「やまぐちエコ市場」ホームページ更改業務仕様書

本仕様書は、やまぐちエコ市場事務局（以下「委託者」という。）と受託者との間で契約する「やまぐちエコ市場」ホームページ更改業務（以下「本業務」という。）の委託について適用する。なお、本業務において更改するホームページを、以下「本サイト」という。

１　背景

「やまぐちエコ市場」は、リサイクル製品等のマッチングと、循環型社会の形成に向けた情報発信を目的として運営されているホームページであり、平成 18 年の開設以来、約 20 年が経過している。この間、構成やデザインの抜本的な見直しは行われておらず、現在の閲覧環境に必ずしも適合していない構成となっているため、見直しが必要な状況にある。

本サイトが担う機能は、大きく次の二つである。

（１）リサイクル製品等のマッチング（会員・非会員の双方を対象とし、事業者間取引（BtoB）及び事業者・消費者間取引（BtoC）の双方を想定する。）

（２）循環型社会の形成に資する情報発信（会員に対する関連法令の改正情報の提供等）

現状では、上記（２）の情報発信に対する利用者からの要望が高い一方、（１）のマッチングについては情報の更新が滞っている。本業務は、これらの課題を踏まえ、利便性が高く時流に合ったサイトへと全面的に更改するものである。

（参考：現行ホームページ URL　https://eco.pref.yamaguchi.lg.jp/ecoichiba/）

２　現行サイトの状況

現行サイトの状況は以下のとおりである。受託者は、これらを参考とした上で、本業務における最適なサイト構成、移行計画及びセキュリティ対策を提案すること。

（１）会員等の状況

- 会員数：約 300 社・団体
- 開設：平成 18 年 5 月
- 月間アクセス数：会員 645PV／約 300 ユーザー、非会員 約 15,000PV
- ピーク時期と時期別アクセス数：ピーク 6～8 月　アクセス約 48,300 人
- 掲載件数：マッチング情報 94 件、お知らせ等 273 件、掲示板 2,408 件
- 総ページ数（固定ページ）：17 ページ

・データベース容量：123MB

・サーバーのディスク使用量：約 200GB

（２）システム構成・稼働環境

・現行のコンテンツ管理システム（CMS）は、独自のシステムにより構築されている。

・ドメインは、委託者が契約している既存のものを継続して使用する。

・現行のサーバー環境は、「さくらインターネット」のレンタルサーバーである。

（３）サイト構成

・トップページには、「売ります・買います・提供・受入・融資します情報」「イベント情報」「環境法令情報等」「掲示板」「会員限定情報」等のコンテンツを掲載している。

・このほか、「市場の概要」「活動案内」「行政情報」「報道記録」「人材情報」「リンク集」「Q&A」「お問い合わせ」等のページを設けている。

（４）主な機能

・会員向けのログイン機能及び会員検索機能を有している。

・「売ります・買います」等の投稿機能では、投稿を区分（仲介・教える、売ります、買います、資源提供、資源受入、資金融資）ごとに一覧表示できるほか、キーワードによる絞り込みができる。

・お知らせ等の情報発信機能を有している。

３　事業の目的

本事業は、単にサイトのデザインを刷新するにとどまらず、利用者が必要な情報を見つけやすい構成へと再設計することにより、次の二つを目的として、本サイトを構築するものである。

（１）リサイクル製品等のマッチングを活性化し、循環型社会の形成に寄与すること。

（２）情報発信の利便性を向上させ、会員及び一般利用者の双方にとって使いやすいサイトとすること。

あわせて、会員等への情報提供や、更改後の継続的な機能改善につながるデータの収集・蓄積・活用の基盤を整備し、マッチング件数の底上げ及び循環型社会の認知向上を図るものとする。

４　本事業における基本的な考え方

本サイトは、委託者が行う循環型社会形成の取組を円滑に推進するための基盤として位置付ける。

（１）情報発信に関する考え方

・掲載情報を整理し、利用者が必要な情報に容易に到達できる構成とすること。重複した項目や古い情報を整理するとともに、アクセスの多いコンテンツや優先的に紹介したいコンテンツ（人材募集等）が下部に埋没しないよう配置すること。

・委託者の担当者が、専門的な知識を要することなく、文書作成ソフトと同等の感覚で記事や写真を投稿・更新できる CMS を導入すること。

（２）マッチングに関する考え方

・投稿された案件の問い合わせ・交渉等の状況を可視化することにより、利用者の関心を高め、参加を促進する構成とすること。

・投稿時の記載項目を整理することにより、情報の平準化及び検索性の向上を図ること。

（３）データの活用に関する考え方

・アクセス状況や利用状況等のデータを収集・蓄積し、更改後の継続的な機能改善や、会員等への情報提供に活用できる構成とすること。

（４）閲覧環境に関する考え方

・一般消費者を含む幅広い利用者の流入を想定し、パソコンに加え、スマートフォン等の各種デバイスにおいても支障なく閲覧・利用できる設計とすること。

（５）AI の取扱いに関する考え方

・本更改においては、データの蓄積が十分でないこと等を踏まえ、AI を用いた機能は採用しないこととする。まずはデータの収集・蓄積・活用の方向性を整備することを優先する。

（６）運営・引継ぎに関する考え方

・構築後は委託者が主体となって運営することを想定し、更新・引継ぎが容易で、特定の事業者に依存しない構成とすること。

（７）最低限仕様及び積極提案の位置付け

・本仕様書に記載している内容は、委託者が本業務を実施するにあたり、最低限必要と考えている事項を示したものである。受託者は、専門的な知見や経験を活かし、本事業の目的達成に資する効果的な提案を積極的に行うものとする。

５　予算限度額

本業務の予算限度額は、金 5,000,000 円（消費税及び地方消費税を含む。）とする。提案金額が予算限度額を超える場合は、審査の対象としない。

６　参加資格

本業務の提案に参加できる者は、次の各号のいずれにも該当する者とする。

（１）過去５年間に、システム構築改修に関する業務の実績を有する者

（２）地方自治法施行令第 167 条の４第１項各号及び第２項各号のいずれにも該当しない者（破産者、暴力団員等でないこと、契約の履行に当たり不正行為等をした者でないこと）

７　委託業務の内容

（１）業務内容

本事業における受託者の業務内容は、以下のとおりとする。

なお、業務に当たっては、「山口県情報セキュリティポリシー」を遵守すること。

ア　ホームページ全体の企画・構成設計・デザイン制作

イ　情報設計（利用者が目的から情報に到達できる導線設計を含む。）

ウ　CMS の構築・実装

エ　本仕様書に定める各機能の開発・実装

オ　現行サイトからのデータ移行及び検証

カ　テスト及び動作確認

キ　本番環境への公開

ク　委託者による「やまぐちエコ市場 WEB システム 情報セキュリティ標準実施手順」作成の支援（情報提供、作成物の技術的確認等）

ケ　納品・引継対応（委託者による運営を前提とした運用・管理面の引継ぎを含む。）

（２）業務範囲外

以下の業務については、本仕様書に基づく契約範囲には含まない。

ア　本サイト公開後の継続的な運営・更新業務（委託者が主体となって実施することを想定する。）

イ　本サイト公開後の保守・運用に係る対応。ただし、契約期間内において、本仕様書に基づき構築した内容に起因する不具合や動作不良、又は本仕様書との不整合が公開後に判明した場合については、受託者の責任において対応するものとする。

ウ　前号ただし書きに該当しない改修、機能追加、仕様変更、運用支援等については、必要に応じて別途協議の上、契約を行うものとする。

（３）次年度以降の運用・保守費用の提示

受託者は、本業務完了後の安定的な運用に資するため、次年度以降に必要となる運用・保守費用（サーバー維持費、システム保守費等）の参考見積り（年額）を提案書に含めるものとする。なお、当該見積りは次年度以降の予算確保に向けた参考資料として活用するものであり、本業務の委託料には含まないものとする。

８　機能要件

本サイトに実装する機能は、以下のとおりとする。各機能は、AI を用いずに実現することを前提とする。

（１）公開サイト機能（一般利用者・非会員向け）

【必須機能】

ア　企業（会員）の情報を紹介する機能。会社案内を基礎とし、リサイクルに関する情報（技術・施設・製品等）や人材募集に関する情報を企業単位で集約して発信できること。これにより、閲覧者が企業の全体像を把握しやすい構成とすること。なお、これらの情報の登録・編集は、会員向け機能において会員自身が行うものとする。

イ　リサイクルに関する情報や人材募集に関する情報について、より詳細な内容を掲載する場合に、会社案内とは別のページ（ミニウェブサイト）を作成し、リンクして提供できること。

ウ　トップページ上部（最も目立つ箇所）に、新着投稿のお知らせや「売ります・買います」等の情報を表示するとともに、リサイクル製品の画像が大きく表示され、かつ動的に切り替わる仕組みを設けること。

エ　サイト内の検索機能。利用者が必要な情報を検索により探せること。

オ　産廃業者の許可情報の連携表示機能。管理者が山口県オープンデータから取得（ダウンロード）した産廃業者の許可情報のファイル（CSV 形式）を、管理画面からアップロードすることにより、会社案内等と連携して表示できること。

- 当該連携にあたっては、山口県オープンデータに公開された情報を経由して取り込む方式とすること。
- 取り込んだファイルの内容を、会社案内等の該当箇所に反映して表示できること。更新頻度は月 1 回程度を想定する。

カ　検索エンジンへの対策（SEO）。サイトマップ（XML）の自動生成やメタ情報の設定等の基本的な対策に加え、特定の言葉（例：山口県　木質ペレット）で検索された際に本サイトが上位に表示されるよう対策を講じ、非会員や一般消費者の流入を見込めること。また、SEO 対策に当たっ

ては、AIによる検索回答（AI Overview）も考慮し、本サイトの情報がAIに正しく引用・参照されるような設計についても検討すること。

（２）会員向け機能

【必須機能】

ア　会員のログイン機能及び会員専用のページ機能。現行サイトが有する会員ログイン機能を踏襲すること。

イ　「売ります・買います」等の投稿機能。会員自身が案件を投稿・編集し、公開又は非公開を設定できること。投稿には複数枚の写真を掲載できることとし、動画については、外部動画サービスのURLを指定することで、投稿内に動画を埋め込んで表示できること。

ウ　投稿時の情報項目の充実。投稿者が必要な項目を記載できるよう、商品の情報として「提供場所」「性状」「発生時期」「BtoB・BtoC」等の項目を、投稿者の情報として「産業廃棄物処理業の許可の有無」「優良産廃事業者の認定の有無」「エコアクション21・ISO等の認証の取得状況」等の項目を設けること。

エ　マッチング状況の見える化機能。問い合わせの状況にある投稿について「交渉中」等の状況を表示し、他の利用者の参加を促進すること。

オ　会員向けのプッシュ通知機能。情報の更新の都度、会員にメールで自動的に通知できること。なお、会員が受け取る情報の種類を選択できることとし、情報過多を防ぐこと。

（３）管理者向け機能（事務局向け）

【必須機能】

ア　コンテンツの管理機能。委託者の担当者が、文書作成ソフトと同等の感覚で、記事・お知らせ・固定ページ等を作成・更新・公開できること。また、記事の下書き保存、公開予約、編集履歴の管理ができること。

イ　会員の管理機能。会員情報の登録・更新・管理、及び会員が投稿したコンテンツの承認・公開管理ができること。

ウ　産廃業者の許可情報のファイル（CSV形式）のアップロード機能（第1号オに定めるもの）。

エ　アクセス状況の把握機能。アクセス状況や利用状況等を把握できる解析手段を備え、更改後の改善検討に活用できること。

（４）共通機能

【必須機能】

ア　関連情報の表示機能。閲覧中の案件・記事に対し、あらかじめ定めた条件に基づき、関連する情報を自動的に表示できること。なお、AI は用いないこと。

イ　レコメンド機能。AI を用いず、投稿内容（カテゴリ・タグ等）を基本とし、必要に応じて閲覧履歴等を活用した簡易な方法により、利用者の関心に応じた情報を提示できること。

９　非機能要件

（１）アクセシビリティと閲覧環境

ア　ウェブサイトの作成に当たっては別記１「ウェブアクセシビリティの確保に関する特記事項」に基づき、ウェブアクセシビリティを確保すること。

イ　一般消費者を含む幅広い利用者の閲覧を想定し、パソコン及びスマートフォン等の主要なデバイスにおいて、適切に表示・操作できるレスポンシブデザインとすること。

（２）セキュリティと安全性

ア　常時 SSL 化（HTTP でのアクセスを HTTPS へ統一すること）に対応すること。また、不正アクセスの防止、データの改ざんの防止、個人情報の保護等に必要なセキュリティ対策を講じること。

イ　CMS は脆弱性が生じ得ることから、公開後に、委託者又は保守事業者が必要なセキュリティアップデートを実施できる構成とし、必要な情報を引き継ぐこと。

ウ　データについては、定期的に自動バックアップが取得される仕組みを構築し、障害発生時に速やかな復旧が可能な構成とすること。

エ　障害又は事故の発生時には、速やかに委託者へ報告し、指示に基づき対応すること。

オ　管理画面については、ID・パスワード認証に加え、多要素認証（MFA）を必須とすること。

カ　公開前に基本的な脆弱性対策（SQL インジェクション、XSS 等）を講じること。

キ　アクセスログを一定期間保存すること。

ク　一定回数以上のログイン試行に失敗した場合は、アカウントロック等の措置を講じること。

ケ　パスワードは一定の複雑性要件を満たすものとすること。

コ　セキュリティ対策にあたっては、別記２「Web アプリケーションセキュリティに係る特記仕様書」に基づき、情報セキュリティを確保すること。

サ　脆弱性診断については、別記２「Web アプリケーションセキュリティに係る特記仕様書」の『別紙１脆弱性リスト』に記載の脆弱性が、本サイトに混入していないか、受託者側で診断し、

「脆弱性診断結果報告書」を成果物として提出すること。なお、診断の実施方法及び実施主体は問わないものとする。また、脆弱性が判明した場合は、速やかに改善策を図ること。

シ　「山口県情報セキュリティポリシー」に準拠した対応及び環境を整えること。

ス　情報セキュリティ体制について、別紙２「受託事業者における情報セキュリティ自己評価シート」を提出すること。また、情報セキュリティの順守状況に関する確認結果に基づき、必要と判断された場合、受託者は委託者による監査に応じるものとする。

（３）システム性能と可用性

ア　利用者がストレスなく閲覧・操作できるよう、ページの表示速度やシステムの応答性に配慮した設計とすること。目安については、以下の通りである。

「１」トップページの表示時間は 3 秒以内を目安とすること。

「２」検索処理は概ね 2 秒以内に結果が表示されること。

イ　可用性については、1 日から 2 日程度の停止が許容可能であることから、冗長構成は必須としない。ただし、障害発生時は原則 24 時間以内の復旧を目標とする。

（４）データ移行

ア　会員情報、及び会員が現に掲載している有効な情報（公開中の案件・需給情報等）については、現行の保守事業者から提供されるデータ及び関連資料を委託者が受領し、受託者に提供するものとする。受託者は当該データ等を用いて、新システムへ移行すること。なお、提供データの形式は CSV その他移行に必要な形式を含むものとする。

イ　過去の古い情報（掲載期間が終了したお知らせ等）は、原則として移行しないこととし、会員が掲載している有効な情報のうち移行の対象としないものについては、新システムの稼働後に会員へ再投稿を案内すること。

ウ　移行の対象とするデータの範囲については、委託者と協議の上で確定するものとする。

（５）ドメイン・サーバー

ア　本サイトの公開にあたっては、委託者が契約している既存のドメインを継続して使用すること。

イ　サーバー環境は現行環境の継続を基本とするが、セキュリティ対策等の観点から、受託者の提案により新規のレンタルサーバー環境へ移行することができる。この場合、サーバーの選定は委託者と協議の上決定し、移行・設定に係る作業は本業務に含むものとする。新システムへの切替えに伴う移行作業及び設定変更作業は、委託者と協議の上、受託者が主体となって実施すること。

１０　成果物の帰属及び運営主体に関する基本条文

（１）成果物の帰属

本業務により作成された成果物の著作権（著作権法第 27 条及び第 28 条の権利を含む。）は、すべて委託者に帰属するものとする。

（２）運営主体

本サイトは、構築後、委託者の責任の下、委託者が主体となって運営するものとする。

１１　成果物の引渡し及び引継ぎ

受託者は、本サイトの構築完了後、委託者の担当者が円滑に運営できるよう、管理方法、更新手順、システム構成等について十分な説明及び引継ぎを行うものとする。

特に、委託者の担当者による記事・お知らせ等の投稿・更新が想定されることから、操作研修を実施すること。

公開後の一定期間内に発見された軽微な修正や設定変更については、第 7 の業務範囲外の定めによるほか、受託者の責任において速やかに対応すること。

１２　個人情報の保護

本サイトは会員（事業者）の情報を取り扱うため、担当者の氏名・連絡先等の個人情報が含まれることに留意すること。受託者は、業務の履行に伴う個人情報の取扱いについて、個人情報の保護に関する法律（平成 15 年法律第 57 号）、関係法令等及び別記３「個人情報取扱特記事項」を遵守することとともに、本業務に従事する者に対して守秘義務を課すこと。なお、当該守秘義務は、本業務の終了後も有効に存続するものとする。。また、別記３「個人情報取扱特記事項」の遵守状況については、別紙３「個人情報の適正管理等に関する確認票」により、契約締結の日から起算して 10 営業日以内に委託者へ報告すること。

１３　スケジュール

本業務に関連するスケジュールは以下のとおりである。各工程の具体的な内容及び詳細なスケジュールについては、契約締結後、受託者の提案を踏まえ、委託者と協議の上で決定する。

新サイト公開後に不具合等が発生した場合においても、会員等へのサービス提供に支障が生じないよう、公開・移行方法及び必要な措置について十分検討すること。

工程	令和8年			令和9年		
	10月	11月	12月	1月	2月	3月
要件定義・現況調査						
サイト設計						
デザイン制作						
ＣＭＳ構築・機能開発						
データ移行						
テスト・動作確認						
操作研修						
本番公開準備・引継ぎ						

※　上表の時期は目安である。本業務の履行期限は令和9年3月31日とし、リニューアル後の本サイトの公開予定日は令和9年4月1日とする。

１４　成果物・納品物

本業務において受託者が作成し、委託者に納品する成果物は、次のとおりとする。なお、以下に記載のない成果物であっても、本業務の目的達成に必要なものについては、協議の上、成果物として納品を求めることがある。

ア　サイト設計書一式（情報設計、画面設計、データ設計、運用設計等）

イ　デザインデータ一式

ウ　操作手順に関する説明資料

エ　業務完了報告書

オ　本システムを構成するプログラム一式および必要な設定情報

カ　脆弱性診断結果報告書

上記のほか、テスト資料等のドキュメントについては、本業務の目的に照らして必要な範囲とし、その要否は委託者と協議の上で定める。

１５　実施計画書の提出

受託者は、業務を円滑に遂行するため、実施体制（業務責任者、連絡担当者及び業務従事者の氏名並びに連絡先）、実施方法、実施スケジュール等を記載した実施計画書を作成し、契約締結の日から起算して10営業日以内に委託者へ提出の上、委託者の承認を得ること。

１６　留意事項

委託者は、受託者が事業の実施にあたり本仕様書に反した場合、委託契約額の一部又は全部を返還させる権利を有するものであること。

１７　業務実施上の注意点

（１）受託者は、業務の実施状況について、必要に応じて委託者と協議・打合せを行いながら進めるものとする。

（２）何らかのトラブルが発生した場合、受託者は委託者と連携の上、速やかに解決を図ること。

（３）業務の履行に関して知り得た情報をほかに漏らしてはならない。この契約が終了し、又は解除された場合においても同様とする。

（４）受託者は、本業務の全部又は一部を第三者に再委託しようとする場合には、あらかじめ委託者の承認を得るものとする。なお、再委託を行う場合であっても、受託者は本業務全体について一切の責任を負うものとし、業務の品質及び情報セキュリティの確保に十分配慮すること。

１８　仕様書の変更等

本仕様書の記載事項で変更する必要があるときは、委託者と受託者の協議により、これに従うものとする。

１９　資料の提供

（１）委託者は、受託者が本仕様を実現するにあたって必要と認められる資料を、受託者に無償で貸与する。

（２）受託者は、提供を受けた資料が不要となったときは、遅滞なく委託者に返還すること。

２０　疑義

本仕様書に関して疑義の生じた事項及び本仕様書に定めのない事項については、すべて委託者と受託者が協議の上、これを解決するものとする。

以　上

別記１

ウェブアクセシビリティの確保に関する特記事項

１　目標とする適合レベル

JIS X 8341-3:2016 のレベル AA に準拠すること。

本仕様書における「準拠」という表記は、情報通信アクセス協議会ウェブアクセシビリティ基盤委員会「ウェブコンテンツの JIS X 8341-3:2016 対応度表記ガイドライン 2021 年 4 月版」で定められた表記による。

２　適合する達成基準

レベル A およびレベル AA 全て。（詳細は「山口県目標達成基準」のとおり）

３　対象範囲

本業務で制作するウェブサイトのすべてのページ

ただし、下記項目については対象範囲から除く

1. Google のサービスを使用しているコンテンツ
2. YouTube のサービスを使用しているコンテンツ
3. Facebook、Ｘ、Instagram などの SNS のコンテンツ
4. PDF 等添付ファイル

４　依存するウェブコンテンツ技術

HTML5, CSS3 及び JavaScript 1.8.5

５　確認の実施

HTML、CSS の雛形作成段階において、受託者にて達成基準への対応状況の確認を実施すること。ツールによる判定が可能な検証項目については、ツールを用いた上で、そのツール名を記録すること。

６　試験の実施

納品前に JIS X 8341-3:2016 に基づく試験を実施すること。受託者は試験結果について委託者に説明を行い、その了承を得ること。

試験の実施においては、ツールによる判定だけでなく、人間による判断も行うこと。

７　試験の対象範囲

JIS X 8341-3:2016 の「JB.1.2 ウェブページ一式単位」とし、「d) ウェブページ一式を代表するウェブページとランダムに選択したウェブページとを併せて選択する場合」にある方法を用いて、両方を合わせて 40 ページを選択して試験を実施すること。

なお、ページ数の内訳は以下の通りとする。

・ウェブページ一式を代表するウェブページ：15 ページ

・ランダムに選択したウェブページ：25 ページ

８　達成方法及びその検証方法を特定できる技術的根拠（実装チェックリスト）の作成

ウェブアクセシビリティ基盤委員会が公開している「JIS X 8341-3:2016 試験実施ガイドライン 2020 年 12 月版」の「3.1 達成方法及びその検証方法を特定できる技術的根拠を示す方法の例」を参考にして実装チェックリストを作成すること。

９　達成基準チェックリストの作成

ウェブアクセシビリティ基盤委員会が公開している「JIS X 8341-3:2016 試験実施ガイドライン 2020 年 12 月版」の「3.2 達成基準チェックリストの例」を参考にして作成すること。

10　成果物

適用する達成基準の要件を満たすウェブコンテンツ一式

適用する達成基準の要件を満たすことを示す試験結果資料

・実装チェックリスト

・達成基準チェックリスト

山口県目標達成基準

項目	JIS X 8341-3:2016		
	細分箇条	達成基準	適合レベル
1	1.1.1	非テキストコンテンツの達成基準	A
2	1.2.1	音声だけ及び映像だけ（収録済み）の達成基準	A
3	1.2.2	キャプション（収録済み）の達成基準	A
4	1.2.3	音声解説又はメディアに対する代替コンテンツ（収録済み）の達成基準	A
5	1.2.4	キャプション(ライブ)の達成基準	AA
6	1.2.5	音声解説（収録済み）の達成基準	AA
7	1.3.1	情報及び関係性の達成基準	A
8	1.3.2	意味のある順序の達成基準	A
9	1.3.3	感覚的な特徴の達成基準	A
10	1.4.1	色の使用の達成基準	A
11	1.4.2	音声の制御の達成基準	A
12	1.4.3	コントラスト（最低限レベル）の達成基準	AA
13	1.4.4	テキストのサイズ変更の達成基準	AA
14	1.4.5	文字画像の達成基準	AA
15	2.1.1	キーボードの達成基準	A
16	2.1.2	キーボードトラップなしの達成基準	A
17	2.2.1	タイミング調整可能の達成基準	A
18	2.2.2	一時停止、停止及び非表示の達成基準	A
19	2.3.1	3回のせん（閃）光,又はしきい（閾）値以下の達成基準	A
20	2.4.1	ブロックスキップの達成基準	A
21	2.4.2	ページタイトルの達成基準	A
22	2.4.3	フォーカス順序の達成基準	A
23	2.4.4	リンク目的（コンテキスト内）の達成基準	A
24	2.4.5	複数の手段の達成基準	AA
25	2.4.6	見出し及びラベルの達成基準	AA
26	2.4.7	フォーカスの可視化の達成基準	AA
27	3.1.1	ページの言語の達成基準	A
28	3.1.2	一部分の言語の達成基準	AA
29	3.2.1	フォーカス時の達成基準	A
30	3.2.2	入力時の達成基準	A
31	3.2.3	一貫したナビゲーションの達成基準	AA
32	3.2.4	一貫した識別性の達成基準	AA
33	3.3.1	エラーの特定の達成基準	A
34	3.3.2	ラベル又は説明の達成基準	A
35	3.3.3	エラー修正の提案の達成基準	AA
36	3.3.4	エラー回避（法的,金融及びデータ）の達成基準	AA
37	4.1.1	構文解析の達成基準	A
38	4.1.2	名前（name）,役割（role）及び値（value）の達成基準	A

※全38項目に対応します

別記２

やまぐちエコ市場 WEB

Web アプリケーションセキュリティに係る特記仕様書

2026 年８月

やまぐちエコ市場事務局

1. 本特記仕様書の目的と運用

本特記仕様書（以下「本書」という。）は、やまぐちエコ市場 WEB（以下「本システム」という。）のシステム調達仕様書（以下「仕様書」という。）に加え、本システムに追加で求めるセキュリティ要件、対応指針を記載するものである。

なお、本書に記載されているセキュリティ要求仕様に関して、契約書及び仕様書の記載が本書と異なる場合は、契約書及び仕様書を優先する。

2. Web アプリケーション脆弱性対応

本システムにおける Web アプリケーションの脆弱性対応として次の要件を満たすこと。

(1)『別紙 1 脆弱性リスト』で示す脆弱性が本システムに混入しないよう Web アプリケーションを構築すること。

(2)『別紙 1 脆弱性リスト』で示す脆弱性が Web アプリケーションに混入しないように構築するための方針をやまぐちエコ市場事務局に提示すること。

3. セキュリティ機能

本システムにおけるセキュリティ機能について、以降に示す機能を設ける場合は、各項の要件を満たすこと。

3.1. ログイン処理

3.1.1. 利用者認証方式

利用者認証を行う場合、認証方式はパスワード認証とする。

3.1.2. アクセス制御機能

(1) 利用者の認証を行い、認証した利用者のみが本システムの「利用者認証を要する機能（画面）」を利用できるようにすること。

(2) 利用者認証を経ていない者は本システムの「利用者認証を要する機能（画面）」を利用できないようにすること。

(3) 「利用者認証を要する機能（画面）」は、セッションが終了した後は利用できないこと。

3.1.3. パスワードに利用できる文字

パスワードに利用する文字は以下を遵守すること。ただし、二要素認証の第 2 要素（ワンタイムパスワードトークンの生成するパスワードなど）はこの限りでない。

(1) パスワードに利用できる文字種は、英字（大文字、小文字を区別）、数字、記号の 3 種とし、それぞれ自由に利用できること。

(2) パスワードに利用する文字数は 8 文字未満を受け付けないようにすること。また、少なくとも 64 文字のパスワードは受け入れられること。

3.1.4. ログインフォームの実装方法

パスワードの入力欄は入力した文字を伏字にすること。又は、伏字にする・しないを選択できる機能を持つこと。

3.1.5. ログイン失敗時のメッセージ出力

パスワード認証に失敗した際に、利用者 ID の間違いか、パスワードの間違いかが区別できるメッセージを表示しないこと。

3.1.6. アカウントロック機能

特定の利用者 ID に対するパスワードの間違いが一定回数を超えた場合に、アカウントをロックする機能を実装すること。

(1) パスワードは平文で保存せず、ソルトつきハッシュの形で保存すること。

(2) ソルトは利用者毎に別々に設定すること。

3.1.7. セッション管理機能

(1) 利用者のセッション管理にはプログラミング言語や Web アプリケーション実行環境の備えるセッション管理機構を用いること。

(2) ログイン状態にある利用者のセッション識別のための情報（セッション ID）は、クッキーを用いて保持すること。

3.1.8. セッションの開始

セッションはログイン処理成功後に開始すること。

3.1.9. セッションの終了

次の場合はセッションを終了し、セッション情報を破棄すること。

(1) 利用者がログアウト機能を呼び出した場合（ログアウトボタンを押す等）

(2) 最後にページが表示された時刻を起点としてセッションの有効期間を超えた（セッションタイムアウト）場合

3.2. 認可処理

3.2.1. 認可処理の要件定義と文書化

認可処理は次のとおり文書化し、権限毎の役割をロールとして作成すること。

(1) 認可処理の必要な機能、情報を識別して、認可処理の必要な画面を、山口県に提示すること。

(2) 各ロールと権限を一覧表（権限マトリックス）に整理すること。

3.2.2. 認可処理の実装

(1) 各利用者の権限確認には、セッション変数に保存された利用者識別情報（利用者 ID 等）を基準とすること。

(2) 認可を要する情報表示や機能実行をする前に、実行中の利用者が、当該情報の表示や機能を実行するための権限を有していることを画面毎に確認すること。

(3) 認可されなかった場合は、適切なエラー表示をすること。

3.3. アカウント管理

3.3.1. 利用者登録（アカウントの作成）時における登録メールアドレスの確認

(1) ログイン処理のあるシステムで、利用者登録時にメールアドレスを登録させた場合は、登録されたメールアドレスに対してメールを送付し、登録メールアドレスが利用者に利用されているアドレスであることを確認すること。

(2) 登録メールアドレスが利用者に利用されているアドレスであると確認できた後に本システムにおける利用者登録を完了（登録の確定）とすること。

(3) 登録されたメールアドレスに対してメールを送付する際に、利用者が登録したパスワードを記載しないこと。

3.3.2. 利用者 ID の重複防止機能

利用者 ID が重複しないよう、チェック処理を含めること。

3.3.3. 登録メールアドレス変更機能

利用者が登録したメールアドレスを変更する機能を実装する場合は、メールアドレス変更機能の実行後は、利用者登録時と同様の処理を経ること。

3.3.4. パスワード変更機能

利用者がパスワードを変更する機能を実装する場合は、パスワード変更機能の実行前に、現在のパスワードの入力を利用者に求め、正しいパスワードであることを確認すること。

3.3.5. パスワードリセット機能

利用者がパスワードを失念した場合の対処機能を備える場合は、次の（1)、(2）いずれかの方式とし、(3) または (4) の要件を満たすこと。(利用者確認の手段として、予め登録したメールアドレスに宛てたメールが受信できることを用いる。)

(1) パスワードリセット機能を利用するための URL を登録メールアドレスにメール送付する方式

(2) 仮パスワードを発行し、メールで通知する方式（仮パスワードでログインした場合は、パスワード変更機能のみが利用できるものとする）

(3) （1）の機能の実装に際して、第三者がパスワードリセット機能を使えないように、URL には十分長い乱数による秘密情報（以下「トークン」という。）をつけること。

(4) （2）の機能に対する総当たり攻撃対策を施すこと。

3.3.6. 管理者によるアカウント削除・一時利用停止機能

(1) 管理者による利用者アカウントの削除機能を実装すること。

(2) 管理者による利用者アカウントの一時利用停止機能を実装すること。

3.3.7. 利用者によるアカウント削除機能

利用者による自身のアカウントを削除する機能を実装する場合は、アカウント削除機能の実行前に、パスワードの入力を利用者に求め、正しいパスワードであることを確認すること。

3.4. ログイン状態にある利用者の意図に反した機能実行の防止機能

外部リンク等により本システムの画面（機能）に遷移するだけで、本システムの機能がログイン状態にある利用者の意図に反して実行されることを防止するため、以下の対策を実施すること。

・クロスサイト・リクエスト・フォージェリ（CSRF） 対策

・クリックジャッキング対策

3.5. ログ出力

システム監査、事故調査の目的のため、本システムで取得するログの内容を検討し、山口県に提示すること。また、ログの出力・保管方法についてもあわせて協議すること。

3.5.1. ログからの情報漏えい・改ざん対策

(1) ログを取得する場合は、ログが不正に参照・変更・削除されないよう保護すること。

(2) ログから個人情報等の秘密情報が漏えいすることを防ぐため、ログの目的（監査、事故追跡）を損なわない範囲で秘密情報を含めない処理又は秘密情報の一部のみの出力（マスク処理）をすること。

3.5.2. ログの保管

(1) ログの保管年限は 1 年以上とする。

(2) ログの安全な保管方法（媒体、保管フォーマット、保管場所等）を定めること。

3.6. 暗号化

3.6.1. 利用者と本システム間における Web アプリケーション通信の暗号化

(1) システムで送受信する情報のうち、機密性・完全性の高い情報を送受する場合は、通信を暗号化すること。

(2) サーバ証明書は利用を想定するすべてのブラウザで警告の出ないものを使用し、証明書の発行先名は、運営者の名称とする。地方公共団体組織認証基盤（LGPKI）を用いる場合は、Firefox を利用想定ブラウザから外すこと。

(3) SSL2.0 及び SSL3.0 は使用しない設定にすること。

3.6.2. データベースの暗号化

(1) 機密性・完全性の高い情報をデータベース・ファイルに保存する際は暗号化を施すこと。

(2) 暗号化アルゴリズムは電子政府推奨暗号リストに記載されたアルゴリズムを用いること。

(3) 暗号鍵の管理方法を計画書に記載すること。

3.7. 出荷時

納品時における OS、ミドルウェア等ソフトウェアのバージョン及び最新パッチのリリース状況を確認すること。

以上。

別紙1 脆弱性リスト

以下に記載するWebアプリケーションの脆弱性について、本システムに混入しないよう対処すること。また、脆弱性対策の実施に際しては、独立行政法人情報処理推進機構（IPA）が示す「安全なウェブサイトの作り方」の最新版における「根本的解決」および「セキュア・プログラミング講座」を参考にすること。

なお、脆弱性項目のうち、本システムのWebアプリケーションに入力フォームがない等、脆弱性がないことが明らかである場合、該当する項目は除外してよい。

項番	脆弱性項目
1	SQLインジェクション
2	OSコマンド・インジェクション
3	ディレクトリ・トラバーサル脆弱性
4	「ログイン機能」の不備 ①推測可能なセッションID ②URL埋め込みのセッションIDの外部への漏えい ③クッキーのセキュア属性不備 ④セッションIDの固定化
5	クロスサイト・スクリプティング(XSS)
6	利用者の意図に反した実行の防止機能の不備 ①クロスサイト・リクエスト・フォージェリ（CSRF） ②クリックジャッキング
7	メールヘッダ・インジェクション脆弱性
8	「アクセス制御」と「認可処理」の不備 ①アクセス制御 ②認可処理
9	HTTPヘッダ・インジェクション
10	evalインジェクション
11	競合状態の脆弱性
12	意図しないファイル公開
13	アップロードファイルによるサーバ側スクリプト実行
14	秘密情報表示時のキャッシュ不停止（キャッシュを介して情報の暴露）
15	オープンリダイレクタ脆弱性（意図しないリダイレクト）
16	クローラへの耐性

別紙２

受託事業者における情報セキュリティ自己評価シート

当社における情報セキュリティ体制については、下記のとおりです。

令和○○年○○月○○日

やまぐちエコ市場事務局　御中

受託者　株式会社○○○○○○

代表取締役社長　○○　○○

受 託 業 務	

＜記入要領及び必要条件＞

(1) 回答欄はすべて②又は③であることとし、②を記入した場合は③に向けて努力すること。

(2) ①を記入した場合は、説明事項欄に改善予定日や代替策を記載すること。

(3) 非該当の項目は、回答欄に「－」を記入し、説明事項欄にその理由を記載すること。

項　　目		選　　択		回答(①～③)	説明事項
1	情報セキュリティに関する社内規定	①	情報セキュリティに関する社内規定がない。		
		②	社内規定を定めているが、周知の徹底はなされていない。		
		③	社内規定を定め、定期的に見直しを行い全社に共有されている。		
2	セキュリティインシデント発生時の体制	①	発生時に都度対応を行うため体制は整えていない。		
		②	発生時に対応を行う担当者を決めている。		
		③	発生時からクロージングまでの対応が明文化されており、休日や夜間などの緊急時にも対応できる体制が整えられている。		
3	機密情報の取扱い	①	機密情報取扱いに関する社内規定がない。		
		②	機密情報取扱いに関する社内規定が存在しており、周知をしている。		
		③	機密情報取扱いに関する社内規定が存在しており、規定通りの運用がなされているか定期的にチェックをする手続きが定められている。		
4	秘密保持に関する誓約	①	従業員（派遣を含む）と秘密保持誓約を締結していない。		
		②	従業員（派遣を含む）と秘密保持誓約を締結している。		
		③	従業員（派遣を含む）と秘密保持誓約を締結しており、セキュリティ違反を犯した従業員に対する懲戒手続が整備されている。		
5	社内教育の実施	①	情報セキュリティや機密情報保護に関する社内教育を実施していない。		
		②	情報セキュリティや機密情報保護に関する社内教育を１年に１回以上実施している。		
		③	経営層や派遣を含む全ての従業員に対し、情報セキュリティや機密情報保護に関する社内教育を１年に１回以上実施している。		
6		①	制限していない。		
		②	委託者が許可した場合を除き、禁止している。		

	個人所有パソコンの社内への持込み	③	一切禁止しており、研修等において定期的に周知している。		
7	受託情報の社外への持出し	①	制限していない。		
		②	委託者が許可した場合を除き、禁止している。		
		③	②に加え、研修等において定期的に周知している。		
8	受託情報を含んだ書類や電子媒体の保管	①	施錠管理を徹底していない。		
		②	施錠管理されているキャビネットや倉庫等で保管している。		
		③	②に加え、入退室者等を記録して、それを責任者が確認している。		
9	受託情報を消去又は廃棄する方法	①	復元不可能な方法で行っていない。		
		②	復元不可能な方法で行っている。		
		③	復元不可能な方法で行い、その記録も取っており、更にその記録を責任者が確認している。		
10	受託情報を取扱うサーバ及び端末について、OS 等のセキュリティパッチやウイルス対策ソフトのパターンファイルの適用	①	適用していない。		
		②	信頼性の高いウイルス対策ソフトを導入し、パターンファイルは、すべてのコンピュータ（現場事務所のパソコンを含む。）で常に最新の状態にしている。セキュリティパッチは、すべてのパソコンを常に最新の状態にしているが、サーバは、システムへの影響を考慮し、可能な限り最新の状態にしている。		
		③	②に加え、定期的にログの確認や全ドライブスキャン等の点検も行っており、それを責任者が確認している。		
11	受託情報へのアクセス	①	ID・パスワード等で認証していない。		
		②	ID・パスワード等で認証し、アクセス制御をしている。		
		③	②に加え、IC カードや指紋認証等による認証も行っており、それを責任者が確認している。		
12	受託情報へのアクセス権限を付与すべき従業者	①	特定していない。		
		②	必要最小限に絞り、特定している。		
		③	必要最小限に絞り、具体的な氏名を書面化した上、定期的に見直しており、それを責任者が確認している。		
13	受託情報を格納した機器が接続されているネットワークへのアクセス制限	①	制限していない。		
		②	ファイアウォール・ルータ等で制限している。		
		③	②に加え、ログ等により不正アクセスを監視しており、それを責任者が確認している。		
14	受託情報をメールやファイル転送サービスで送信する場合の漏えい対策	①	暗号化等の対策を実施せずに送信している。		
		②	暗号化等の対策を実施した上で送信している。		
		③	暗号化等の対策を実施した上で、送信先のダブルチェックを行うなど誤送信対策を実施している。		
15	再委託先のセキュリティ自己評価確認		再委託先がある場合、委託先は、再委託先のセキュリティ自己評価確認を実施し、その写しをやまぐちエコ市場事務局に提出している。		

別記３

個人情報取扱特記事項

（基本的事項）

第１ 受託者（以下「乙」という。）は、この契約による業務の実施に当っては、個人情報の保護に関する法律（平成 15 年法律第 57 号）及び以下の事項を遵守し、個人の権利利益を害することのないよう、個人情報の取扱いを適正に行わなければならない。

（秘密の保持）

第２ 乙は、この契約による業務に関して知り得た個人情報をみだりに他に漏らしてはならない。この契約による業務が終了し、又はこの契約が解除された後においても、同様とする。

（取得の制限）

第３ 乙は、この契約による業務を実施するために取得する個人情報については、当該業務を達成するために必要な範囲内で、適法かつ適正な方法により取得しなければならない。

（目的外利用及び提供の禁止）

第４ 乙は、やまぐちエコ市場事務局（以下「甲」という。）の指示又は承認があるときを除き、この契約による業務に関して知り得た個人情報を契約の目的以外のために利用し、又は第三者に提供してはならない。

（適正管理）

第５ 乙は、この契約による業務に関して知り得た個人情報の漏えい、滅失、毀損の防止その他の個人情報の適切な管理のため、アクセス制限の設定、個人情報が記録されている媒体の管理その他の必要な措置を講じなければならない。

２ 乙は、前項の個人情報の管理に当たっては、管理責任者を定め、内部における責任体制を確保しなければならない。

３ 乙は、この契約による業務の従事者に対して、その在職中であると職を退いた後であるとを問わず、業務に関して知り得た個人情報をみだりに他人に知らせ、又は不当な目的に使用してはならないことその他個人情報の保護に関し必要な事項を周知させなければならない。

（派遣労働者等の利用時の措置）

第６ 乙は、この契約による業務を派遣労働者、契約社員その他正社員以外の労働者に行わせる場合は、正社員以外の労働者に、この契約に基づく個人情報の取扱いに関する一切の義務を遵守させるものとする。

２ 乙は、甲に対して、正社員以外の労働者の全ての行為及びその結果について責任を負うものとする。

（複写・複製等の禁止）

第７　乙は、甲の指示又は承認がある場合を除き、この契約による業務を実施するために甲から引き渡された個人情報が記録された資料等の複写、複製、又は持ち出しを行ってはならない。

（再委託の禁止）

第８　乙は、この契約による業務を実施するための個人情報の処理は、自ら行うものとし、甲の承認があるときを除き、第三者にその取扱いを委託（乙の子会社（会社法（平成 17 年法律第 86 号）第２条第１項第３号に規定する子会社をいう。）に委託する場合を含む。）又はこれに類する行為（以下「再委託」という。）をしてはならない。

２　乙は、前項の承認を得て再委託をする場合には、再委託先に対し、甲及び乙と同様の安全管理措置を講じなければならないことを周知するとともに、この契約に基づく個人情報の取扱いに関する一切の義務を遵守させるものとする。

（再委託に係る連帯責任）

第９　乙は、再委託先の行為について、再委託先と連帯してその責任を負うものとする。

（再委託先に対する管理及び監督）

第 10　乙は、再委託をする場合には、再委託をする業務における個人情報の適正な取扱いを確保するため、再委託先に対し適切な管理及び監督をするとともに、甲から求められたときは、その管理及び監督状況を報告しなければならない。

（返還、廃棄又は消去）

第 11　乙は、この契約による業務を実施するために甲から引き渡され、又は乙自らが取得し、若しくは作成した個人情報が記録された資料等について、業務完了後、直ちに甲の指示に基づいて返還、廃棄、又は消去しなければならない。

２　乙は、前項の資料等を廃棄する場合、記録媒体を物理的に破壊する等個人情報が判読、復元できないように確実な方法で廃棄しなければならない。

（遵守状況に関する報告）

第 12　乙は、甲からこの特記事項の遵守状況について報告を求められた場合には、直ちにその状況を甲に報告しなければならない。

（監査等）

第 13　甲は、この契約による業務の実施に伴う個人情報の取扱いについて、この特記事項の規定に基づき必要な措置が講じられているかどうか検証及び確認するため、乙及び再委託先に対して、監査、実地検査又は調査（以下「監査等」という。）を行うことができる。乙及び再委託先は、合理的事由のある場合を除き、甲又は甲の指定した者の行う監査等に協力しなければならない。

２　甲は、前項の目的を達成するため、乙及び再委託先に対して必要な情報を求め、又はこの契約による業務の実施に関して必要な指示をすることができる。

（事故発生時における報告等）

第 14 乙は、この契約による業務に関し個人情報の漏えい、滅失、毀損その他の個人情報の安全の確保に係る事態が発生し、又は発生するおそれのあること（再委託先により発生し、又は発生するおそれがある場合を含む。）を知ったときは、速やかに甲に報告し、甲の指示のもとセキュリティ上の補完、情報の修復等の措置をとるとともに再発防止の措置を講じなければならない。

2 甲は、前項の事態が発生した場合には、個人情報の取扱いの態様、損害の発生状況等を勘案し、乙及び再委託先の名称等の必要な事項を公表することができる。

（契約の解除及び損害の賠償）

第 15 甲は、乙がこの特記事項に定める義務を履行しない場合又は法令に違反した場合には、この契約を解除することができる。

2 乙は、この特記事項に定める義務に違反し、又は怠ったことにより甲又は第三者が損害を被った場合には、その損害を賠償しなければならない。

別紙3

個人情報の適正管理等に関する確認票

住　　所	
事 業 者 名	
受託業務名	
記　入　者	
確認年月日	年　月　日

この確認票は、委託契約書の別記「個人情報取扱特記事項」に記載された事項の遵守状況を確認するものです。
個人情報の適正管理が不十分である場合には、個人情報保護委員会の「個人情報の保護に関する法律についてのガイドライン（通則編）」（https://www.ppc.go.jp/personalinfo/legal/）などを参考に、早急に対応していただく必要があります。

1　「個人情報取扱特記事項」の遵守について

下記各条項の遵守について確認を行い、確認を行ったものはチェック（☑）してください。

□基本的事項　□秘密の保持　□取得の制限　□目的外利用及び提供の禁止　□派遣労働者当の利用時の措置　□複写・複製等の禁止
□再委託の禁止　□再委託に係る連帯責任　□再委託の相手方に対する管理及び監督　□返還、廃棄又は消去　□遵守状況に関する報告
□監査等　□事故発生時における報告

＊派遣労働者等の利用がない場合、再委託がない場合など該当がない場合は■にしてください。

＊遵守状況が不十分又は遵守されていないものについては、早急に改善又は代替措置等を行ってください。

2　適正管理（特記事項第5）について

＊個人情報の適正管理に関する具体的な対応状況を記載してください。

※評価欄……適切に対応されているものは〇、対応されているが不十分であるものは△、対応できていないものは×

＊必要な対応がなされていないもの(評価×)又は対応不十分であるもの(評価△)については、早急に改善又は代替措置等を行ってください。

区分	個人情報の適切な管理のために必要な措置の類型	具体的な措置の確認例	具体的な対応	評価
組織的安全管理措置	個人情報を適切に管理するための組織及び規程の整備	個人情報の取扱いに関する組織・規程を整備していますか		
		個人情報の取扱いに関する規程等に基づいて、個人情報の管理責任者を適切に指名していますか		
		個人情報の取扱いに関する規程等に従った運用をしていますか		
		個人情報の漏えい等の事故発生時の連絡・報告の体制を整備していますか		
	その他の管理的保護措置	個人情報の移送・送信の際の手続きが定められ、遵守していますか		
		報告徴収・監査・検査についての定めがあり、実行していますか		
		決められた手順の遵守についての定期的な確認等、従業員の監督を適切に行っていますか		
人的安全管理措置	従業員の意識啓発・研修	個人情報の保護に関する従業員の意識啓発のための教育・研修を行っていますか		
物理的安全管理措置	個人情報を管理している施設への第三者の立入制限等	個人情報を管理している施設を特定し、当該施設への立入制限、当該施設からの個人情報の持出禁止を実施していますか		
	施設及び設備の整備	個人情報を管理している施設の入退室管理を行うための鍵の設置や、機器・装置の物理的な保護等を適切に行っていますか		
	その他の物理的な保護措置	個人情報が記録された媒体について、盗難、漏えい、改ざん防止について適切な管理をしていますか		
		委託者の指示・許可を得て、個人情報が記録された資料等を持ち出す場合、漏えい等の防止を行っていますか。		
		委託者の指示により、個人情報を廃棄する場合、復元不可能な方法で行っていますか。		
		出力装置及び印刷について、出力（印刷）したものを放置することのないよう教育・訓練をしていますか		
技術的安全管理措置	ユーザーID、パスワードなどによるアクセス制限	ユーザーID、パスワード等によるアクセス制限を行っていますか		
	その他の技術的保護措置	外部からの不正アクセス等を防止するための対策を実施していますか		
		ログ等により不正アクセスを監視しており、それを責任者が確認していますか		

山口県情報セキュリティポリシー

令和８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。

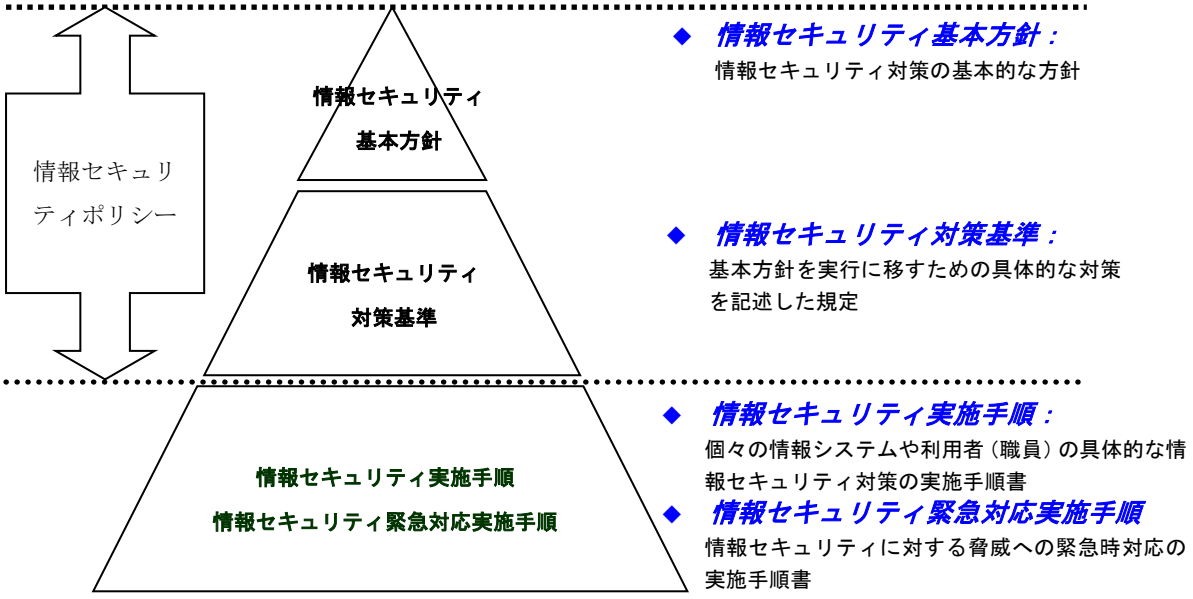
本県においても、令和３年３月に策定した「やまぐちデジタル改革基本方針」に基づき様々な取組を進めてきたところであるが、令和４年12月に策定した新たな県の総合計画「やまぐち未来維新プラン」や、国の「デジタル田園都市国家構想」の基本方針・総合戦略、県議会「人にやさしいデジタル社会実現特別委員会」の調査報告書に基づく要請等を的確に反映するとともに、これまでの取組成果やCIO補佐官から得た知見等を踏まえ、取組内容の拡充等を図るため、令和５年３月に本方針の改訂を行い、①『やまぐちＤＸ』の創出、②『デジタル・ガバメントやまぐち』の構築、③『デジタル・エリアやまぐち』の形成の３つの柱に沿って、デジタルの力を活用した取組の更なる強化・拡充を図っ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、情報資産の機密性、完全性及び可用性を維持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。

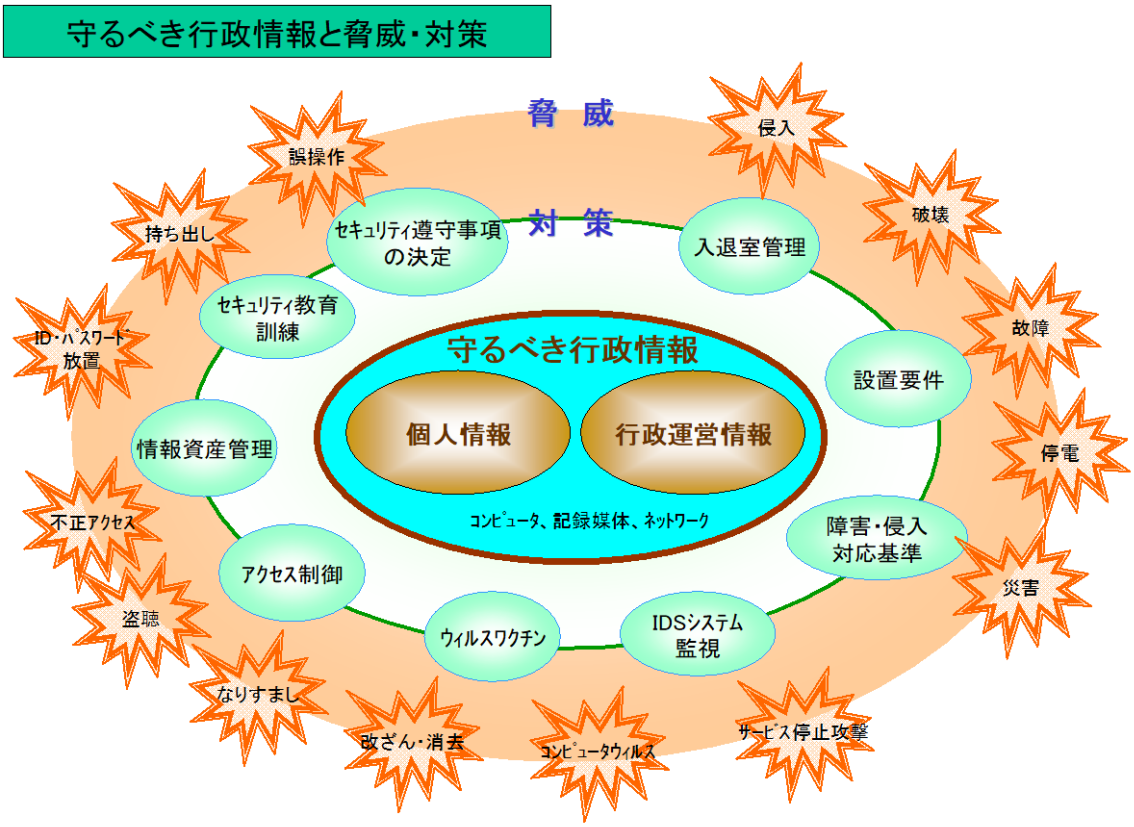
（１）　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（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、行政組織規則（昭和４３年山口県規則第１５号)第３条に規定する本庁及び出先機関並びに企業局､議会事務局、監査委員事務局、労働委員会事務局、人事委員会事務局、選挙管理委員会事務局及び教育庁（ただし、県立学校等を除く。）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）　業務委託とクラウドサービスの利用

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。

クラウド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

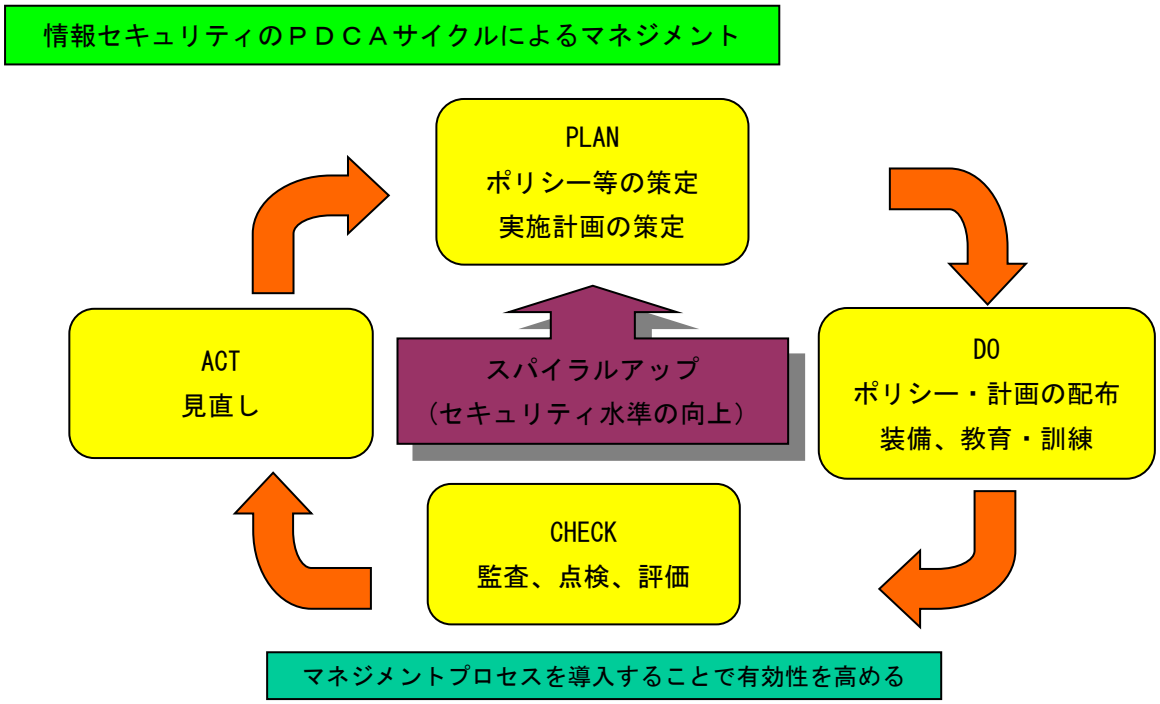
情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、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） クラウドサービス管理者

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

② クラウド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。

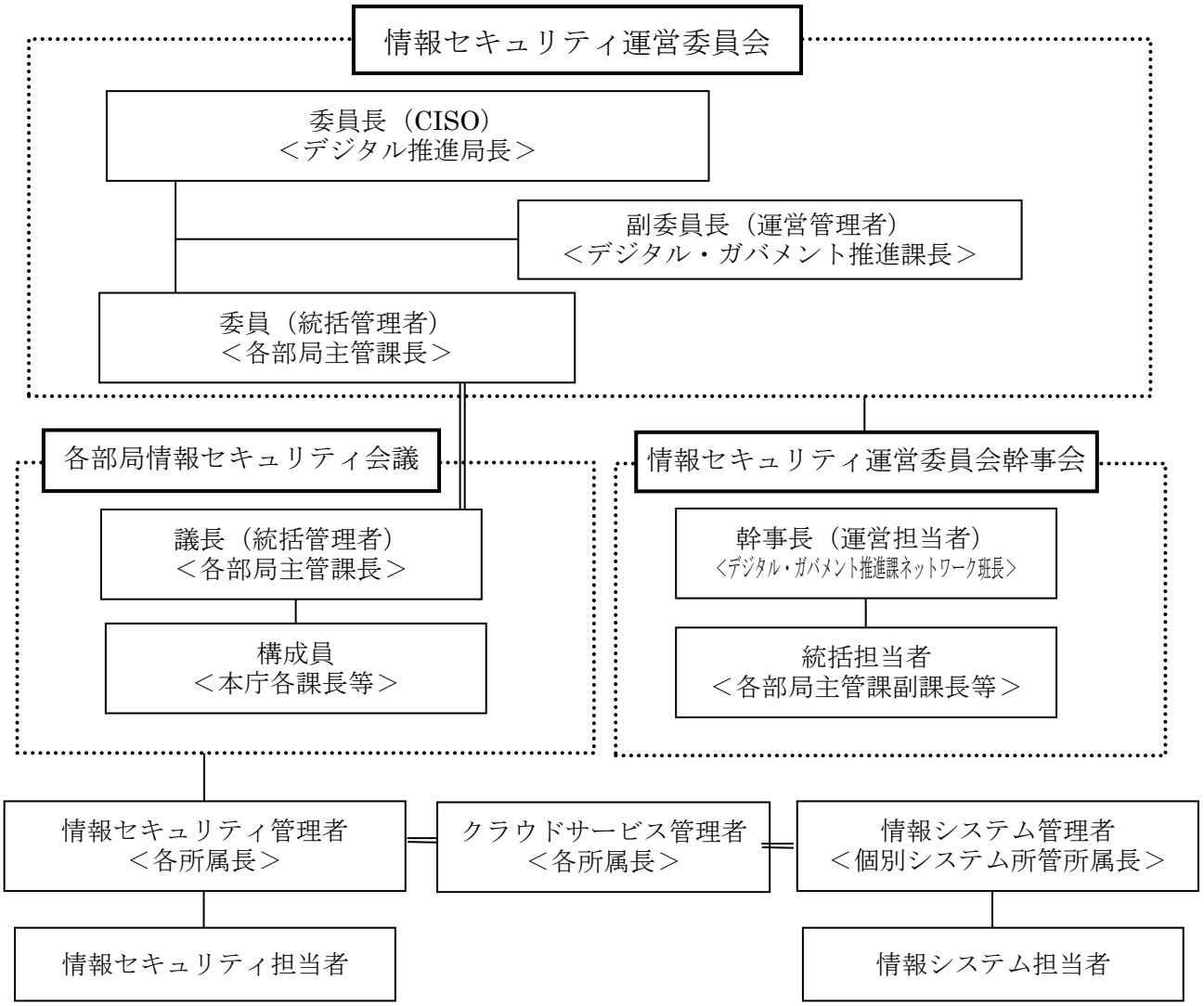
③ 緊急対応チームの運営は、「情報セキュリティ緊急対応実施手順」に従うものとする。

（１７）クラウドサービス利用における組織体制

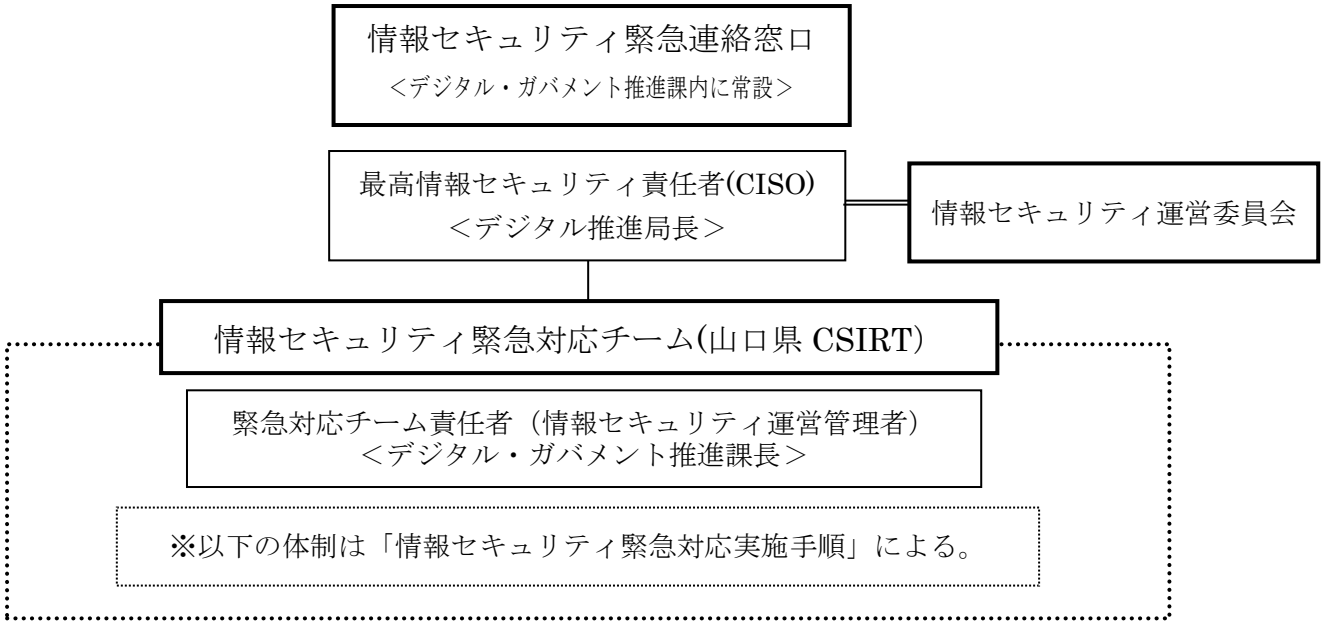
① クラウドサービス管理者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

＜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）　情報資産の分類

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情報資産については情報システム管理者をいう。以下同じ。）は、情報資産について、機密性、完全性及び可用性により、次のとおり分類するものとする。

＜機密性による情報資産の分類＞

分類	分類基準	参考例
自治体機密性３A	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」(平成 23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書	極秘文書、秘文書等
自治体機密性３B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	データベースや台帳形式になった県民情報を含む個人情報ファイル及びこれに準ずる情報等 （県民記録システム、税務システム、生活保護システム、貸付金償還システム等に保存される県民の個人情報等）
自治体機密性３C	行政事務で取り扱う情報資産のうち、自治体機密性３B 以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	・職員としての属性に基づく個人情報等 ・オンライン申請の処理等により、システム処理上一時的にインターネット上に保管されるデータ等 ・文書管理システムの決裁文書として保存されている個人情報等 ・施設設計情報や入札予定価格など非公開情報等
自治体機密性２	行政事務で取り扱う情報資産のうち、自治体機密性３に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	政策検討に関する情報等
自治体機密性１	自治体機密性２又は自治体機密性３の情報資産以外の情報資産	・将来公表する予定の文書等(白書の案等) ・公表された情報等

※「重要な情報資産」は、自治体機密性３の情報資産をいう。また、別途、情報セキュリティ管理者が重要な情報資産と指定した情報。

＜完全性による情報資産の分類＞

分類	分類基準
自治体完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産
自治体完全性１	自治体完全性２の情報資産以外の情報資産

＜可用性による情報資産の分類＞

分類	分類基準
自治体可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、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（軽微なものを除く。）を及ぼすおそれがある情報資産
自治体可用性１	自治体可用性２の情報資産以外の情報資産

② 分類に当たっては、個人情報の保護に関する法律、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。

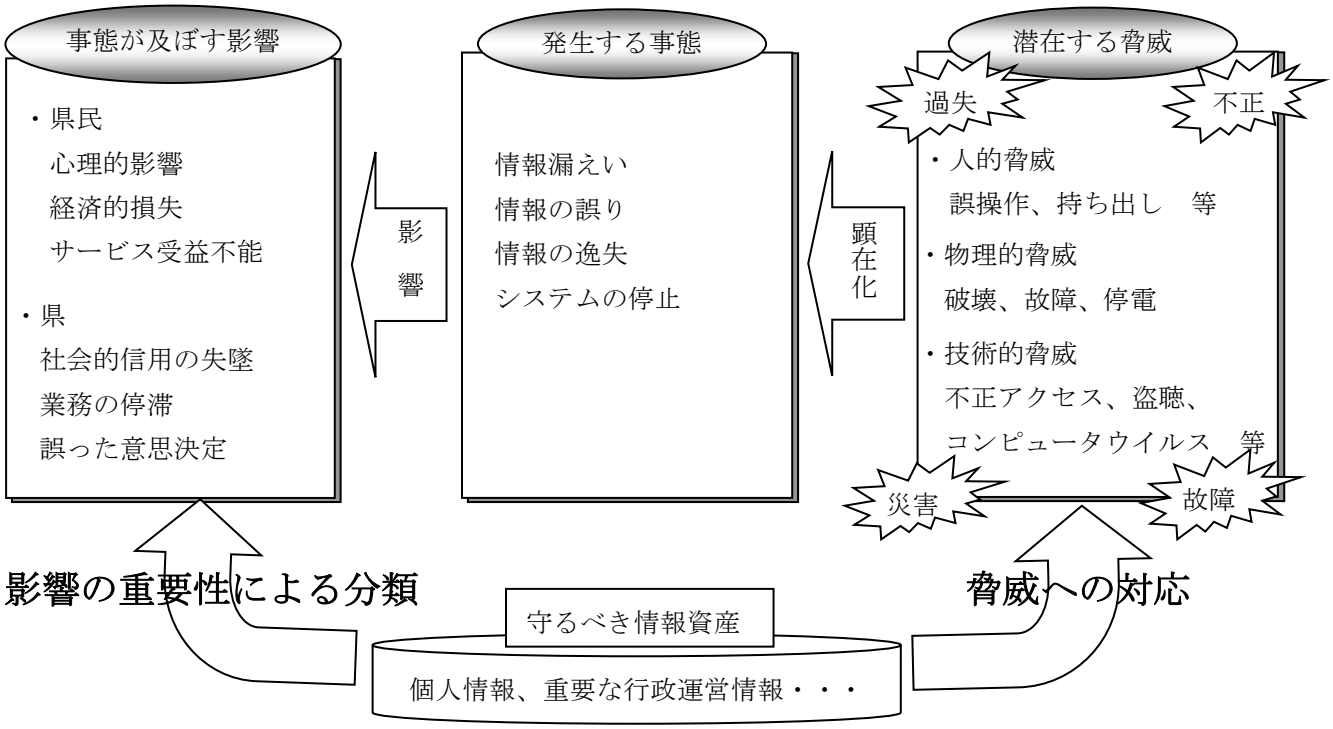
（イ）情報システム管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

（ウ）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、当該行政情報を分類し､必要に応じて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、自治体機密性２以上、自治体完全性２又は自治体可用性２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自治体機密性２以上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）車両等により自治体機密性２以上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）自治体機密性２以上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）自治体機密性２以上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）自治体機密性２以上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又は、情報資産の破棄やリース返却等を行う者は、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。

③ マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本県の他の領域とはネットワークを分離しなければならない。

④ マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

（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

② LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域を LGWAN 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

（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、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、重要な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、自治体可用性２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

① 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。

② クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。なお、当該確認にあたっ

ては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

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、自治体機密性２以上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、保守のため自治体機密性２以上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、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。

③ 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。

④ 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。

⑤ 運営管理者は、自治体機密性２以上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。

⑥ 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、不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。

⑦ 運営管理者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。

⑧ 運営管理者は、自治体可用性２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、取り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 及び情報セキュリティ管理者は、自治体機密性２以上、自治体可用性２、自治体完全性２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、本県の情報資産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。

⑨ クラウドサービス利用時等の遵守事項

職員等は、クラウドサービスの利用にあたっても情報セキュリティポリシーを遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

（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

① 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 CISO は、定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施するとともに、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認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

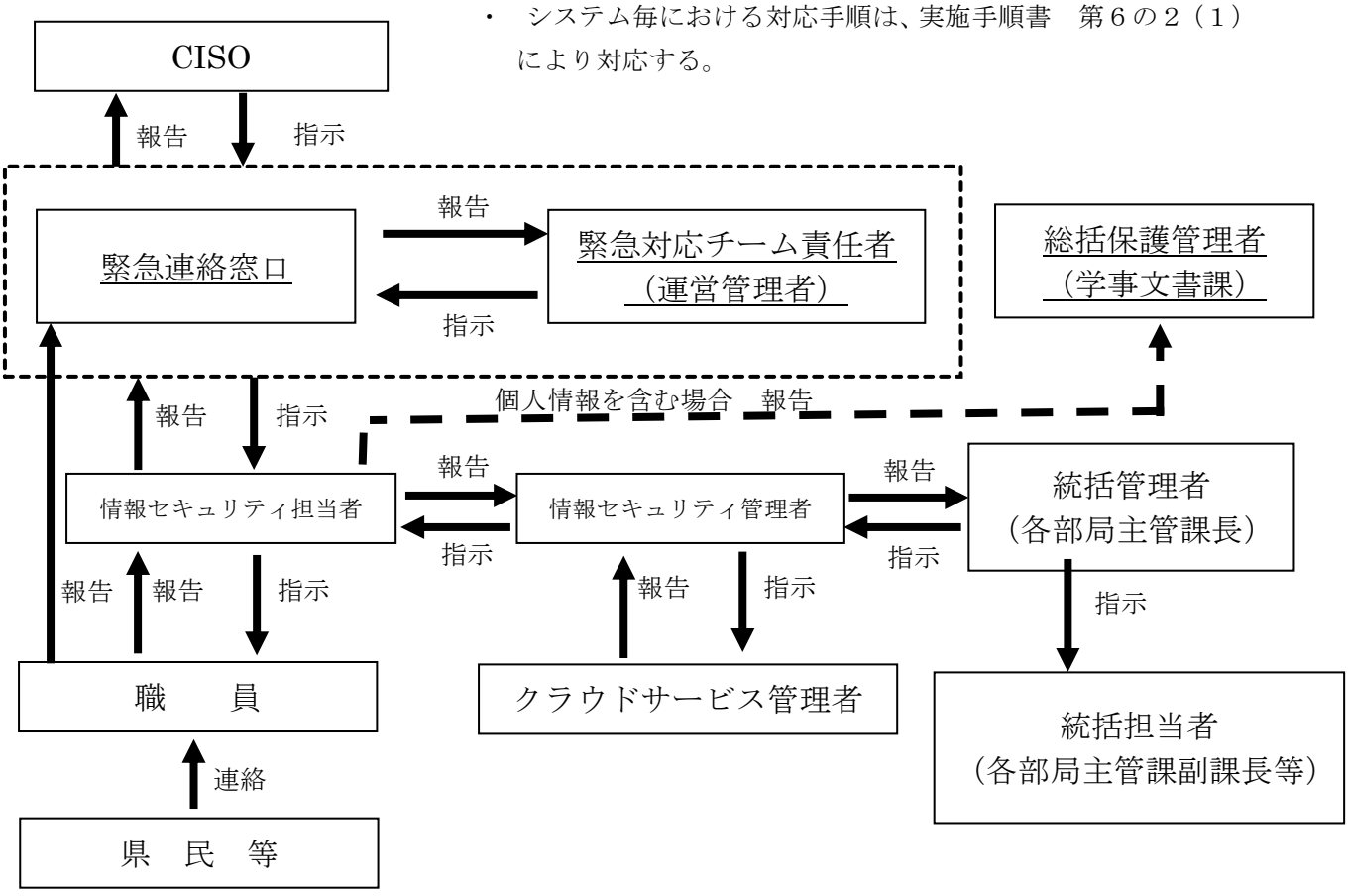
① 職員等は、情報セキュリティインシデントを発見又は県民等外部から連絡を受けた場合には、速やかに情報セキュリティ担当者及び緊急連絡窓口に報告し、指示を仰がなければならない。

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、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。
⑤ 情報セキュリティインシデントにより個人情報・特定個人情報の漏えい等が発生した場合は、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に基づき、必要に応じて個人情報保護委員会へ報告しなければならない。
⑥ 情報セキュリティ管理者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告しなければならない

＜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 運営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ることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。

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

①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かかわらず、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。

②運営管理者及び情報システム管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得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、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

④ 運営管理者、情報システム管理者及びクラウドサービス管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その機能の仕様が本県の求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

（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、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。

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、記録媒体にかか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。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

④ 運営管理者及び情報システム管理者は、監査及びデジタルフォレンジックに必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確に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。

③ 運営管理者は、保守又は、診断のために、外部の通信回線からな部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保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、定期的な確認により見直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、次のセキュリティ対策を実施しなければならない。

（ア）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。

（イ）脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。

（ウ）ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。

（エ）情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定しなければならない。

（オ）インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じるよう努めるものとする。

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。

⑨ 仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報告を求めなければならない。

（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、運営管理者及び情報システム管理者の了承なく、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）を取り扱ってはならない。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（運営管理者が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、外部から Web 会議に招待される場合、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、必要最小限の範囲で適切に設定する等、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。

（オ）運営管理者及びシステム管理者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。

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）運営管理者及び情報システム管理者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するため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。

（エ）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等に通知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 及びパスワードに

ついて、人事異動の際のパスワードの変更、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。

（カ）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）　自動識別の設定

運営管理者又は情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

（４）　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。

（５） 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） 機器等の調達に係る運用規程の整備

① 運営管理者及び情報システム管理者は、機器等の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策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、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。

（２） 機器等及び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。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載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、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。

（３） 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、それ以外のものを利用させてはならない。

（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。

④ アプリケーション・コンテンツの開発時の対策

情報システム管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

（４） 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。重要な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。

（オ）情報システム管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

③ 機器等の納入時又は情報システムの受入れ時

（ア）情報システム管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければなら

ない。

（イ）情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

（５）　情報システムの基盤を管理又は制御するソフトウェア導入時の対策

① 情報システム管理者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置に努めらければならない。

② 利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備しなければならない。

（ア）情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順。

（イ）情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順。

（６）　情報システムの基盤を管理又は制御するソフトウェア運用時の対策

① 情報システム管理者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策に努められなければならない。

（ア）情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策。

（イ）脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策。

② 情報システム管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

（７）　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。

（ア）情報システム管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について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。

（イ）情報システム管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む情報システム関連文書を整備しなければならない。

・情報システムを構成するサーバ装置及び端末関連情報

・情報システムを構成する通信回線及び通信回線装置関連情報

（ウ）情報システム管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整

備しなければならない。
・情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順
・情報セキュリティインシデントを認知した際の対処手順
・情報システムが停止した際の復旧手順

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適正な方法で保管しなければならない。

（８） 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、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

（ア）利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直ししなければならない。

（イ）運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。

（ウ）ウェブアプリケーションやウェブコンテンツにおいて、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。

（９） 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。

（１０） 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。

（１１） 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。

（１２）　情報システムについての対策の見直し

情報システム管理者は、監査や自己点検の結果等に合わせ、情報セキュリティ対策を適切に見直さなければならない。また、横断的に改善が必要となる情報セキュリティ対策が確認された場合は、情報セキュリティ対策を適切に見直さなければならない。なお、措置の結果については、運営管理者へ報告しなければならない。

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、情報セキュリティ管理者等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 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 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。
④ 本県が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。
⑤ クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。
⑥ パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、本県が定めたクラウドサービスの利用に関するポリシー(情報セキュリティポリシー)を満たすことを確認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

① 情報セキュリティ管理者等は、サーバ装置、端末及び通信回線装置等における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 運営管理者及び情報システム管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本県の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認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）　情報システムの運用・保守時の対策

① 運営管理者及び情報システム管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用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、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

③ 運営管理者及び情報システム管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

（２）　情報システムの監視機能

① 運営管理者及び情報システム管理者は、情報システム運用時の監視に係る運

用管理機能要件を策定し、監視機能を実装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、情報システムの運用において、情報システムに実装された監視機能を適切に運用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、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。
④ 運営管理者及び情報システム管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

（3） 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。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認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。
⑤ 運営管理者及び情報システム管理者は、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。
⑥ 運営管理者及び情報システム管理者は、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討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、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。
（ア）サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除
（イ）クラウドサービス利用の終了手順
（ウ）バックアップ及び復旧

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

① 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 CISO 又は情報セキュリティ委員会は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した緊急時対応計画を定めておき、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

（１）　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 26 年法律第 104 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）

（２）　運営管理者及び情報システム管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があ

るため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

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　業務委託とクラウドサービスの利用

８．１　業務委託

（１）　委託事業者の選定及び判断基準

① 自治体機密性３を取り扱う場合は、知事が保有する個人情報に関しては、「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」に基づき、委託事業者の選定及び判断を行うこと。

② 上記情報以外の情報を取り扱う場合は、自治体機密性等を参考に必要に応じて第三者認証を求めること。

（２）　業務委託実施前の対策

① 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

（ア）委託する業務内容の特定

（イ）委託事業者の選定条件を含む仕様の策定

（ウ）仕様に基づく委託事業者の選定

（エ）情報セキュリティ要件を明記した契約の締結（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等に係る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
・個人情報漏えい防止のための技術的安全管理措置に関する取り決め
・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）

（オ）委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結

② 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

（ア）仕様に準拠した提案
（イ）契約の締結
（ウ）委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結

（３）　業務委託実施期間中の対策

① 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施機関において、以下を全て含む事項を実施しなければならない。

（ア）委託判断基準に従った重要情報の提供
（イ）契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施
（ウ）運営管理者への措置内容の報告（重要度に応じてCISOに報告）
（エ）委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

② 情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。

（ア）情報の適正な取扱いのための情報セキュリティ対策
（イ）契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告

（ウ）委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

（４）　業務委託終了時の対策

① 情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。

（ア）業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収

（イ）委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

② 情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。

（ア）業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検

（イ）提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

８．２　情報システムに関する業務委託

（１）　情報システムに関する業務委託における共通的対策

情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに本県の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

（２）　情報システムの構築を業務委託する場合の対策

情報システム管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。

① 情報システムのセキュリティ要件の適切な実装

② 情報セキュリティの観点に基づく試験の実施

③ 情報システムの開発環境及び開発工程における情報セキュリティ対策

（３）　情報システムの運用・保守を業務委託する場合の対策

① 情報システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

② 情報システム管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

（４）　本県向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

① 情報セキュリティ管理者等は、外部の一般の者が本県向けに重要情報を取り

扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。

② 情報セキュリティ管理者等は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。

③ 情報セキュリティ管理者等は、委託事業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しなければならない。

④ 情報セキュリティ管理者等は業務委託サービスを利用する場合には、運営管理者へ当該サービスの利用を届け出なければならない。

⑤ 運営管理者及び情報セキュリティ管理者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。

⑥ 運営管理者及び情報セキュリティ管理者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。

（５） 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。

８．３ クラウド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クラウドサービスの利用に関する規程に従ってクラウドサービス利用の検討及び許可を得なければならない。

８．４ クラウドサービスの利用（自治体機密性２以上の情報を取扱う場合）

（１） クラウド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、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウド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、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウド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） クラウド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、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービス（自治体機密性２以上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 クラウドサービス管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。なお、情報システム台帳に記録又は記載した場合は、運営管理者へ報告しなければならない。

③ クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。

（ア）クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

（イ）クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

（ウ）利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

④ クラウドサービス管理者は、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） クラウド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、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービス（自治体機密性２以上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 クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正しなければならない。なお、情報システム台帳を更新又は修正した場合は、運営管理者へ報告しなければならない。

③ クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な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は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウド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。

⑤ クラウドサービス管理者は、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） クラウド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、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービス（自治体機密性２以上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 クラウドサービス管理者は、前項において定める規定に対し、クラウド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。

③ クラウドサービス管理者は、クラウドサービス上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態と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

① 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。

② クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査を行わなければならない。クラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

（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

① 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（改善計画の策定等）を指示しなければならない。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

② CISO は、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（改善計画の策定等）を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告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リスク評価を行い、必要があると認めた場合、改善を行うものとする。なお、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内部の職制及び職務に応じた措置の実施又は指示し、措置の結果についてCISO に報告しなければならない。

（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。

附　則
この情報セキュリティポリシーは、令和７年４月１日から施行する。

附　則
この情報セキュリティ対策基準は、令和８年４月１日から施行する。