管理者は、情報セキュリティ担当者を指名する。

② 情報セキュリティ担当者は、情報セキュリティ管理者を補佐し、所属における情報セキュリティに関する事務を行う。

（９） 情報システム担当者

① 情報システム管理者は、情報システム担当者を指名する。

② 情報システム担当者は、情報システム管理者を補佐し、所管するシステムにおける情報セキュリティに関する事務を行う。

（１０）情報セキュリティ運営担当者

① 運営管理者は、情報セキュリティ運営担当者（以下「運営担当者」という。）を指名する。

② 運営担当者は、運営管理者を補佐し、情報セキュリティ運営委員会（以下「運営委員会」という。）に関する事務を行う。

（１１）情報セキュリティ運営委員会

① 情報セキュリティ対策を体系的、総合的に推進するため、運営委員会を設置する。

② 委員長は CISO、副委員長は運営管理者とし、委員は統括管理者の他、委員長が指名する。

③ 運営委員会は、情報セキュリティポリシーの検討・見直しなど情報セキュリティに関する重要事項について審議する。

④ 運営委員会は、委員長が招集する。委員は、委員長に運営委員会の招集を要請することができる。

⑤ 運営委員会の事務を処理するため、事務局をデジタル・ガバメント推進課に置く。

（１２）情報セキュリティ運営委員会幹事会

① 運営委員会の円滑な運営のため、情報セキュリティ運営委員会幹事会(以下「幹事会」という。）を設置する。

② 幹事長は、運営担当者とし、幹事は統括担当者の他、幹事長が指名する。

③ 幹事会は、幹事長が招集する。幹事は、幹事長に幹事会の招集を要請することができる。

（１３）部局情報セキュリティ会議

① 各部局に、各部局での情報セキュリティを推進するため、部局情報セキュリティ会議を設置する。

② 議長は、統括管理者とし、構成員は本庁各課（室）長の他議長が指名する。

③ 部局情報セキュリティ会議は、議長が招集する。構成員は、議長に部局情報セキュリティ会議の招集を要請することができる。

（１４）兼務の禁止

① 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。

② 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。

（１５）情報セキュリティ緊急連絡窓口

① 情報セキュリティ障害、侵害、及び情報システム上の欠陥及び誤動作等(以下「情報セキュリティインシデント」という。）が発生した場合の職員等からの連絡窓口として、情報セキュリティ緊急連絡窓口（以下、「緊急連絡窓口」という。）を設置する。

② 緊急連絡窓口は、デジタル・ガバメント推進課内に常設する。

（１６）情報セキュリティ緊急対応チーム（山口県 CSIRT）

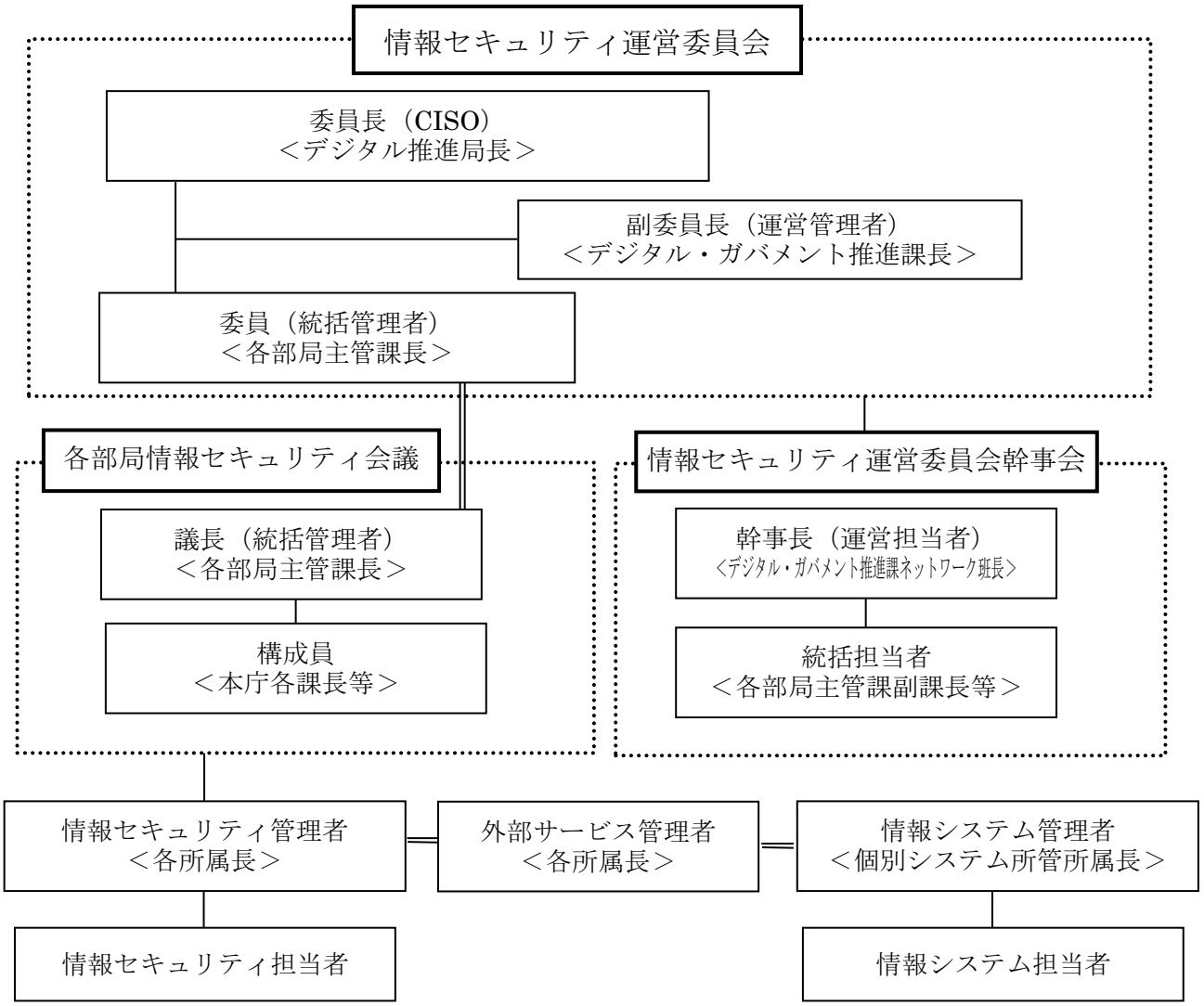
① 運営管理者は、重大な情報セキュリティインシデント対応のために、情報セキュリティ緊急対応チーム（山口県 CSIRT : Computer Security Incident Response Team）（以下、「緊急対応チーム」という。）を設置する。

② 緊急対応チーム責任者は、運営管理者とする。

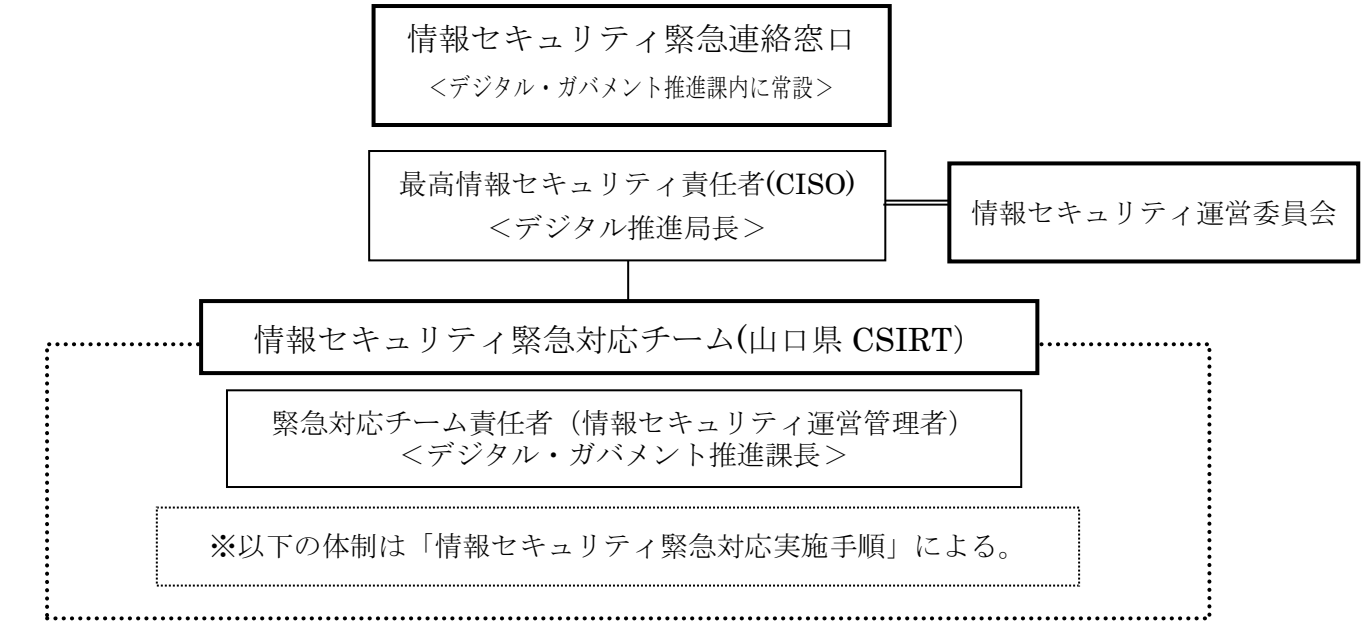
③ 緊急対応チームの運営は、「情報セキュリティ緊急対応実施手順」に従うものとする。

＜図１　組織・体制＞

○平常時



○緊急時



第２　情報資産の分類と管理

（１）　行政情報の分類

① 情報セキュリティ管理者（情報システム管理者が所管する行政情報については情報システム管理者をいう。以下同じ。）は、収集又は作成した行政情報について、機密性、完全性及び可用性毎に以下の重要性分類に基づき評価し、分類するものとする。

重　要　性　分　類	
Ⅰ　県民生活や県政全体に重大な影響を及ぼす情報	高
Ⅱ　業務の執行等に重大な影響を及ぼす情報	
Ⅲ　業務の執行等に軽微な影響を及ぼす情報	
Ⅳ　上記以外の情報	低

＜分類の例＞

	機密性	完全性	可用性
	情報が漏えいし、暴露された時の影響度	情報が改ざんされた時の影響度	利用妨害などでシステムが停止した時の影響度
Ⅰ	個人情報（県民、職員）、企業の営業機密	個人情報（県民）、金額にかかわる情報（税額、給付額等）	県民に業務サービスを提供するシステム（電子申請、入札、税務、証明書発行等）、全庁的に業務に影響するシステム（県庁 LAN、総合文書管理等）
Ⅱ	重要な意思形成過程・行政運営情報、請負・委託等の外注管理情報、情報システム設定情報	個人情報（職員）、多数の県民へ提供する情報、重要な意思形成過程・行政運営情報、請負・委託等の外注管理情報、資産管理情報、情報システム設定情報	重要な庁内の業務システム（財務、土木事業管理・設計積算、人事給与等のシステム）
Ⅲ	軽易な意思形成過程・行政運営情報	軽易な意思形成過程・行政運営情報	その他軽易な庁内の業務システム
Ⅳ	公開情報	その他	その他

② 分類に当たっては、個人情報の保護に関する法律、個人情報の保護に関する法律施行条例、知事が保有する個人情報の適切な管理のための措置に関する要綱その他の法令に配慮するものとする。

（２）　情報資産の管理

情報資産は、その取扱う行政情報の重要性によって分類し、その重要性に応じて管理するものとする。

① 管理責任

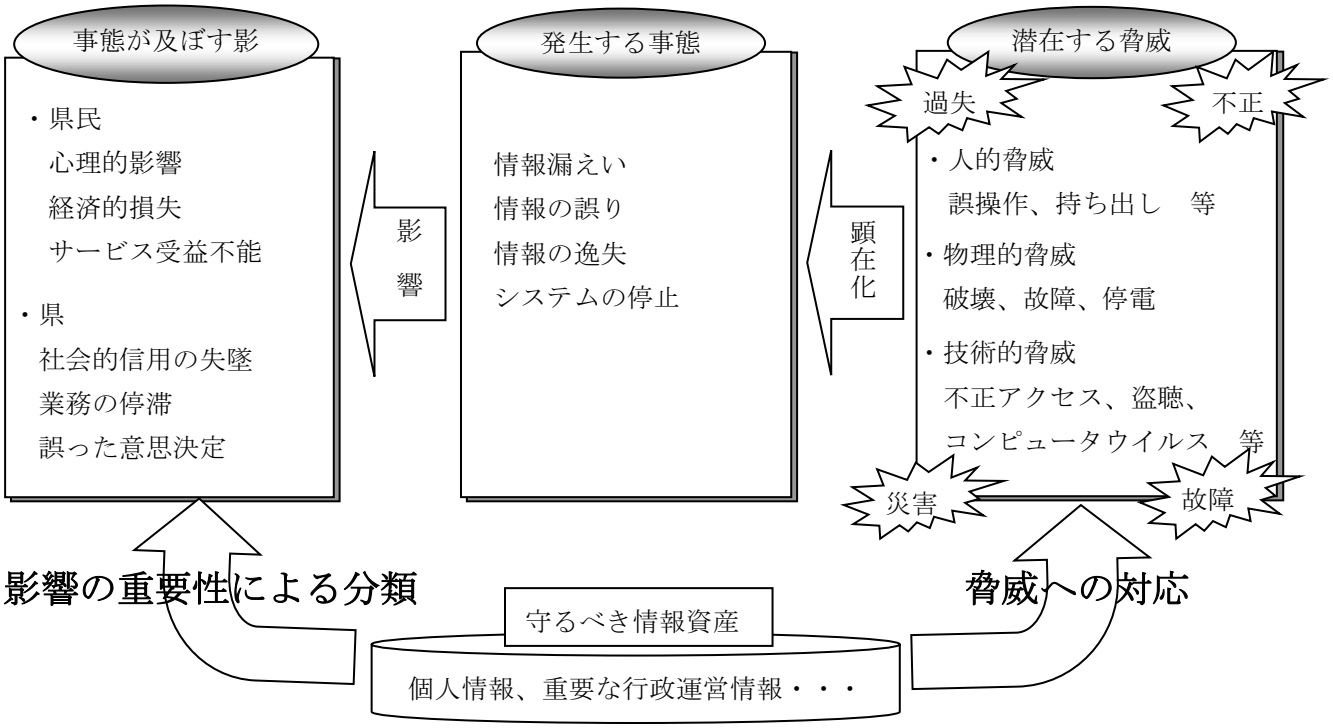
（ア）情報セキュリティ管理者及び情報システム管理者（以下「情報セキュリティ管理者等」という。）は、所管のコンピュータ、周辺機器等を管理する職員等を定め、誰がどのコンピュータ等を管理するのか明確にしなければならない。

（イ）情報セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製等された情報資産も(１)の分類に基づき管理しなければならない。

② 情報資産の分類の表示

情報セキュリティ管理者は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

＜図２　情報の分類と対策＞



潜在する脅威とともに、脅威が顕在化した際の事態が及ぼす影響を考慮して、情報セキュリティ対策を講ずる。

③ 行政情報の作成

（ア）職員等は、業務上必要のない行政情報を作成してはならない。

（イ）行政情報を作成する者は、行政情報の作成時に（１）の分類に基づき、当該行政情報の分類と取扱制限を定めなければならない。

（ウ）行政情報を作成する者は、作成途上の行政情報についても、紛失や流出等を防止しなければならない。また、行政情報の作成途上で不要になった場合は、当該行政情報を消去しなければならない。

④ 情報資産の入手

（ア）庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

（イ）庁外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ）情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

⑤ 情報資産の利用

（ア）情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

（イ）情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

（ウ）情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取扱わなければならない。

⑥ 情報資産の保管

（ア）情報セキュリティ管理者等は、情報資産の分類に従って、情報資産を適正に保管しなければならない。なお、重要度の高いものについては、自然災害を被る可能性が低い地域にバックアップを保管するように努めるものとする。

（イ）情報セキュリティ管理者等は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

（ウ）情報セキュリティ管理者等は、機密性Ⅰ、Ⅱ及びⅢ、完全性Ⅰ及びⅡ又は可用性Ⅰ及びⅡの行政情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦ 行政情報の送信

電子メール等により機密性Ⅰ、Ⅱ及びⅢの行政情報を送信する者は、必要に応じ、パスワード等による暗号化を行わなければならない。

⑧ 情報資産の運搬

（ア）車両等により機密性Ⅰ、Ⅱ及びⅢの情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

（イ）機密性Ⅰ、Ⅱ及びⅢの情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

⑨ 情報資産の提供・公表

（ア）機密性Ⅰ、Ⅱ及びⅢの情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

（イ）機密性Ⅰ、Ⅱ及びⅢの情報資産を外部に提供する者は、情報セキュリテ

ィ管理者に許可を得なければならない。

（ウ）情報セキュリティ管理者は、県民に公開する情報資産について、完全性を確保しなければならない。

⑩ 情報資産の廃棄等

（ア）情報セキュリティ管理者等は、情報資産の破棄やリース返却等を行う場合、記録されている情報の機密性に応じ、情報を復元できないように処置した上で廃棄しなければならない。また、当該措置を外部の者に依頼する場合は、確実に実施されたことを確認しなければならない。

（イ）情報セキュリティ管理者等は、行った処理について日時、担当者及び処理内容を記録しなければならない。

（ウ）情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

第３　情報システム全体の強靭性の向上

（１）　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領域との分離

マイナンバー利用事務系と他の領域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系と外部との通信をする必要がある場合は、通信経路の限定（MAC アドレス、IP アドレス）及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。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、インターネット等から LGWAN-ASP を経由しマイナンバー利用事務系にデータを取り込むことを可能とする。

② 行政情報のアクセス及び持ち出しにおける対策

（ア）行政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手段は、「知識」、「所持」、「存在」のうち、二つ以上の要素を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

（イ）行政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行政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。

（２）　LGWAN 接続系

① LGWAN 接続系とインターネット接続系の分割

LGWAN 接続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 LGWAN 接続系に取り込む場合は、次の実現方法等により、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 LGWAN 接続系に転送するメールテキスト化方式

（イ）インターネット業務端末から、LGWAN 接続系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

（３）　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行わなければならない。
② 山口県情報セキュリティクラウドに参加するとともに、関係省庁や市町等と連携しながら、情報セキュリティ対策を推進しなければならない。

第４　物理的セキュリティ

４．１　サーバ等の管理

（１）　機器の取付け

情報セキュリティ管理者等は、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､必要な措置を講じなければならない。

（２）　サーバの冗長化

情報セキュリティ管理者等は、可用性Ⅰ及びⅡの重要情報を格納しているサーバ、セキュリティサーバ、県民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持するよう努めるものとする。

（３）　機器の電源
① 情報セキュリティ管理者等は、運営管理者及び施設管理部門と連携し、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を備え付けなければならない。
② 情報セキュリティ管理者等は、可用性Ⅰ及びⅡの情報システムに係る機器の電源について、非常用発電機からの供給が確保されるよう努めるものとする。
③ 情報セキュリティ管理者等は、運営管理者及び施設管理部門と連携し、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なければならない。

（４）　通信ケーブル等の配線
① 運営管理者及び情報システム管理者は、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なければならない。
② 運営管理者及び情報システム管理者は、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

対応しなければならない。

③ 運営管理者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

④ 運営管理者、情報システム管理者は、自ら又は情報システム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なければならない。

（５） 機器の定期保守及び修理

① 情報セキュリティ管理者等は、可用性Ⅰ及びⅡのサーバ等の機器の定期保守を実施しなければならない。

② 情報セキュリティ管理者等は、電磁的記録媒体を内蔵する機器を事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、事業者に故障を修理させるにあたり、修理を委託する事業者との間で、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わなければならない。

（６） 庁外への機器の設置

情報セキュリティ管理者等は、庁外にサーバ等の機器を設置する場合、CISOの承認を得なければならない。また、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しなければならない。

（７） 機器の廃棄等

情報セキュリティ管理者等は、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、全ての行政情報を消去の上、記録されている情報の機密性に応じ、物理的破壊等の方法により、復元不可能な状態にする措置を講じなければならない。また、当該措置を外部の者に依頼する場合は、確実に実施されたことを確認しなければならない。

４．２ 管理区域（情報システム室等）の管理

（１） 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う。

② 情報セキュリティ管理者等は、管理区域を外部からの侵入が容易にできないようにしなければならない。

③ 情報セキュリティ管理者等は、施設管理部門と連携して、管理区域から外部に通ずるドアを必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

④ 情報セキュリティ管理者等は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

⑤ 情報セキュリティ管理者等は、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しなければならない。

（２）　管理区域の入退室管理等

① 情報セキュリティ管理者等は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

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、求めに応じて提示しなければならない。

③ 情報セキュリティ管理者等は、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を付き添わせるものとし、外見上職員等と区別できる措置を講じなければならない。

④ 情報セキュリティ管理者等は、機密性Ⅰ、Ⅱ及びⅢの情報資産を扱うシステムを設置している管理区域について、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、電磁的記録媒体等を持ち込ませないようにしなければならない。

（３）　機器等の搬出入

① 情報セキュリティ管理者等は、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、あらかじめ職員又は委託事業者に確認を行わせなければならない。

② 情報セキュリティ管理者等は、納入・搬出業者等による機器等の搬入・搬出時には、職員を指名し、立ち会わせなければならない。また、業者に対し作業に必要な情報資産以外の情報資産を持ち込ませてはならない。

③ 情報セキュリティ管理者等は、保守のため機密性Ⅰ、Ⅱ及びⅢの情報資産を搬出する場合は、保守及び搬出する者に秘密を保持させなければならない。

４．３　通信回線及び通信回線装置の管理

① 運営管理者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。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しなければならない。

② 運営管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

③ 運営管理者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。

④ 運営管理者は、機密性Ⅰ、Ⅱ及びⅢの情報資産を取扱う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、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

⑤ 運営管理者は、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しなければならない。

⑥ 運営管理者は、可用性Ⅰ及びⅡの情報を取扱う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なければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

４．４　職員等の利用する端末や電磁的記録媒体等の管理

① 情報セキュリティ管理者等は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。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しなければならない。

② 情報セキュリティ管理者等は、情報システムへのログインに際し、取扱う情報の重要度に応じて、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

③ 情報セキュリティ管理者等は、マイナンバー利用事務系及び機密性Ⅰ及びⅡのうち重要な情報資産を取扱う情報システムでは「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認証（多要素認証）を行うよう設定しなければならない。

④ 情報セキュリティ管理者等は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末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しなければならない。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媒体を使用しなければならない。

⑤ 情報セキュリティ管理者等は、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、端末の機能制限、紛失・盗難時の対策等の措置を講じなければならない。

第５　人的セキュリティ

５．１　職員等の遵守事項

（１）　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しなければならない。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、速やかに情報セキュリティ管理者に相談し、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）CISO は、機密性Ⅰ、Ⅱ及びⅢ、可用性Ⅰ及びⅡ、完全性Ⅰ及びⅡの情報資産を外部で処理する場合における安全管理措置を定めなければならない。

（イ）職員等は、本県のモバイル端末、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す場合には、情報セキュリティ管理者の許可を得なければならない。

（ウ）職員等は、許可を得て情報資産を持ち出す場合、盗難、破損、紛失等に注意しなければならない。また、許可された期間内に返却するとともに、私的に所有するコンピュータや電磁的記録媒体に行政情報を複写した場合は、専用ソフト等によりこれを完全に消去し、復元不可能な状態にしなければならない。

（エ）職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

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業務利用

（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、支給以外の端末の利用が業務上必要と CISO が判断した場合は、運営管理者の定める実施手順に従い、情報セキュリティ管理者の許可を得て利用することができる。

（イ）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用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

（ウ）職員等は、ファイル共有ソフトについて、情報漏えい等の危険性を十分認識し、支給以外のパソコン、モバイル端末においても、これを使用しないよう努めるものとする。

⑤ 持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑥ パソコンやモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

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、適正な措置を講じなければならない。

⑧ 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。

（２）　会計年度任用職員等への対応

① 情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、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等のうち、会計年度任用職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

② 情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、会計年度任用職員等の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意を求めるものとする。

③ インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、会計年度任用職員等にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（3） 情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、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掲示しなければならない。

（4） 委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を委託事業者に発注する場合、再委託事業者も含めて、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説明しなければならない。

５．２ 研修・訓練

（1） 情報セキュリティに関する研修・訓練

CISO 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。

（2） 研修計画の策定及び実施

① CISO は、幹部を含め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い、運営委員会の承認を得なければならない。

② 研修計画において、職員等が情報セキュリティ研修を毎年度最低 1 回は受講できるようにしなければならない。

③ 新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

④ 研修は、運営管理者、統括管理者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対して、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤ 情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、運営管理者及び情報セキュリティ管理者に対して、報告しなければならない。

⑥ 運営管理者は、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研修の実施状況について報告しなければならない。

⑦ CISO は、毎年度 1 回、運営委員会に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

（３）　緊急時対応訓練

CISO は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

（４）　研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

５．３　情報セキュリティインシデントの報告

（１）　情報セキュリティ障害・侵害時の報告

① 職員等は、情報セキュリティインシデントを発見又は県民等外部から連絡を受けた場合には、速やかに情報セキュリティ担当者及び緊急連絡窓口に報告し、指示を仰がなければならない。

② 情報セキュリティ担当者は、情報セキュリティインシデントの報告を受けた場合、軽微な事案を除き、情報セキュリティ管理者に報告し、指示を仰がなければならない。なお、情報セキュリティ管理者は、情報セキュリティインシデントの報告を受けた場合、必要に応じて、統括管理者に報告しなければならない。

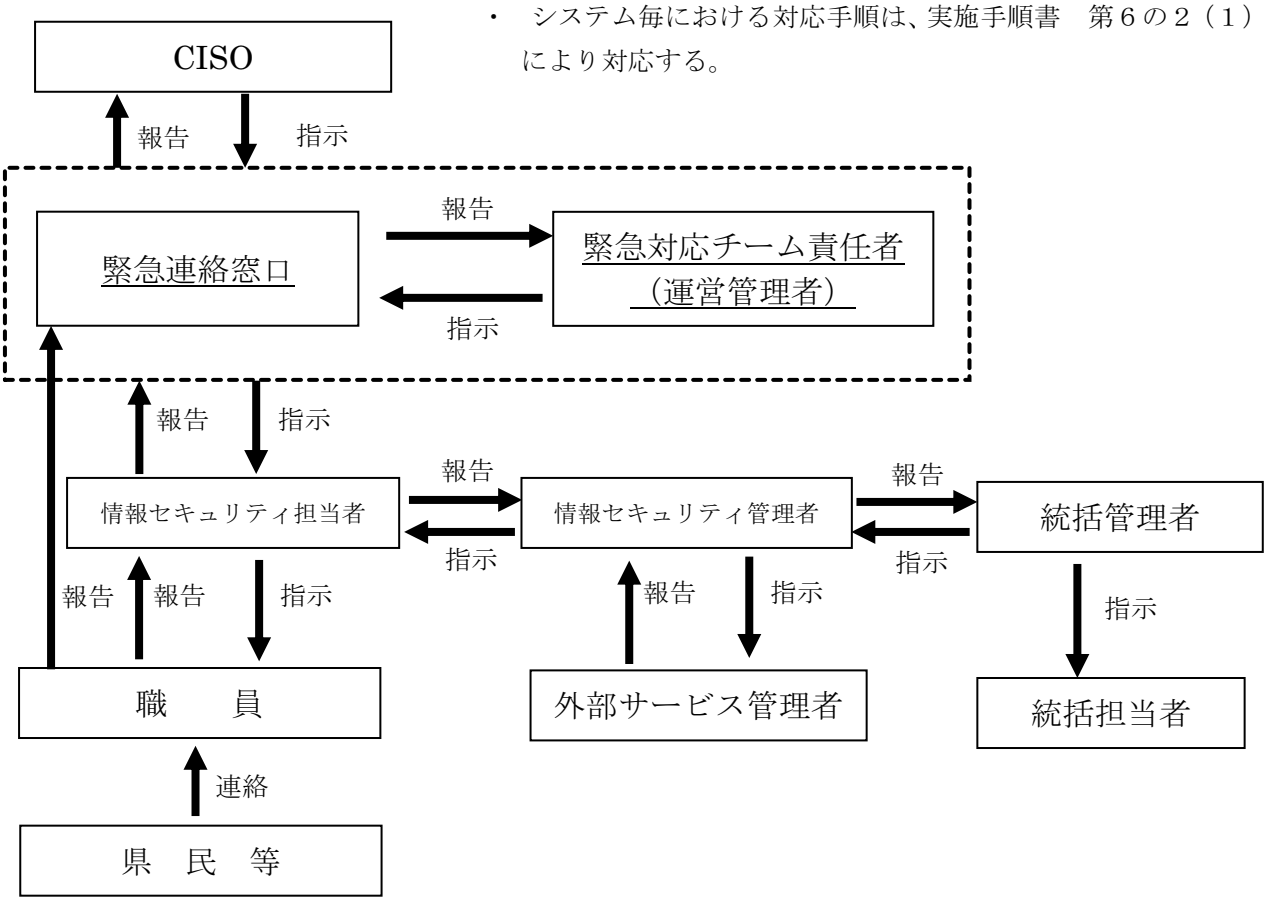
③ 統括管理者は、情報セキュリティ管理者から情報セキュリティインシデントの報告を受けた場合、必要に応じて、情報セキュリティ管理者及び統括担当者に指示を行うものとする。

④ 緊急連絡窓口は、情報セキュリティインシデントの報告を受けた場合、事態の軽重にかかわらず速やかに運営管理者に報告し、指示を仰がなければならない。また、軽微な事案を除き、CISO に報告し、指示を仰がなければならない。

＜図３　障害・侵害時の連絡図＞ (注)

・　県民の生活の安定、県民の生命、身体、財産等に重大な被害の想定される場合は、危機管理マニュアルにより対応する。

・　システム毎における対応手順は、実施手順書　第６の２（１）により対応する。



（２）　情報セキュリティ障害・侵害への対応及び再発防止

① CISO は、緊急を要する情報セキュリティインシデントに対応するため情報セキュリティ管理者等の同意を得ずに、県庁 LAN や外部のネットワークとの切離し及び情報システムの停止を指示することができる。なお、指示内容については、関係部局の統括管理者に速やかに連絡するものとする。

② 情報セキュリティ管理者等は、発生した情報セキュリティインシデントが県民生活の安定、県民の生命、身体、財産等に重大な被害を及ぼすおそれのある場合は、統括管理者と協議の上、山口県危機管理マニュアルにより対応する。

③ 情報セキュリティインシデントの発生時の対応手順を明確にすること。また、発生した際には、その原因及び対応記録を取り再発防止対策を検討・実施すること。

④ 情報セキュリティ管理者等は、情報セキュリティインシデントに対する状況調査を行い、CISO に報告しなければならない。また、情報セキュリティインシデントの原因が「不正アクセス行為の禁止等に関する法律」に触れる場合は、警察などの関係機関と連絡をとり、指示を受けなければならない。

⑤ 情報セキュリティ管理者等は、情報セキュリティインシデントの原因調査及び分析を行い、統括管理者との協議の上、再発防止策を講じなければならない。
⑥ CISO は、情報セキュリティ管理者等から報告された原因調査及び分析結果、並びに再発防止策について、必要に応じて助言を行うことができる。

５．４　ID 及びパスワード等の管理

（１）　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、次の事項を遵守しなければならない。
（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等の端末のスロット等から抜いておかなければならない。
（ウ）IC カード等を紛失した場合には、速やかに情報セキュリティ管理者等に通報し、指示に従わなければならない。
② 情報セキュリティ管理者等は、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しなければならない。
③ 情報セキュリティ管理者等は、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しなければならない。

（２）　ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。
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。

（３）　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、次の事項を遵守しなければならない。
① パスワードは、他者に知られないように管理しなければならない。
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（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）にしなければならない。
④ パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
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、最初のログイン時点で変更しなければならない。
⑦ サーバ、ネットワーク機器及び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。

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）。

第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

（１）　文書サーバの設定等

① 情報システム管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。

② 情報システム管理者は、文書サーバを課室等の単位で構成し、職員等が他課室等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、設定しなければならない。

③ 情報システム管理者は、県民の個人情報、人事記録等、特定の職員等しか取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、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

（２）　バックアップの実施

運営管理者及び情報システム管理者は、業務システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。滅失により業務継続に甚大な影響を及ぼす情報資産については、遠隔地にバックアップを保管するよう努めなければならない。

（３）　他団体との情報システムに関する情報等の交換

情報システム管理者は、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、運営管理者及び情報セキュリティ管理者の許可を得なければならない。

（４）　システム管理記録及び作業の確認

① 情報システム管理者は、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、作業記録を作成しなければならない。

② 運営管理者及び情報システム管理者は、所管するシステムにおいて、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しなければならない。

③ 運営管理者、情報システム管理者又は情報システム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よう努めるものとする。

（５）　情報システム仕様書等の管理

情報システム管理者は、設定情報及びバックアップの最新の状況、ネットワーク構成図、情報システム仕様書について適切に記録するとともに、記録媒体に関わらず紛失や業務上必要とする者以外の閲覧等がないよう適正に管理しな

ければならない。

（６）　ログの取得等

① 運営管理者及び情報システム管理者は、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、一定の期間保存しなければならない。

② 運営管理者及び情報システム管理者は、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、適正にログを管理しなければならない。

③ 運営管理者及び情報システム管理者は、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しなければならない。

（７）　障害記録

運営管理者及び情報システム管理者は、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し、適正に保存しなければならない。

（８）　ネットワークの接続制御、経路制御等

① 運営管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

② 運営管理者は、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さなければならない。

（９）　外部の者が利用できるシステムの分離等

情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

（１０）外部ネットワークとの接続制限等

① CISO の許可無く外部システムと接続してはならない。

② ①の許可について、相手先とのデータ交換手順、情報管理手法及び責任分界点について、事前に CISO と協議しなければならない。

③ 県庁 LAN に情報システムを接続する場合、運営管理者の許可を得なければならない。

④ 外部システム及びネットワークへのアクセス経路に係るルーティング設定並びにアクセス制御等について、CISO に協議しなければならない。

⑤ 情報システム管理者は、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、機器構成、セキュリティ技術等を詳細に調査し、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しなければならない。

⑥ 情報システム管理者は、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しなければならない。

⑦ 運営管理者及び情報システム管理者は、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しなければならない。

⑧ 情報システム管理者は、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、運営管理者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（１１）複合機のセキュリティ管理

① 情報セキュリティ管理者は、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しなければならない。

② 情報セキュリティ管理者は、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なければならない。

③ 情報セキュリティ管理者は、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なければならない。

（１２）IoT 機器を含む特定用途機器のセキュリティ管理

情報セキュリティ管理者等は、特定用途機器について、取扱う情報、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しなければならない。

（１３）無線 LAN 及びネットワークの盗聴対策

① 情報セキュリティ管理者等は、無線 LAN 環境を無断で構築してはならない。無線 LAN 環境を構築する必要がある場合は、事前に運営管理者へ協議し了承を得なければならない。また、了承を得て構築する場合は、データ通信の暗号化、無線 LAN ルータのアクセス制御等、安全に配慮しなければならない。

② 情報セキュリティ管理者等は、コンピュータ、周辺機器等を①で了承された無線 LAN 環境以外に接続してはならない。

③ 情報システム管理者は、データ通信の暗号化を行う場合は、安全なプロトコルとアルゴリズムを選択しなければならない。

（１４）電子メールのセキュリティ管理

① 運営管理者は、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、電子メールサーバの設定を行わなければならない。

② 運営管理者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。
③ 運営管理者は、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しなければならない。
④ 運営管理者は、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しなければならない。
⑤ 運営管理者は、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の作業員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なければならない。

（１５）電子メールの利用制限
① 職員等は、自動転送機能を用いて、電子メールを外部のメールアドレスへ転送してはならない。
② 職員等は、割り当てられたメールアドレスを業務以外に使用してはならず、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。
③ 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、他の送信先のメールアドレスが分からないようにしなければならない。
④ 職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。
⑤ 職員等は、県の情報資産に該当する電子データを、運営管理者の了承なく、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（フリーメール、ファイルストレージ、グループウェア等のクラウドサービスなど）で取扱ってはならない。また、業務上の理由によりやむを得ず使用する場合を除き、県庁LANを利用してウェブメール（グループウェアで提供するものを除く。）を使用してはならない。

（１６）電子署名・暗号化
① 職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、運営管理者が定めた電子署名、パスワード等による暗号化等、セキュリティを考慮して、送信しなければならない。
② 職員等は、暗号化を行う場合に運営管理者が定める以外の方法を用いてはならない。また、運営管理者が定めた方法で暗号のための鍵を管理しなければならない。
③ CISO は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

（１７）無許可ソフトウェアの導入等の禁止
① 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。
② 職員等は、業務上の必要がある場合は、情報セキュリティ管理者等の許可を得て、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、情報セ

キュリティ管理者等は、ソフトウェアのライセンスを管理するとともに、ライセンス数や使用許諾条件を遵守しなければならない。

③ 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。

④ 情報セキュリティ管理者等は、コンピュータへのソフトウェアの導入状況を適切に記録し、管理しなければならない。

⑤ 情報セキュリティ管理者等は、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しなければならない。

（１８）機器構成の変更の制限

① 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。

② 職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、運営管理者及び情報システム管理者の許可を得なければならない。

（１９）業務外でのネットワークへの接続の禁止

① 職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報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。

② 情報セキュリティ管理者は、支給した端末について、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ことが望ましい。

（２０）業務以外の目的でのウェブ閲覧の禁止

① 職員等は、業務以外の目的でウェブを閲覧してはならない。

② 情報システム管理者は、必要に応じて、職員等のウェブ閲覧の内容を確認することができる。

③ 情報システム管理者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

（２１）Web 会議サービスの利用時の対策

① 情報セキュリティ管理者は、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、本県の定める利用手順に従い、Web 会議の参加者や取扱う情報に応じた情報セキュリティ対策を実施すること。

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こと。

④ 職員等は、県の利用手順と同様の情報セキュリティ対策が取られていることを確認すること。

（２２）ソーシャルメディアサービスの利用

情報セキュリティ管理者は、山口県ソーシャルメディア利用ガイドラインに従い利用方針を定めなければならない。

６．２　アクセス制御

（１）　アクセス制御等

① アクセス制御

（ア）運営管理者又は情報システム管理者は、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、システム上制限しなければならない。

（イ）情報資産へのアクセスについて、当該情報資産の機密性に応じ使用時間や使用可能端末の限定などに配慮すること。

② 利用者 ID の取扱い

（ア）情報セキュリティ管理者等は、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 の取扱い等を適切に管理しなければならない。

（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、運営管理者又は情報システム管理者に通知しなければならない。

（ウ）運営管理者及び情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

（エ）認証に複数回の失敗した際は、当該 ID によるアクセスが不能となる機能を設けることに努めるものとする。

③ 特権を付与された ID の管理等

（ア）情報セキュリティ管理者等は、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しなければならない。

（イ）情報セキュリティ管理者等の特権を代行する者は、情報セキュリティ管理者等が指名し、CISO が認めた者でなければならない。

（ウ）CISO は代行者を認めた場合、速やかに運営管理者、統括管理者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

（エ）情報セキュリティ管理者等は、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定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

（オ）情報セキュリティ管理者等は、特権を付与された ID を初期設定以外のものに変更しなければならない。

（２）　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、運営管理者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

② 運営管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、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しな

ければならない。

③ 運営管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④ 運営管理者は、外部からのアクセスを認める場合、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なければならない。

⑤ 運営管理者及び情報システム管理者は、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じなければならない。

⑥ 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、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって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。

⑦ 運営管理者は、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しなければならない。ただし、止むを得ず接続を許可する場合は、利用者の ID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

⑧ 職員等は、県が保有するコンピュータ、周辺機器等を運営管理者が認めるネットワーク以外のネットワークに無断で接続してはならない。

（３） 認証情報の管理

① 運営管理者又は情報システム管理者は、職員等の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

② 運営管理者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、必要に応じて仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

③ 運営管理者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

（４） 特権による接続時間の制限

情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

６．３ システム開発、導入、保守等

（１） 情報システムの調達

① 運営管理者及び情報システム管理者は、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し、CISO の承認を得なければならない。

② 運営管理者及び情報システム管理者は、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しなければならない。

（2） 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

情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

② システム開発における責任者、作業者の ID の管理

（ア）情報システム管理者は、システム開発責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。

（イ）情報システム管理者は、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とともに、情報資産の提供を必要最小限に限らなければならない。

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）情報システム管理者は、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しなければならない。

（イ）情報システム管理者は、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しなければならない。

（3） 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）情報システム管理者は、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しなければならない。

（イ）情報システム管理者は、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しなければならない。

（ウ）情報システム管理者は、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しなければならない。

（エ）情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

② テスト

（ア）情報システム管理者は、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わなければならない。

（イ）情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

（ウ）情報システム管理者は、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。重要性Ⅰ及びⅡの情報資産に係るテストデータは、複製を使用し、厳重に保管・管理しなければならない。

（エ）情報システム管理者は、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わなければならない。

（４）　システム開発・保守に関連する資料等の整備・保管

① 情報システム管理者は、システム開発・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・保管しなければならない。

② 情報システム管理者は、テスト結果を一定期間保管しなければならない。

③ 情報システム管理者は、情報システムに係るソースコードを重要性Ｉの情報資産として適正な方法で保管しなければならない。

（５）　情報システムにおける入出力データの正確性の確保

① 情報システム管理者は、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しなければならない。

② 情報システム管理者は、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しなければならない。

③ 情報システム管理者は、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しなければならない。

④ 情報システム管理者は、入出力されるデータの正確性及び妥当性の確認を定期的に検査しなければならない。

（６）　情報システムの変更管理

情報システム管理者は、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しなければならない。

（７）　開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等（OS 等も含む）を更新又はパッチの適用をする場合、不具合の有無及び他の情報システムとの整合性を確認し、計画的に導入しなければならない。

（８）　システム更新又は統合時の検証等

情報システム管理者は、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わなければならない。

６．４　不正プログラム対策

（１）　運営管理者の措置事項

運営管理者は、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しなければならない。
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しなければならない。
③ 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しなければならない。
④ 所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。
⑤ 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。
⑥ 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
⑦ 業務で利用するソフトウェアは、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。

（２） 情報セキュリティ管理者等の措置事項

情報セキュリティ管理者等は、不正プログラム対策に関し、次の事項を措置しなければならない。

① 情報セキュリティ管理者等は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。
② 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。
③ 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。
④ 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職員等に利用させてはならない。また、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、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しなければならない。
⑤ 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、情報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はならない。

（３） 職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

① 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。
② 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。
③ 職員等は、メールを受信する場合は、標的型攻撃やコンピュータウイルス感染のリスクを認識し、細心の注意を払って取扱うこととし、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、速やかに削除しなければならない。
④ 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。
⑤ 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。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 LGWAN 接続系に取り込む場合は無害化しなければならない。
⑥ 運営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。
⑦ 職員等は、ウイルスへの感染を発見した場合（感染が疑われる場合も含む。）は、速やかにネットワークから切り離すとともに情報セキュリティ担当者及び緊急連絡窓口に報告しなければならない。また、情報セキュリティ担当者は、緊急連絡窓口（緊急対応チーム）に感染したウイルスの名称、被害状況、感染経路等を報告し、緊急対応チームの指示のもと、被害拡大の防止及び修復措置を行わなければならない。

（４） 専門家の支援体制

運営管理者は、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かなければならない。

６．５ 不正アクセス対策

（１） 運営管理者の措置事項

運営管理者は、不正アクセス対策として、以下の事項を措置しなければならない。
① 使用されていないポートを閉鎖しなければならない。
② 不要なサービスについて、機能を削除又は停止しなければならない。
③ 運営管理者は、緊急連絡窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

（２） 攻撃への対処

CISO 及び運営管理者は、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なければならない。また、総務省等と連絡を密にして情報の収集に努めなければならない。

（３） 記録の保存

CISO 及び運営管理者は、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なければならない。

（４）　内部からの攻撃

運営管理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等の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。

（５）　職員等による不正アクセス

運営管理者及び情報システム管理者は、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課室等の情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

（６）　サービス不能攻撃

運営管理者及び情報システム管理者は、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なければならない。

（７）　標的型攻撃

運営管理者及び情報システム管理者は、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

（１）　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

情報セキュリティ管理者等は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。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しなければならない。

（２）　不正プログラム等のセキュリティ情報の収集・周知

CISO 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、職員等に周知しなければならない。

（３）　情報セキュリティに関する情報の収集及び共有

CISO は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。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なければならない。

第７　運用

７．１　情報システムの監視

① 情報セキュリティ管理者等は、重要な情報資産については、アクセス権限情報や動作履歴等を取得する機能を設け、各種履歴情報を記録、保存、管理するとともに、定期的に履歴情報を分析するものとする。

② 運営管理者及び情報システム管理者は、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なければならない。

③ 情報システム管理者は、情報システムを監視し、適切な維持管理を実施するため、定期的な検査を行うものとする。

④ 情報システム管理者は、外部と常時接続するシステムを必要に応じて常時監視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

（１）　遵守状況の確認及び対処

① 統括管理者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに CISO 及び運営管理者に報告しなければならない。

② CISO は、発生した問題について、適正かつ速やかに対処しなければならない。

③ 運営管理者及び情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

（２）　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

情報セキュリティ管理者は、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パソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信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

① 職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに運営管理者及び情報セキュリティ管理者に報告を行わなければならない。

② 当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると運営管理者が判断した場合において、職員等は、緊急時対応計画に従って適正に対処しなければならない。

７．３　侵害時の対応等

（１）　緊急時対応計画の策定

CISO 又は運営委員会は、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、情報セキュリティ緊

急対応実施手順を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

（２）　緊急時対応計画に盛り込むべき内容

情報セキュリティ緊急対応実施手順には、以下の内容を定めなければならない。

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

（３）　業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定するとともに、業務継続計画の策定時及び変更時等において、運営委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（４）　緊急時対応計画の見直し

CISO 又は運営委員会は、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、必要に応じて情報セキュリティ緊急対応実施手順の規定を見直さなければならない。

７．４　例外措置

（１）　例外措置の許可

情報セキュリティ管理者等は、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。

（２）　緊急時の例外措置

情報セキュリティ管理者等は、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 に報告しなければならない。

（３）　例外措置の申請書の管理

CISO は、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

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。

① 地方公務員法（昭和 25 年法律第 261 号）
② 著作権法（昭和 45 年法律第 48 号）

③ 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）
④ 個人情報の保護に関する法律（平成 15 年法律第 57 号）
⑤ 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）
⑥ サイバーセキュリティ基本法（平成 28 年法律第 31 号）
⑦ 知事が保有する個人情報の適切な管理のための措置に関する要綱（令和 5 年 3 月 13 日　令 4 学事文書第 1564 号）

７．６　懲戒処分等

（１）　懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

（２）　違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

① 運営管理者が違反を確認した場合は、運営管理者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
② 情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに運営管理者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
③ 情報セキュリティ管理者の指導によっても改善されない場合、運営管理者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、運営管理者は、職員等の権利を停止あるいは剥奪した旨を CISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

第８　業務委託と外部サービスの利用

８．１　業務委託

（１）　委託事業者の選定基準

① 情報セキュリティ管理者等は、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しなければならない。
② 情報セキュリティ管理者等は、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、委託事業者を選定しなければならない。

（２）　契約項目

重要な情報資産を取扱う業務を委託する場合には、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しなければならない。

・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

・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
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・委託事業者の従業員に対する教育の実施
・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
・個人情報保護
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・県による監査、検査
・県による情報セキュリティインシデント発生時の公表
・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

情報セキュリティ管理者等は、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、（２）の契約に基づき措置を実施しなければならない。また、その内容を運営管理者に報告するとともに、その重要度に応じて CISO に報告しなければならない。

（４）　委託業者の違反行為発見時の対応

職員等は、委託業者の違反行為を発見した場合は、情報セキュリティ管理者等に報告し、指示を仰がなければならない。

８．２　外部サービスの利用に係る規程

情報セキュリティ管理者は、運営管理者が定める外部サービスの利用に関する規程に従って外部サービス利用の検討及び許可を得なければならない。

８．３　外部サービスの利用（機密性Ⅰ、Ⅱ及びⅢの情報を取扱う場合）

（１）　外部サービスの利用に係る調達・契約

① 情報セキュリティ管理者は、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書に含めなければならない。

② 情報セキュリティ管理者は、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なければならない。

（２）　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 情報セキュリティ管理者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、外部サービス（機密性Ⅰ、Ⅱ及びⅢの情報を取扱う場合）の利用に関する規程に従って導入・構築時のセキュリティ対策を講じなければならない。

② 外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。

（３） 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 情報セキュリティ管理者は、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（機密性Ⅰ、Ⅱ及びⅢの情報を取扱う場合）の利用に関する規程に従って運用・保守時のセキュリティ対策を講じなければならない。

② 情報セキュリティ管理者は、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しなければならない。

③ 外部サービス管理者は、前各項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・記録しなければならない。

（４） 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 情報セキュリティ管理者は、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（機密性Ⅰ、Ⅱ及びⅢの情報を取扱う場合）の利用に関する規程に従って更改・廃棄時のセキュリティ対策を講じなければならない。

② 外部サービス管理者は、前項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・記録しなければならない。

第９　評価・見直し

９．１　監査

（１） 実施方法

CISO は、情報セキュリティを監査する担当者として、運営管理者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

（２） 監査を行う者の要件

① 運営管理者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

② 監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

（３） 監査実施計画の立案及び実施への協力

① 運営管理者は、監査を行うに当たって、監査実施計画を立案し、運営委員会の承認を得なければならない。監査は、必要に応じて外部の者を交えて実施するものとする。

② 被監査部門は、監査の実施に協力しなければならない。

（４） 委託事業者に対する監査

委託事業者に業務委託を行っている場合、運営管理者は委託事業者（再委託事業者を含む）に対して、情報セキュリティポリシーの遵守について監査を定

期的に又は必要に応じて行わなければならない。

（５） 報告

運営管理者は、監査結果を取りまとめ、運営委員会に報告する。

（６） 保管

運営管理者は、監査の実施を通し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、紛失等が発生しないように適正に保管しなければならない。

（７） 監査結果への対応

CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、庁内で横断的に改善が必要な事項については、運営管理者に対し、当該事項への対処を指示しなければならない。

（８） 情報セキュリティポリシー及び関係規程等の見直し等への活用

運営委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

９．２ 自己点検

（１） 実施方法

① 運営管理者及び情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

② 統括管理者は、情報セキュリティ管理者と連携して、所管する部局における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状況について、毎年度及び必要に応じて自己点検を行わなければならない。

（２） 報告

運営管理者、情報システム管理者及び情報セキュリティ管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、運営委員会に報告しなければならない。

（３） 自己点検結果の活用

① 職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

② 運営委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

９．３ 情報セキュリティポリシー及び関係規程等の見直し

（１） 運営委員会は、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踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

（２）　運営委員会は、情報セキュリティポリシーの見直しについて、必要に応じて外部の専門家からの助言を求めることができる。

（３）　情報システム管理者は、情報セキュリティポリシーの改訂に応じて実施手順を見直すものとする。

附　則
この情報セキュリティポリシーは、平成１６年６月１７日から施行する。

附　則
この情報セキュリティポリシーは、平成２０年２月２２日から施行する。

附　則
この情報セキュリティポリシーは、平成２２年４月１日から施行する。

附　則
この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。

附　則
この情報セキュリティポリシーは、平成２８年４月１日から施行する。

附　則
この情報セキュリティポリシーは、平成３０年４月１日から施行する。

附　則
この情報セキュリティポリシーは、令和元年７月１６日から施行する。

附　則
この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。

附　則
この情報セキュリティポリシーは、令和６年４月１日から施行する。