業務仕様書

１　業務の名称

「山口県県民活動スーパーネット」及び「やまぐち社会貢献活動支援ネット　あいかさねっと」に係る再構築・保守運用管理業務

２　目的

○「山口県県民活動スーパーネット（以下、「スーパーネット」という。）」及び「やまぐち社会貢献活動支援ネット　あいかさねっと（以下、「あいかさねっと」という。）」は、県民や県民活動団体等を主な利用対象とし、団体・企業情報やイベント・講座等の募集情報、助成情報のほか、ボランティア情報など、県民活動に関する各種情報を一元的に提供している。年間アクセス数は 20 万件超。

○現在のシステム（※）は平成 30 年度に構築し、令和６年度にシステムサーバーの移転を行った。今後、現事業者による保守管理が困難になることから、継続してサービスを提供するため、他事業者によるシステムの再構築を行い、セキュリティ強化を図るとともに、ウェブアクセシビリティ対応を実施し、サービスの利便性向上を図る。

※現在のシステム概要

プログラミング言語	PHP version8.3
OS	AlmaLinux 9

３　委託期間

契約締結の日から令和８年３月３１日まで

※再構築に係る業務は契約締結の日から６か月を目途に完了させ、再構築後、委託期間の末日まで保守運用管理に係る業務を行うものとする。

４　業務内容

(1)「スーパーネット」及び「あいかさねっと」の再構築

○現在公開しているウェブサイト及びシステムを再構築して公開すること。なお、各ウェブサイトの概要について「スーパーネット」は別紙１、「あいかさねっと」は別紙２を参照。

「スーパーネット」トップページ：https://www.kenmin.pref.yamaguchi.lg.jp/

「あいかさねっと」トップページ：https://www.kenmin.pref.yamaguchi.lg.jp/boranet201909/

○ウェブサイトの構築及び管理運用にはコンテンツ管理システム(CMS)を利用すること。

○Web サーバ等、本システムの構築に当たり、クラウドサービスを利用する場合においては、「ISMAP クラウドサービスリスト」掲載のサービスを利用すること。

○再構築と運用に当たっては「山口県情報セキュリティポリシー」を遵守すること。

○UI、UX に配慮したウェブサイトのデザインを提案する。ただし、現状の機能は踏襲した上で、サイト利用者、管理者が使いやすいサイトの提案、構築を実施すること。

○事前に委託者及びウェブサイトの管理運営を行う「やまぐち県民活動支援センター（以下、「センター」という。）」と協議し、不要な項目の削除、誤字の修正、掲載画像のセンター提供データへの差し替え等、委託者及びセンターの要望を、再構築時

に反映させるよう努めること。

○現在のシステムに登録されている団体、企業及び個人等の登録会員に係る初期データならびに過去も含めたボランティア募集データ・メルマガメンバーについて、再構築後のシステムに登録すること。なお、団体、企業及び個人がシステムに登録する際の入力項目について「スーパーネット」は別紙３、「あいかさねっと」は別紙４を参照。

○現在のシステムに登録されているデータ、並びに現在のウェブサイトに掲載されている内容については、別途委託者から提供する。なお、データはCSVファイル及びSQLファイルによる提供を想定している点に留意すること。

○「スーパーネット」と「あいかさねっと」の連携機能についても、現状の機能を踏襲した上で、必要に応じて、よりシステム利用者の利便性向上に向けた改善を提案、実装すること。

※「連携機能」の概要
①一方のシステムへ新規登録した際に、もう一方への登録を促す画面が表示される
②同意することで、もう一方のシステムへの登録ページへ遷移する
③遷移後のページには、先の登録時に入力した情報が自動的に反映される

○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。

○管理画面以外について、デザインをレスポンシブなものとし、PCやスマートフォン、タブレットなど、端末の画面サイズを問わず、最適に表示されるよう構築すること。

○Googleアクセス解析をそれぞれ設置し、センターで確認できるようにすること。また、必要に応じて更新すること。

○ドメイン(kenmin.pref.yamaguchi.lg.jp)及びドメインメール(@kenmin.pref.yamaguchi.lg.jp)については、現状のまま移行すること。

(2)「スーパーネット」及び「あいかさねっと」の保守運用管理

○「スーパーネット」及び「あいかさねっと」の保守運用管理に必要な業務を行うこと。
・システムの保守及び運用管理に係るソフトウェア整備
・サーバーの維持管理
・独自ドメインの管理（廃止する場合は廃止後３年間のドメイン維持管理）
・ウェブサイトデザイン、レイアウト等の調整及び修正
・常時SSL化対応などによるセキュリティ確保
・日常的な管理及びメンテナンス
・データのバックアップ（１日１回以上）
・緊急時における復旧作業
・委託者による「スーパーネット」及び「あいかさねっと」利用状況調査への回答
・その他、センター職員によるシステム運用のサポート等

なお、これに必要となる端末等の機器は受託者負担により整備するとともに、当該端末をもって、受託者の責任により情報管理等を行うこと。

○ウェブサイト（トップページ）には現在、年間約20万件のアクセス数があるため、再構築後、同程度のアクセスに対して滞りなく情報発信できるよう対応すること。

○センターの職員を対象としたマニュアルを作成し、ウェブサイトの更新やドメインメールの設定等について職員が自ら利用できるような支援を実施すること。また、当該マニュアルは作成・更新の都度、委託者に共有すること。

○再構築後、速やかに、センターの職員を対象とした運用操作研修（ハンズオン）を実施すること。

○再構築時に受託者、委託者及びセンターで確認した仕様と異なる仕様が実装されていた場合、並びに必要な仕様が満たされていなかった場合、速やかに修正又は追加の実装を行うこと。

○センター及び委託者から、システムの操作説明やシステム障害の復旧要請を受けた場合は、速やかに対応すること。

５　付帯事項

⑴ セキュリティ対策

○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。

○山口県情報セキュリティポリシーに準拠した対応を行うこと。

○山口県情報セキュリティポリシーに準じた対応ができるよう環境を整えること。

○ホームページへの不正アクセス防止、データ改ざん防止、個人情報の保護等に必要なセキュリティ対策をとること。

○県が実施する情報セキュリティ監査（検証用ネットワークに検証用パソコンを接続し、インターネット経由で検証ツールによる Web アプリケーションの脆弱性の有無を確認するもの）への協力を行うこと。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。

⑵ 誤登録の防止

受託者が情報更新する際、誤入力・誤登録を防止する対策をとること。

⑶ 緊急時の対応

緊急時の対応のため、受託者に担当者を置き、受託者が速やかに対応すること。

⑷ その他

○本システムに安定稼働の観点から改善すべき点を発見した場合は、速やかに委託者に連絡の上、プログラムの修正作業を行うこと。

○本システムに係るドキュメントに変更すべき点がある場合は、必要な加筆修正を行い、変更後のドキュメントを提出すること。

○毎月１回、システムの保守点検を行うこと。

○本システムに異常を察知した場合は、速やかに委託者へ報告するとともに、初期措置を講ずること。

○システムダウン時は、特別の理由がない限り、連絡を受けてから 24 時間以内に復旧させること。

○ホームページの運用の保全を図るため、データのバックアップを実施すること。

○ホームページのアクセス数、登録者一覧、掲載情報等について、データ管理・分析ができるものとする。

６　知的財産権等

業務の成果物の所有権、著作権及びその他の権利は、委託者に帰属する。
ただし、受託者はあらかじめ、委託者の許諾を得た場合には、開発業務の成果物を基に翻案して二次的著作権を制作し、譲渡、貸与等をすることができる。

７　事故等の処理

受託者は、事故などが発生した場合及びその他異常があった場合は委託者へ遅滞なく通報し、その指示に従い、その都度事故報告書を作成し、提出すること。

８　損害の負担

受託者の行った業務により生じた損害は、受託者の負担とする。ただし、その損害の発生が委託者の責めに帰すべき理由による場合は、この限りではない。

９　諸費用の負担

業務において必要な器具、資材、消耗品等に係る費用は、受託者の負担とする。

10　成果物

(1)システム概要
(2)基本設計書
(3)詳細設計書
(4)運用・操作マニュアル
(5)緊急時対応マニュアル
(6)プログラムソフト一式（電子媒体によるもの）
(7)業務完了報告書

成果物の納入期日は、(1)システム概要～(5)緊急時対応マニュアルはウェブサイト稼働予定日までに、(6)プログラムソフト一式（電子媒体によるもの）及び(7)業務完了報告書は令和８年３月３１日までに提出すること。

11　委託条件

(1)実施体制等

受託者は業務責任者、連絡担当者及び業務従事者を定め、契約締結後、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。

⑵ 実施計画書

受託者は、契約締結の日から起算して 10 営業日以内に、実施方法を取りまとめた業務実施計画書（任意様式）を作成し、委託者の了解を得ること。

⑶ 委託料の支払等

①業務履行のための受託者の人件費、旅費、通信費、印刷製本費及び契約費用の一切の経費は、委託料に含まれるものとする。

②受託者は、委託料の５割（千円未満の端数があるときは、その端数を切り捨てた額）を超えない範囲で前払金を請求することができる。

⑷ 経理処理

受託者は本業務に係る経理処理について、ほかの経理と明確に区分した会計帳簿を備えるとともに、収入額及び支出額を記載し、経費の使途を明らかにすること。

また、その支出の内容を証する書類を整備し、会計帳簿とともに業務の完了した日の属する会計年度の終了後５年間保存すること。

⑸ 秘密の保持

業務の履行に関して知り得た相手方固有の秘密情報を第三者に漏らしてはならない。

⑹ 個人情報の保護

業務の履行に伴う個人情報の取扱いについては、別記３「個人情報取扱特記事項」を遵守することとし、特記事項の遵守状況を「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。

⑺ 業務の再委託

受託者は、本業務の全部又は一部を第三者へ再委託することはできない。ただし、知事が適当と認めた場合は、この限りではない。

⑻ その他

①業務の実施に当たり、本仕様書に不都合、変更、追加が発生した場合には、双方協議の上、誠意を持って対応する。

②仕様書に定めがない事項や、その他細部についての必要な事項は、指示するところによる。

別紙１

「山口県県民活動スーパーネット」の概要

１　「山口県県民活動スーパーネット」について

（１）概　要

県民や県民活動団体などを主な対象として、団体情報やイベント・募集情報、助成情報など、県民活動に関する各種情報を一元的に提供する、県内最大の県民活動情報サイト（平成１４年度 運用開始）

※やまぐち県民活動支援センターにおいて管理・運営（指定管理業務）

（２）登録者数

時　点	任意団体	NPO 法人	企　業	合　計
令和 7 年 2 月末	603 件	221 件	28 件	852 件

（３）ホームページアクセス数（令和７年２月末）

「山口県県民活動スーパーネット」アクセス数：191,228

→うち「あいかさねっと」アクセス数： 67,351

２　構　成

タブ表示（位置）	掲載項目
HOME（上部）	○お知らせ：センターの利用について ○団体情報 ○募集情報（直近掲載情報３件） ○助成金情報（直近掲載情報３件） ○印刷機・交流コーナー（Zoom ルーム）予約状況カレンダー ○センターからのお知らせ ＜下部のバナー＞ ○スーパーネットについて ○センターからのお知らせ（過去掲載情報） ※現データ件数：133 ○お知らせ（過去掲載情報） ※現データ件数：249 ○蔵書情報 書籍名、著者・編集者、内容説明、発行所、発行日、受付番号 ※現データ件数：3,101 ○さぽ～とメール（過去掲載情報） ※現データ件数：397

別紙１

タブ表示（位置）	掲載項目
HOME（上部）	○掲載登録 【掲載登録】 ・企業・団体情報 →ＮＰＯ法人・県民活動団体・企業別の登録案内ページへ →登録フォームのリンクあり ・募集情報 イベント・講座・参加その他（作品・意見等）募集の掲載方法 →登録フォームのリンクあり ・活動実績・事例情報 ・助成情報 【修正依頼】 ・企業・団体情報 →団体・企業情報修正の検索フォームへ ○あいかさねっと ※「あいかさねっと」（外部リンク）へ ○センターのブログ ※やまぐち県民活動支援センター便りのページへ ○探す ※キーワード検索機能 ・団体・企業を探す ・助成を探す ・活動実績・事例を探す ・蔵書を探す ・お知らせを探す ・センターからのお知らせを探す ○相談する ・相談窓口（一覧掲載） ・関連団体リンク（一覧掲載） ○やまぐち県民活動支援センター ※以下のページへ ・センターの概要 ・センターの事業 ・利用の手引き ・アクセス ・申し込み・予約 ・情報収集・提供 ○サイトマップ ○情報登録規約・個人情報保護方針 ○お問い合わせ

別紙１

タブ表示（位置）	掲載項目
団体・企業を探す（上部）	【県民活動団体情報】 団体名、組織形態、分野、対象エリア、活動内容、代表者、代表者役職、担当者名、主たる事務所、住所、電話番号、メールアドレス、設立年月日・発足年月日、会員数、会費、会員資格、広報、活動目的、特徴 ※現データ件数：スーパーネット登録 1,010 【ＮＰＯ法人情報】 団体名、組織形態、分野、対象エリア、活動内容、代表者、代表者役職、担当者名、主たる事務所、住所、電話番号、メールアドレス、設立年月日・発足年月日、会員数、会費、会員資格、広報、活動目的、特徴 ※現データ件数：スーパーネット登録 270 【企業情報】 組織形態、事業内容、CSR の取り組み、社会貢献活動等の概要、ひとこと PR、代表者名、住所、電話番号、FAX、設立年月日・発足年月日、参考 URL、特徴 ※現データ件数：スーパーネット登録 76 スーパーネット登録以外も含めて全登録件数は１，６77
イベント・募集を探す（上部）	主催者、タイトル、開催日時、開催場所、事業の主旨、内容、分野、参加料・入場料、対象者、募集期間、申込み・応募方法、問い合わせ先団体情報、共催・後援など、参考 URL、参考資料 ※現データ件数：5,827
ボランティア（上部）	※「あいかさねっと」（外部リンク）
活動実績・事例を探す（上部）	タイトル、内容、団体名、団体名ふりがな、開催日、開催時間、開催場所、人数、関連団体、写真、参考 URL ※現データ件数：95
助成を探す（上部）	※募集締め切りカレンダーを表示 募集団体、助成名、対象分野、対象エリア、助成の目的、助成金額、対象事業、対象者、募集期間、申込み・応募方法、問い合わせ先団体情報（問い合わせ先団体名、郵便番号、住所、電話番号、FAX、メールアドレス）、参考 URL ※現データ件数：8,552
やまぐち県民活動支援センター（右横）	※「やまぐち県民活動支援センター」のページへ
企業のみなさまへ（右横）	※「企業情報の掲載について」のページへ
団体登録・修正（右横）	※「NPO 法人・県民活動団体情報の掲載のご案内」ページへ
Facebook（右横）	※Facebook のサイトへ（外部リンク）

別紙１

３　登録者入力事項

・団体、企業別の登録項目は別紙３のとおり
・登録前に「山口県県民活動スーパーネット登録規約」を表示させ、「同意する」場合に登録フォームに進めるようにすること。

別紙２

「やまぐち社会貢献活動支援ネット　あいかさねっと」の概要

１　「やまぐち社会貢献活動支援ネット　あいかさねっと」について

（１）概　要

ボランティアをしたい個人・団体・事業者（企業）とボランティアしてほしい団体をつなぐマッチングサイト（平成２７年１１月～運用開始）

※県内には福祉や国際交流など、分野ごとにボランティアの募集を行っているものはあるが、県域で分野を限定せず一元的にボランティア等の情報をインターネットにより提供するものは、本県では初めての取組
※やまぐち県民活動支援センターにおいて管理・運営（指定管理業務）

（２）目　的

県民が、地域づくり活動などに積極的に参加し、県内各地で活躍していただくとともに、人材不足という課題を抱える県民活動団体の自立的な活動を支援し、県民活動を活発化させることにより、誰もがいきいきと輝く地域社会の実現を目指す。

（３）登録者数

時　点	個　人	団　体	企　業	合　計	LINE 友だち
令和 7 年 2 月末	1,371 件	213 件	28 件	1,612 件	849 件

（４）ホームページアクセス数（令和７年２月末）

「山口県県民活動スーパーネット」アクセス数：191,228
→うち「あいかさねっと」アクセス数：　67,351

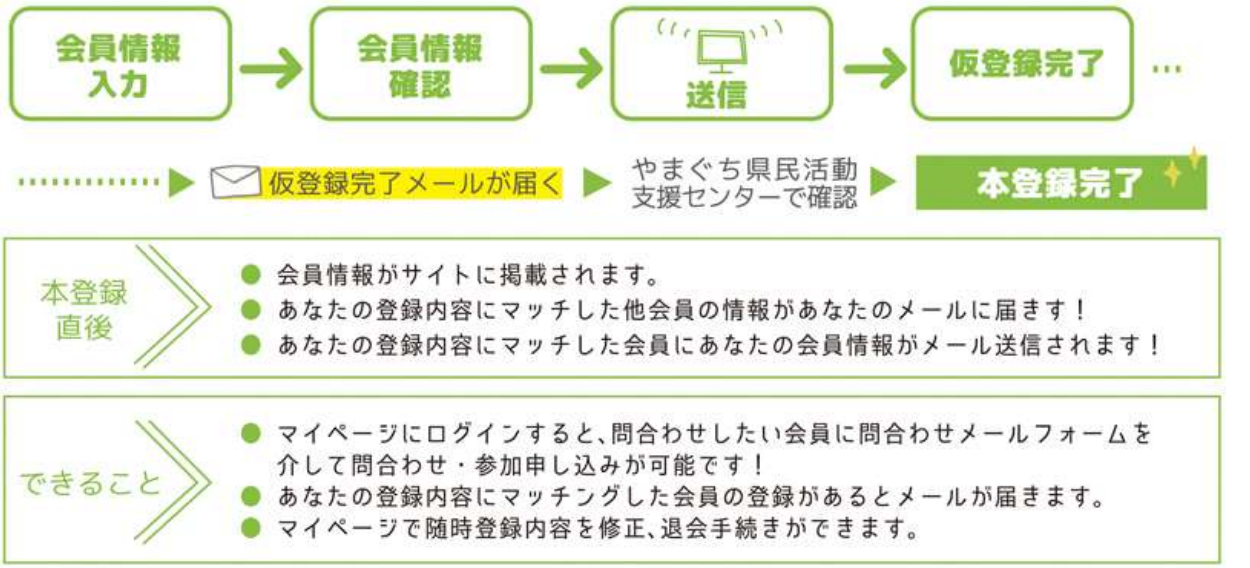
２　機　能

・ボランティア希望者（個人、団体、企業）の登録、検索、参加要請
・ボランティア募集情報・団体の登録、検索、参加申込
・参加条件、募集条件が合致した情報の送信
・会員制とし、会員は、情報の登録・修正・削除・追加依頼が可能
・管理画面により、各種情報の修正が可能
・「やまぐち健幸アプリ」との連携
※ボランティア募集情報を掲載した団体に対し、やまぐち健幸アプリを使用して読み込むことでやまぐち健幸アプリ内のポイントが付与される、二次元バーコードを自動送信する。団体側が、ボランティア活動当日に参加者へ二次元コードを提供することで、ボランティア参加者はやまぐち健康アプリ内でポイントを受け取れる。

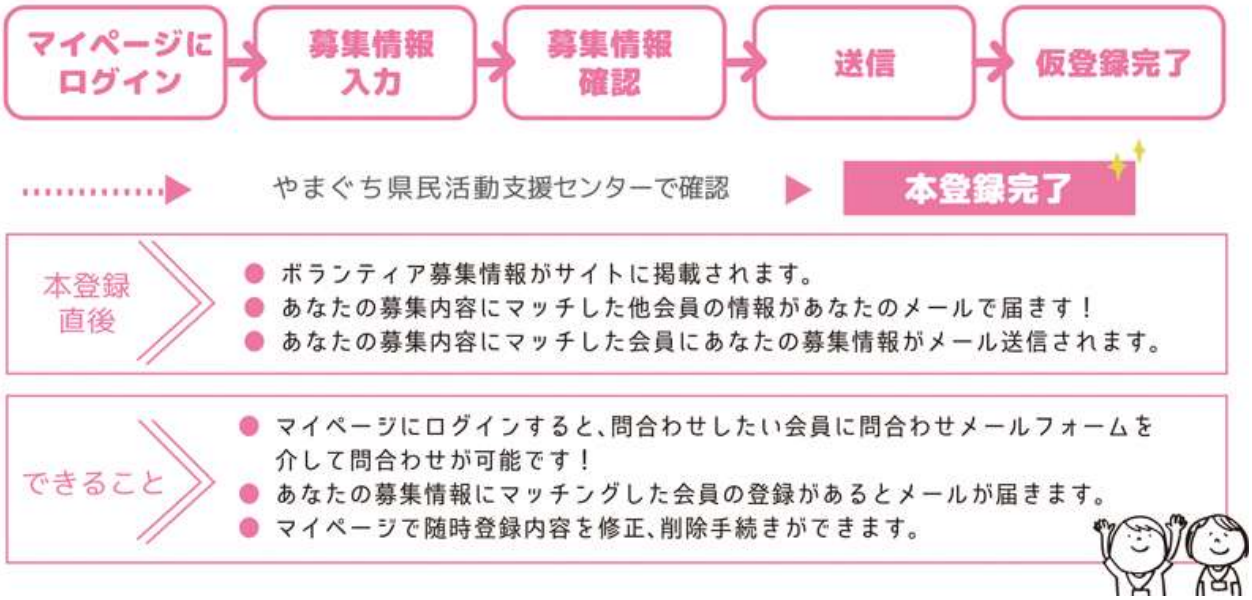
・LINE メッセージを利用したマッチングメールの送信
※あいかさねっとから配信されるボランティアマッチングメールと同様の情報を LINE 公式アカウントお友達登録者に対し LINE メッセージで送信

別紙２

＜会員登録の流れ＞



＜ボランティア募集の流れ＞



別紙２

３　構　成

タブ表示（位置）	掲載内容
HOME（上部）	○ボランティア募集情報（直近の募集情報３件） ○会員情報（現在の会員数及び直近の登録者情報６件） ○活動ニュース（直近のメールマガジン６件） ○お知らせ（直近のお知らせ７件） ＜下部のバナー＞ ○ボランティアしたい →ボランティアしたい会員一覧 （直近に登録した個人・団体・企業 20 者） ○ボランティア募集中 →募集中のボランティア一覧、ボランティア募集カレンダー、 過去のボランティア募集一覧 ○ご利用の方へ →概要説明と登録フォーム掲載 ○関連団体リンク →関連団体のリンクあり ○サイトマップ ○個人情報保護
募集中（上部）	※現在募集中のボランティア一覧、ボランティア募集カレンダー、 過去のボランティア募集一覧
探す（上部）	○【ボランティアをしたい会員･ボランティアを募集している団体】 検索フォーム ・会員種類（企業、団体、個人） ・地域（１９市町） ・分野（２０分野） ・一芸・プロボノ分野（１０分野） ・フリーワード検索
取材報告（上部）	○あいかさねっと取材報告の一覧あり ○取材報告の内容（写真あり） ※現データ件数：20 件
Q&A（上部）	○会員登録の流れ →登録フォームのリンクあり ○ボランティア募集の流れ →登録フォームのリンクあり
利用案内（上部）	○概要説明 ○登録フォームのリンクあり
ログインページへ （右横）	○ログイン ID、パスワード入力画面 ※パスワード再発行画面への誘導あり ※会員登録フォームのリンクあり
会員登録はこちら （右横）	○会員登録フォームのリンクあり
利用のかたへ （右横）	○概要説明 ○登録フォームのリンクあり

別紙２

タブ表示（位置）	掲載内容
ボランティア情報を探す（右横）	○【ボランティアをしたい会員・ボランティアを募集している団体】検索フォーム ・会員種類（企業、団体、個人） ・地域（１９市町） ・分野（２０分野） ・一芸・プロボノ分野（１０分野） ・フリーワード検索
登録用紙ダウンロード（右横）	○個人会員申込用紙（PDF 版、Word 版） ○団体会員申込用紙（PDF 版、Word 版） ○企業会員申込用紙（PDF 版、Word 版）
メルマガ会員登録（右横）	○メルマガ概要 ○登録フォーム、解除フォームのリンクあり
LINE Log in（右横）	※「あいかさねっと」LINE Official Account のサイトへ（外部リンク） https://page.line.me/789ubsdn
山口県県民活動スーパーネット（右横）	※「山口県県民活動スーパーネット」のサイトへ（外部リンク）
やまぐち健幸アプリ（右横）	※「やまぐち健幸アプリ」のサイトへ（外部リンク） https://kenko.pref.yamaguchi.lg.jp/kenko-app

４　登録者入力事項

・個人、団体、企業別の登録項目は別紙４のとおり
・登録前に「あいかさねっと利用規約」を表示させ、「同意する」場合に登録フォームに進めるようにすること。

５　募集情報の掲載内容

・活動分野　・活動内容　・活動日時　・活動地域　・活動場所
・募集主体（名称、連絡先、ﾎｰﾑﾍﾟｰｼﾞ URL）　・募集人員　・服装、準備物等
・募集期間　・その他連絡事項　・参考ファイル（チラシデータ等）

６　登録者の権限

項　目	一般閲覧者	登録者	管理者
参加情報・募集情報の検索	○	○	○
参加情報・募集情報の掲載	×	○	○
条件に合致する情報の配信	×	○	○
参加申込、参加要請	×	○	○
連絡先等その他登録情報の確認	×	×	○

別紙３

「山口県県民活動スーパーネット」への団体・企業情報　登録項目一覧

	項　目 （県民活動団体・NPO法人／企業）	県民活動団体・NPO法人		企　業	
		区分	留意事項	区分	留意事項
1	団体の分類／企業の分類	必須	※以下プルダウン 任意団体、財団法人、社団法人、一般財団法人、一般社団法人、公益財団法人、公益社団法人、社会福祉法人、行政、その他 ※NPO法人は初期設定で「NPO法人」を表示	必須	※以下プルダウン 株式会社、合同会社、合名会社、合資会社、その他
2	団体名／企業名	必須		必須	
3	団体名ふりがな／企業名ふりがな	必須		必須	
4	代表者名	必須	※以下の内容を掲載 （未成年者の方へ） 親権者など保護者の同意を得たうえで、本サイトの会員登録及び利用を行ってください。また、本サイトを利用し、ボランティアに参加する際には、親権者など保護者の同意を得て申し込んでください。 （「上記に同意する」に☑必須） ※未成年者からの申込みであって、親権者など保護者の同意を得ていると判断できない場合は、本サイトの利用停止、又は会員資格の取消しを行うことがございます。ご注意ください。	必須	※以下の内容を掲載 （未成年者の方へ） 親権者など保護者の同意を得たうえで、本サイトの会員登録及び利用を行ってください。また、本サイトを利用し、ボランティアに参加する際には、親権者など保護者の同意を得て申し込んでください。 （「上記に同意する」に☑必須） ※未成年者からの申込みであって、親権者など保護者の同意を得ていると判断できない場合は、本サイトの利用停止、又は会員資格の取消しを行うことがございます。ご注意ください。
5	役職名	任意		任意	
6	担当者名	必須		必須	
7	担当者役職	任意		任意	
8	活動分野	必須	※☑をつける ※19分野掲載（別途提示）	―	
9	対象エリア	必須	※以下プルダウン 山口県内市町、県内全域、中四国地域、西日本、全国	―	
10	対象市町	必須 （※）	※「対象エリア」で「山口県内市町」を選択したら必須 ※☑をつける ※19市町掲載	―	

11	活動目的	必須		—	
12	活動内容／業務内容	必須		必須	
13	CSR活動（CSRの取り組み、社会貢献活動等の概要）	—		必須	
14	協働・連携実績	任意		任意	
15	アピールポイント・広報・設立の経緯など	任意		任意	
16	主たる事務所	任意		—	
17	従たる事務所	任意		—	
18	郵便番号	任意		任意	
19	都道府県	必須	※47都道府県＋「—」からプルダウン	必須	※47都道府県＋「—」からプルダウン
20	市町	必須	※19市町＋山口県外からプルダウン	必須	※19市町＋山口県外からプルダウン
21	住所	必須		必須	
22	電話番号	任意		任意	
23	FAX	任意		任意	
24	Eメール	任意		任意	
25	設立年月日・発足年月日	任意		任意	
26	前年度総決算	任意	※以下プルダウン 10万円未満、10万円～30万円未満、30万円～50万円未満、50万円～100万円未満、100万円～500万円未満、500万円～1,000万円未満、1,000万円以上	—	
27	会員数／従業員数	任意		任意	
28	会費	任意		—	
29	会員資格	任意		—	
30	活動日時	任意		—	
31	URL	任意	※3種類入力可能 ※URLの説明記入欄あり	任意	※3種類入力可能 ※URLの説明記入欄あり
32	参考ファイル	任意	※以下の項目ごとにファイルを選択してアップロード可能 1.団体の定款又は規約ファイル 2.活動内容が分かる資料ファイル 3.その他参考ファイル	任意	※3種類添付可能

33	特徴	任意	※☑をつける ☐連携・協働の実績がある ☐CSR・社会貢献の実績がある ☐助成団体である ☐活動団体である ☐支援団体である ☐企業の社会貢献活動による地域づくり支援事業への参加を希望する	任意	※☑をつける ☐連携・協働の実績がある ☐CSR・社会貢献の実績がある ☐助成団体である ☐活動団体である ☐支援団体である ☐企業の社会貢献活動による地域づくり支援事業への参加を希望する
34	登録担当者（一般非公開）	必須		必須	
35	登録担当者役職（一般非公開）	任意		任意	
36	登録担当者電話番号（一般非公開）	必須		必須	
37	登録担当者Eメール（一般非公開）	必須		必須	
38	登録要件	必須	※一つずつ☑を入れてもらう ※一つでも☑が入っていなければ登録できない ※登録要件については、別途提示	―	

別紙４

「やまぐち社会貢献活動支援ネット　あいかさねっと」への個人・団体・企業情報　登録項目一覧

	項　目	個　人		団　体		企　業	
		区分	留意事項	区分	留意事項	区分	留意事項
1	ログインID（非公開）	必須		必須		必須	
2	パスワード（非公開）	必須		必須		必須	
3	氏名（非公開）	必須		―		―	
4	ふりがな（非公開）	必須		―		―	
5	団体の分類／企業の分類	―		必須		必須	※以下プルダウン 株式会社、合同会社、合名会社、合資会社、その他
6	団体名／企業名	―		必須		必須	
7	団体名ふりがな／企業名ふりがな	―		必須	※以下プルダウン NPO法人、任意団体、財団法人、社団法人、一般財団法人、一般社団法人、公益財団法人、公益社団法人、社会福祉法人、行政、その他	必須	
8	代表者名	―		必須	※以下の内容を掲載 （未成年者の方へ）　※ 親権者など保護者の同意を得たうえで、本サイトの会員登録及び利用を行ってください。また、本サイトを利用し、ボランティアに参加する際には、親権者など保護者の同意を得て申し込んでください。 □上記に同意する ※未成年者からの申込みであって、親権者など保護者の同意を得ていると判断できない場合は、本サイトの利用停止、又は会員資格の取消しを行うことがございます。ご注意ください。	必須	※以下の内容を掲載 （未成年者の方へ）　※ 親権者など保護者の同意を得たうえで、本サイトの会員登録及び利用を行ってください。また、本サイトを利用し、ボランティアに参加する際には、親権者など保護者の同意を得て申し込んでください。 □上記に同意する ※未成年者からの申込みであって、親権者など保護者の同意を得ていると判断できない場合は、本サイトの利用停止、又は会員資格の取消しを行うことがございます。ご注意ください。
9	役職名	―		必須		必須	
10	都道府県	必須	※47都道府県＋「―」からプルダウン	必須	※47都道府県＋「―」からプルダウン	必須	※47都道府県＋「―」からプルダウン
11	市町	必須	※19市町＋山口県外からプルダウン	必須	※19市町＋「―」からプルダウン	必須	※19市町＋「―」からプルダウン
12	電話番号	必須	（非公開）	必須		必須	
13	Eメール	必須	（非公開）	必須		必須	
14	性別	必須	※以下プルダウン 空欄、男性、女性、回答しない	―		―	
15	生年月日（非公開）	必須	※以下の内容を掲載 （未成年者の方へ）　※ 親権者など保護者の同意を得たうえで、本サイトの会員登録及び利用を行ってください。また、本サイトを利用し、ボランティアに参加する際には、親権者など保護者の同意を得て申し込んでください。 □上記に同意する ※未成年者からの申込みであって、親権者など保護者の同意を得ていると判断できない場合は、本サイトの利用停止、又は会員資格の取消しを行うことがございます。ご注意ください。	―		―	

別紙４

「やまぐち社会貢献活動支援ネット　あいかさねっと」への個人・団体・企業情報　登録項目一覧

	項　目	個　人		団　体		企　業	
		区分	留意事項	区分	留意事項	区分	留意事項
16	ボランティアを募集する・ボランティアに参加する	—		任意	※☑をつける □ボランティアを募集する □ボランティアに参加する	—	
17	参考ファイル	—		任意	※以下の項目ごとにファイルを選択してアップロード可能 1.団体の定款又は規約ファイル 2.活動内容が分かる資料ファイル 3.その他参考ファイル	—	
18	登録要件	—		必須	※一つずつ☑を入れてもらう ※一つでも☑が入っていなければ登録できない ※登録要件については、別途提示	—	
	＜以下、詳細登録画面で入力＞						
19	郵便番号	必須	（非公開）	必須		必須	
20	住所	必須	（非公開）	必須		必須	
21	FAX	任意	（非公開）	任意		任意	
22	URL	任意	※3種類入力可能 ※URLの説明記入欄あり	任意	※3種類入力可能 ※URLの説明記入欄あり	任意	※3種類入力可能※URLの説明記入欄あり
23	職業	必須		—		—	
24	資格	任意		—		—	
25	セールスポイント	任意		任意		任意	
26	会員数／社員数	—		必須		必須	
27	設立年月日／創立年月日	—		必須		必須	
28	設立目的	—		必須		必須	
29	主な活動内容／事業概要	—		必須		必須	
30	担当部署名（非公開）	—		任意		任意	
31	担当者名（非公開）	—		必須		必須	
32	役職名（非公開）	—		任意		任意	
33	ボランティア実績	—		—		任意	
	ボランティアに参加する場合の希望詳細						
34	活動可能地域	必須	※☑をつける ※19市町掲載	必須	※☑をつける※19市町掲載	必須	※☑をつける※19市町掲載
35	活動希望分野	必須	※☑をつける ※20分野掲載（別途提示）	必須	※☑をつける ※20分野掲載（別途提示）	必須	※☑をつける※20分野掲載（別途提示）
36	活動可能曜日	必須	※☑をつける ※月～日まで掲載	必須	※☑をつける ※月～日まで掲載	必須	※☑をつける※月～日まで掲載
37	活動可能時間帯	必須	※プルダウンから選択	必須	※プルダウンから選択	必須	※プルダウンから選択
38	趣味・特技・専門性を活かした一芸ボランティア・プロボノ詳細						
39	分野	任意		—		—	
40	内容や対象	任意		—		—	
41	準備するもの・経費	任意		—		—	
42	その他（非公開）	任意	※希望する場合は☑ □メルマガ配信を希望する	任意	※希望する場合は☑ □メルマガ配信を希望する	任意	※希望する場合は☑ □メルマガ配信を希望する

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

Web アプリケーションセキュリティに係る特記仕様書

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、山口県が導入するシステム（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山口県に提示すること。

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、山口県知事（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。

【参考資料：現保守事業者より提供受】

スーパーネット仕様書

一般	トップページ	緊急のお知らせ掲載枠	管理画面から掲載可
		団体情報	新着順
		募集情報	新着順
		助成金情報	新着順
		ページの途中	可変枠 ※管理画面から掲載可能　現在はセンターがカレンダーを表示
		センターからのお知らせ	新着順
	団体・企業	一覧	
		簡易検索	簡易項目・必須入力・IDの重複チェック・DB登録
		詳細検索	
		検索結果一覧	
	団体・企業新規登録	NPO法人	事前に規約表示あり
		その他非営利	事前に規約表示あり
		企業	事前に規約表示あり
	新規登録時処理	イベント	センターに会員登録依頼ありのメールを自動送信
			登録者に仮登録依頼完了のメールを自動送信
			団体・企業のみ：仮登録完了画面表示時に引きつづき「あいかさねっとに登録」ボタンを表示し、クリックするとあいかさねっとの登録画面に遷移する(同一項目の入力が省略できるよう同じ項目は選択・入力済みの状態とする)
	修正	検索	登録団体や企業の情報を修正するために検索する
		検索結果一覧	
	修正画面	NPO法人	

		その他非営利	
		企業	
	イベント・募集	カレンダー	
		簡易検索	
		詳細検索	
		検索結果一覧	
	活動実績・事例	一覧	※現在は利用団体が限られている
		詳細	
	助成金情報	募集締め切りカレンダー	
		簡易検索	
		詳細検索	
		検索結果一覧	
	蔵書情報	一覧	
		詳細	
		詳細検索する	
		検索結果一覧	
	全体検索		
	その他		センターホームページ他、多数は固定ページにあり
管理画面	トップページ		現在の団体数集計(県民活動団体・NPO法人・企業)×(活動中・解散・退会)
			団体情報のCSV出力あり
	団体	一覧	
		詳細	仮登録(レビュー)から本登録(公開)にすると、団体に公開した旨が自動メール送信される
	団体情報修正依頼	一覧	

		詳細	仮登録(レビュー)から本登録(公開)にすると、団体に修正公開した旨が自動メール送信される。データは修正内容を本登録用TBにアップデートする
	募集情報	一覧	
		詳細	仮登録(レビュー)から本登録(公開)にすると、団体に公開した旨が自動メール送信される
	募集情報修正依頼	一覧	※こちらからの修正依頼件数はわずか
		詳細	仮登録(レビュー)から本登録(公開)にすると、団体に修正公開した旨が自動メール送信される。データは修正内容を本登録用TBにアップデートする
	メルマガバックナンバー	一覧	
		詳細	下書・仮登録(レビュー)・公開(登録)・複製機能あり
		仮登録→登録	仮登録(レビュー)から登録(公開)に変更すると、メルマガ会員のうち、メール送信を停止していない会員にメルマガが送信される
	蔵書情報	一覧	
		詳細	登録・修正・削除
	報告	一覧	
		詳細	登録・修正・削除
	助成	一覧	
		詳細	登録・修正・削除
	お知らせ	一覧	
		詳細	登録・修正・削除
	センターからのお知らせ	一覧	
		詳細	登録・修正・削除
	メルマガメンバー	一覧	
		詳細	登録・修正・削除

	固定ページ	一覧	
		詳細	登録・修正・削除
	管理画面ユーザー情報	一覧	管理者・編集者(センター職員)あり
		詳細	登録・修正・削除・休止　あり

文字サイズ・背景色変更機能あり

googleアクセス解析はいれているが解析自体はセンターがしている

情報はwordpressのDBを提供

あいかさねっと仕様書

一般	トップページ	緊急のお知らせ掲載枠	管理画面から掲載可
		お知らせ	
		ボランティア募集情報	新着順
		その他	会員情報自動集計掲載　例)現在の会員数　：　個人〇件 団体〇件 企業〇件　〇全件
		会員情報	新着順
		活動ニュース	メルマガ新着順
		お知らせ	新着順
	ボランティア募集	現在募集中の一覧	
		募集カレンダー	
		過去の一覧	
		詳細	
	会員を探す	検索フォーム	検索条件に一致した会員を検索
		検索結果一覧	
		会員情報詳細	ボランティア募集情報(過去も含む)について一覧表示
	取材報告	一覧	
		詳細	
	Q&A	使い方への質問と回答	複数ページあり　※画面と内容を最新の状態とする必要あり
	利用案内	利用の仕方	複数ページあり　※画面と内容を最新の状態とする必要あり
	その他案内・説明ページ		複数ページあり　※画面と内容を最新の状態とする必要あり
	団体関連リンク		※内容を最新の状態とする必要あり
	サイトマップ		※内容を最新の状態とする必要あり
	個人情報保護		※内容を最新の状態とする必要あり
	登録用紙ダウンロード		※様式を最新の状態とする必要あり

	新規登録	個人	簡易項目・必須入力・IDの重複チェック・DB登録、事前に規約表示あり
		企業	簡易項目・必須入力・IDの重複チェック・DB登録、事前に規約表示あり
		団体	簡易項目・必須入力・IDの重複チェック・DB登録、事前に規約表示あり
	新規登録時処理	イベント	センターに会員登録ありのメールを自動送信
			登録者に仮登録完了と、ログインして詳細入力を依頼するメールを自動送信
			団体・企業のみ：仮登録完了画面表示時に引きつづき「スーパーネットに登録」ボタンを表示し、クリックするとスーパーネットの登録画面に遷移する(同一項目の入力が省略できるよう同じ項目は選択・入力済みの状態にする)
	ログイン		
	パスワード再発行		
	全体検索		
マイページ	ログアウト		
	マイページ	登録情報	
		募集情報一覧(団体のみ)	
	会員情報修正	個人	新規より項目増
		企業	新規より項目増
		団体	新規より項目増
	休止・再開依頼・退会	会員共通	
	ボランティア募集	一覧	過去の登録したボランティアの募集一覧
		修正・削除	
		新規登録	※ボランティア募集は団体のみが登録可能
	ボランティア募集	イベント	センターにボランティア募集登録ありのメールを自動送信
			登録者に仮登録完了をメールを自動送信

	マッチングメール	イベント	ボランティアしたい会員が、マッチングメールに記載のURLをクリックすることで、募集団体向けに、会員がログインせずともワンクリックで参加申込または問い合わせを送信することができる
		イベント	上記で参加申込をクリックすることで、募集団体に参加申込した会員の名前とメールアドレス、電話番号がメールにより自動送信される
		イベント	センターにもBCCにより送信される
		イベント	DB保存される(管理画面からは閲覧できない)
		イベント	上記で問い合わせをクリックすることで、募集団体に問い合わせした会員の名前とメールアドレス、問い合わせ内容がメールにより自動送信される
		イベント	センターにもBCCにより送信される
		イベント	DB保存される(管理画面からは閲覧できない)
			サイドバーにログイン中と分かるよう表示
	ログイン中		ボランティア募集情報詳細の下に「問い合わせる」「参加する」ボタンを表示
		イベント	上記で参加申込をクリックすることで、募集団体に参加申込した会員の名前とメールアドレス、電話番号がメールにより自動送信される
		イベント	センターにもBCCにより送信される
		イベント	DB保存される(管理画面からは閲覧できない)
		イベント	上記で問い合わせをクリックすることで、募集団体に問い合わせした会員の名前とメールアドレス、問い合わせ内容がメールにより自動送信される
		イベント	センターにもBCCにより送信される
		イベント	DB保存される(管理画面からは閲覧できない)
		団体会員ログイン	団体がログインしている場合、会員情報詳細の下に「問い合わせる」ボタンを表示
		イベント	上記をクリックすることで問い合わせフォームを表示
		イベント	上記で問い合わせをクリックすることで、会員に向けて、団体情報と問い合わせ内容がメールにより自動送信される
		イベント	センターにもBCCにより送信される

		イベント	DB保存される(管理画面からは閲覧できない)
	メルマガ会員	登録	
		停止	
管理画面	会員情報	一覧	
		詳細	下書・仮登録(レビュー)・公開(登録)・複製機能あり
		会員登録後処理	会員一覧ページに仮登録(レビュー)表示
			会員詳細ページで内容確認 OKであれば公開、NGであればセンターが個別に電話等で連絡
		仮登録→登録	仮登録(レビュー)から登録(公開)に変更して一般画面で会員情報が閲覧可能となる
			登録(公開)時、個人・企業・団体(ボランティアをしたい)にマッチングする募集団体情報を登録者へメールで自動送信する
			登録(公開)時、団体(ボランティアを募集する)の分野や地域にマッチングする会員情報を登録者(団体)へメールで自動送信する
			登録(公開)時、登録者が募集情報のいずれかにマッチしている場合、新たな会員登録があったことを募集団体へメールで自動送信する
		その他機能	メール停止(メールが不通になったときセンター側で停止する)
		その他機能	データエキスポート
	ボランティア募集情報	一覧ページ	
		詳細	下書・仮登録(レビュー)・公開(登録)・複製機能あり
			センターが内容確認し仮登録(レビュー)から登録(公開)に変更する
			募集期間内または随時募集であり、団体も公開されている場合、一般画面で募集情報を閲覧できる
			ボランティアを募集した団体へ、募集内容の曜日と地域にマッチングした会員情報一覧がメールにより自動送信される
			募集内容の曜日と地域がマッチングしているボランティアしたい会員に向けてマッチングメールを自動送信

	メルマガバックナンバー	一覧	
		詳細	下書・仮登録(レビュー)・公開(登録)・複製機能あり
		仮登録→登録	仮登録(レビュー)から登録(公開)に変更すると、メルマガ会員のうち、メール送信を停止していない会員にメルマガが送信される
	取材記事	一覧	
		詳細	下書・仮登録(レビュー)・公開(登録)・複製機能あり
	お知らせ	一覧	
		詳細	下書・仮登録(レビュー)・公開(登録)・複製機能あり
	ヘルプ	一覧	
		詳細	下書・仮登録(レビュー)・公開(登録)・複製機能あり
	固定ページ	一覧	
		詳細	下書・仮登録(レビュー)・公開(登録)・複製機能あり
	管理画面ユーザー情報	一覧	システム管理者・編集者(センター職員)あり
		詳細	登録・修正・削除・休止　あり

文字サイズ・背景色変更機能あり
年1回FTPで健康アプリとの連携用のファイルをアップデートし、自動メール送信の文面を変更する作業あり
googleアクセス解析はいれているが解析自体はセンターがしている
データの必須項目は、必須→必須でない→必須に変わるなどした経緯があり、not nullにしていないが必須の項目あり(年齢)
情報はwordpressのDBを提供のほか、メルマガメンバー、問合せ履歴、募集情報、団体情報は独自テーブルあり

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。

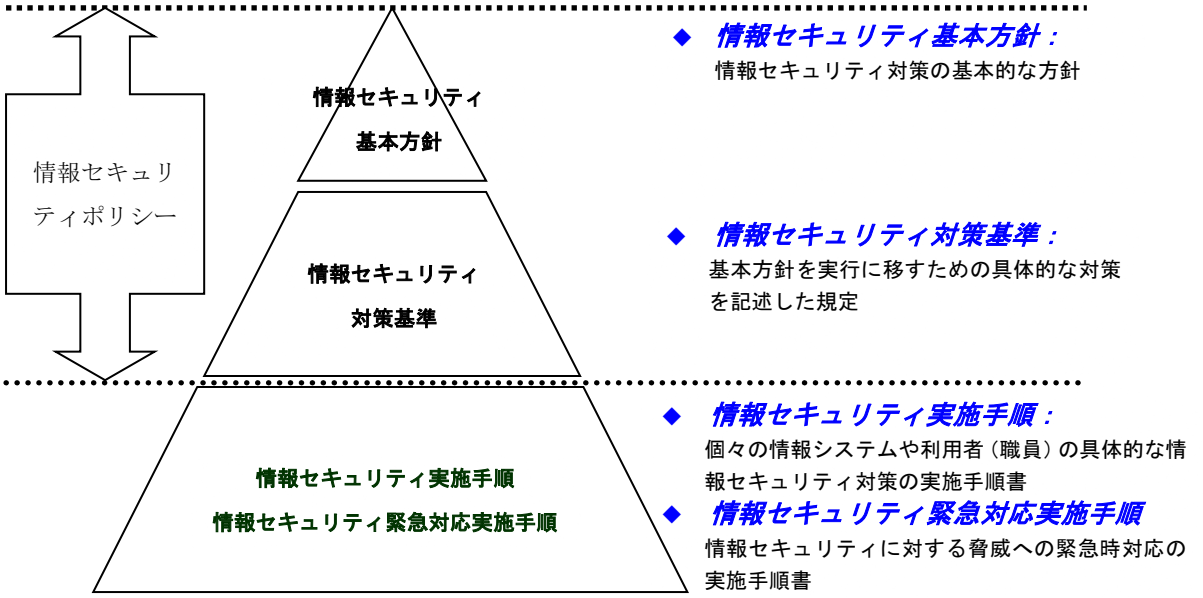
本県においても、令和２年12月に閣議決定された国の「デジタル社会の実現に向けた改革の基本方針」及びデジタル庁において策定された「デジタル社会の実現に向けた重点計画」や総務省において策定された「自治体ＤＸ推進計画」等を踏まえながら、令和３年３月に「やまぐちデジタル改革基本方針」を策定し、①『やまぐちＤＸ』の創出、②『デジタル・ガバメントやまぐち』の構築、③『デジタル・エリアやまぐち』の形成の３つの柱を掲げ、社会全体のデジタル化に向けた取組を進めているところである。

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。

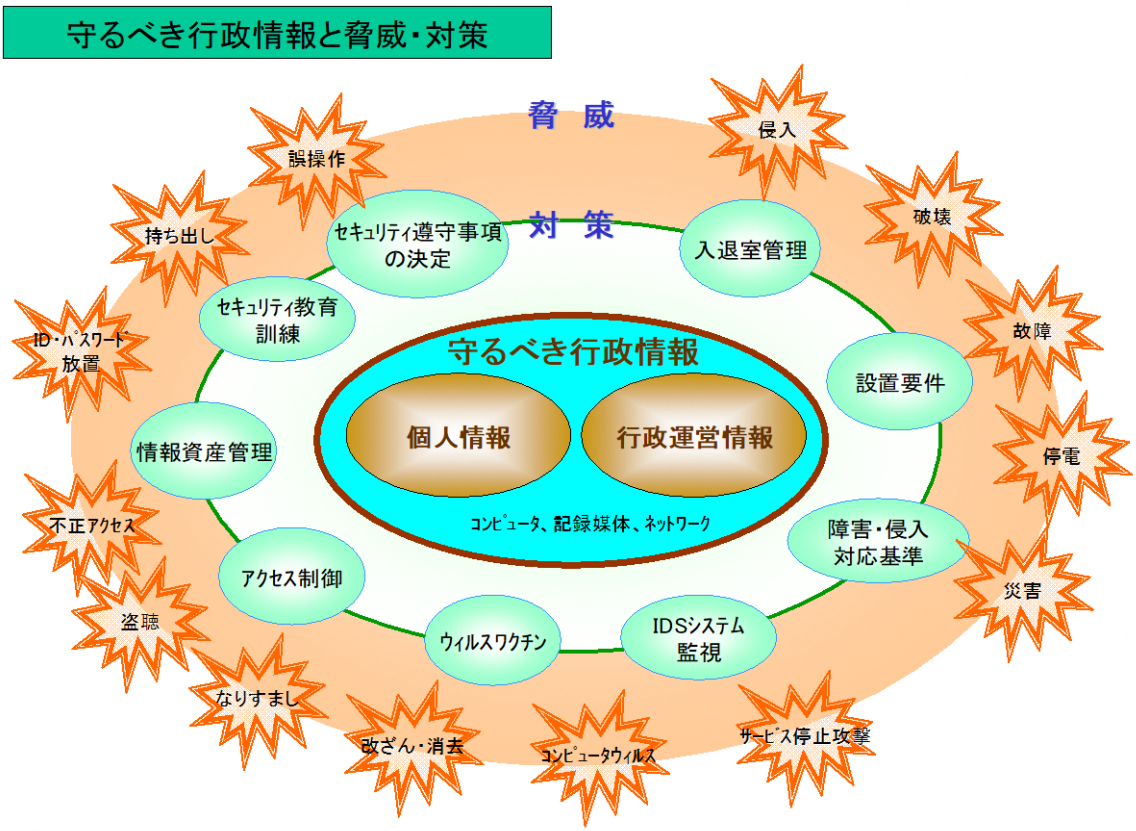
（１）　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（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

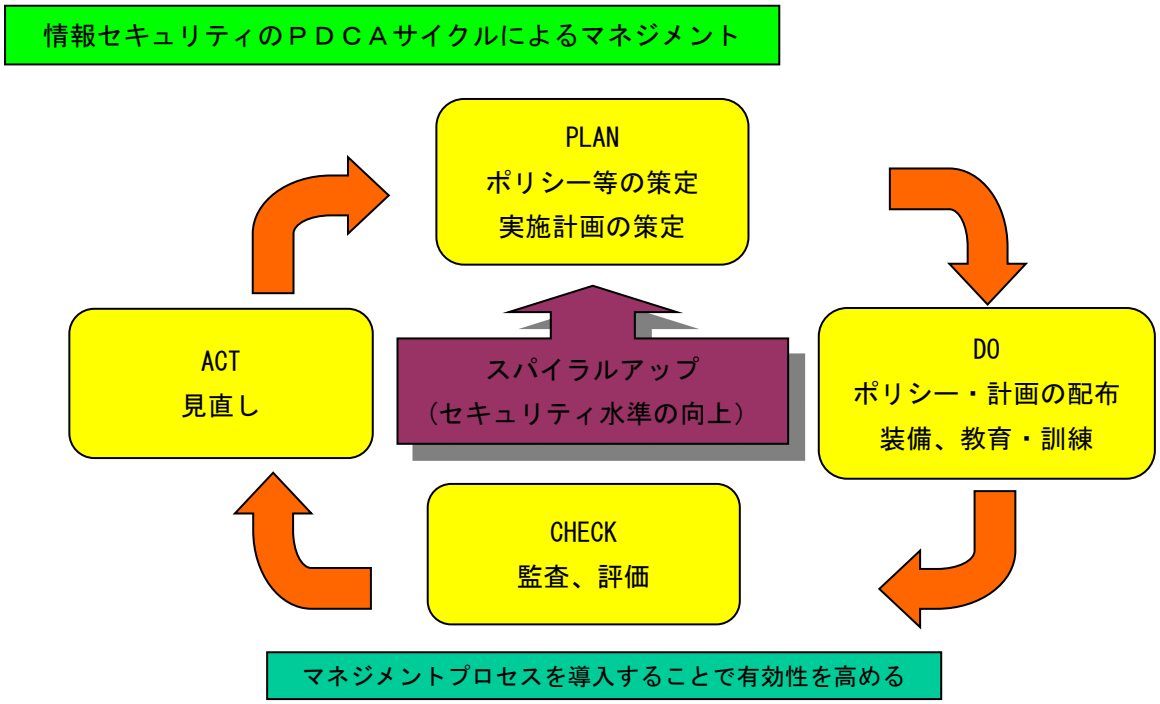
情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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）

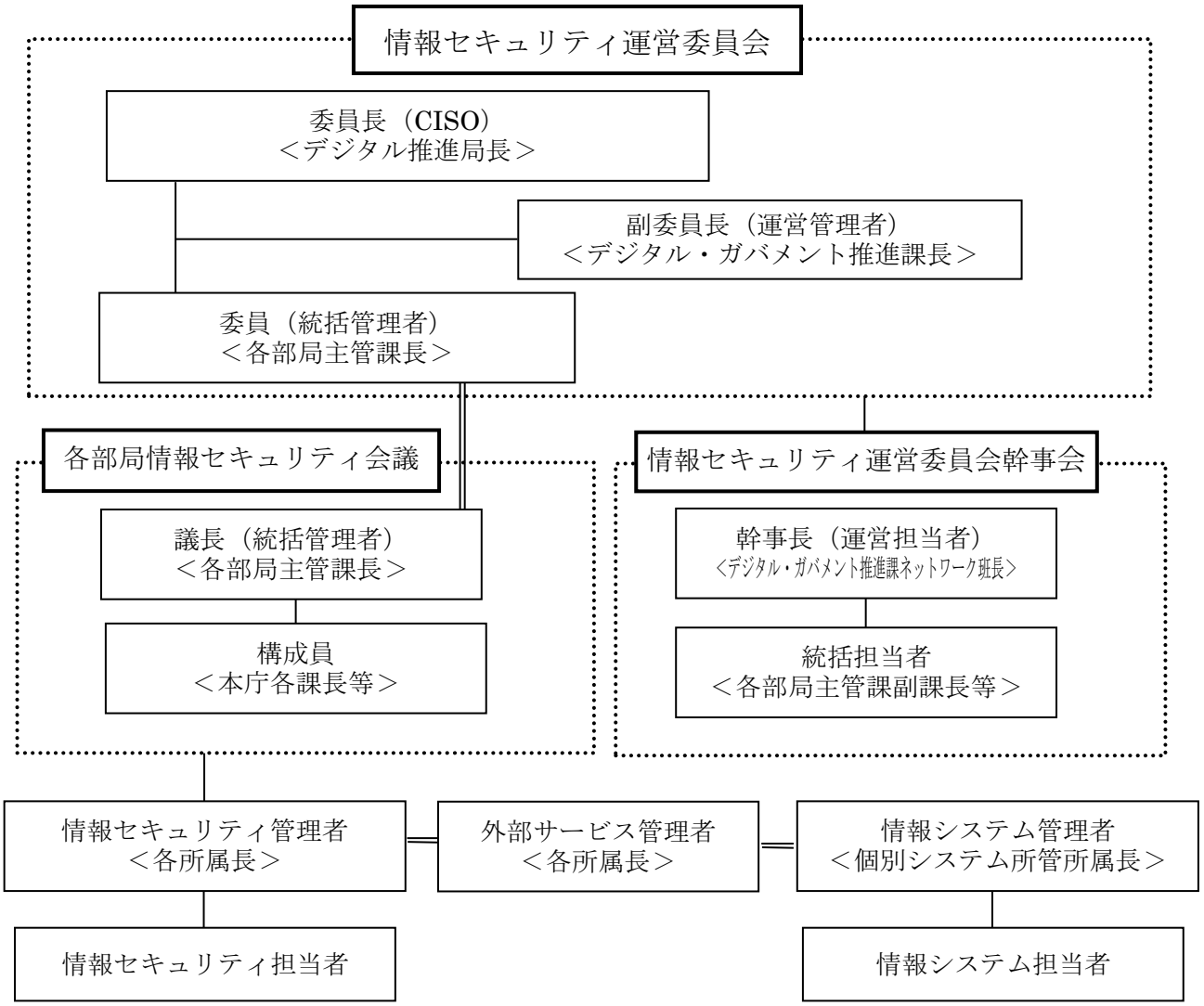
① 運営管理者は、重大な情報セキュリティインシデント対応のために、情報セキュリティ緊急対応チーム（山口県 CSIRT : Computer Security Incident Response Team）（以下、「緊急対応チーム」という。）を設置する。

② 緊急対応チーム責任者は、運営管理者とする。

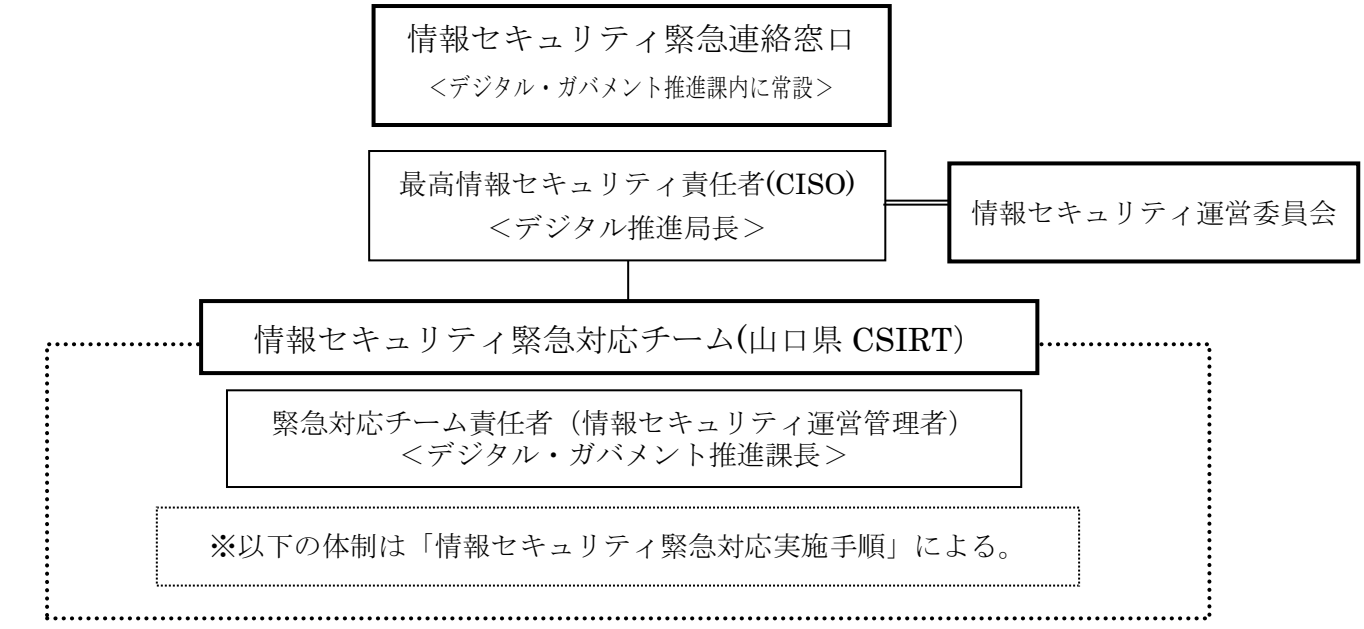
③ 緊急対応チームの運営は、「情報セキュリティ緊急対応実施手順」に従うものとする。

＜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

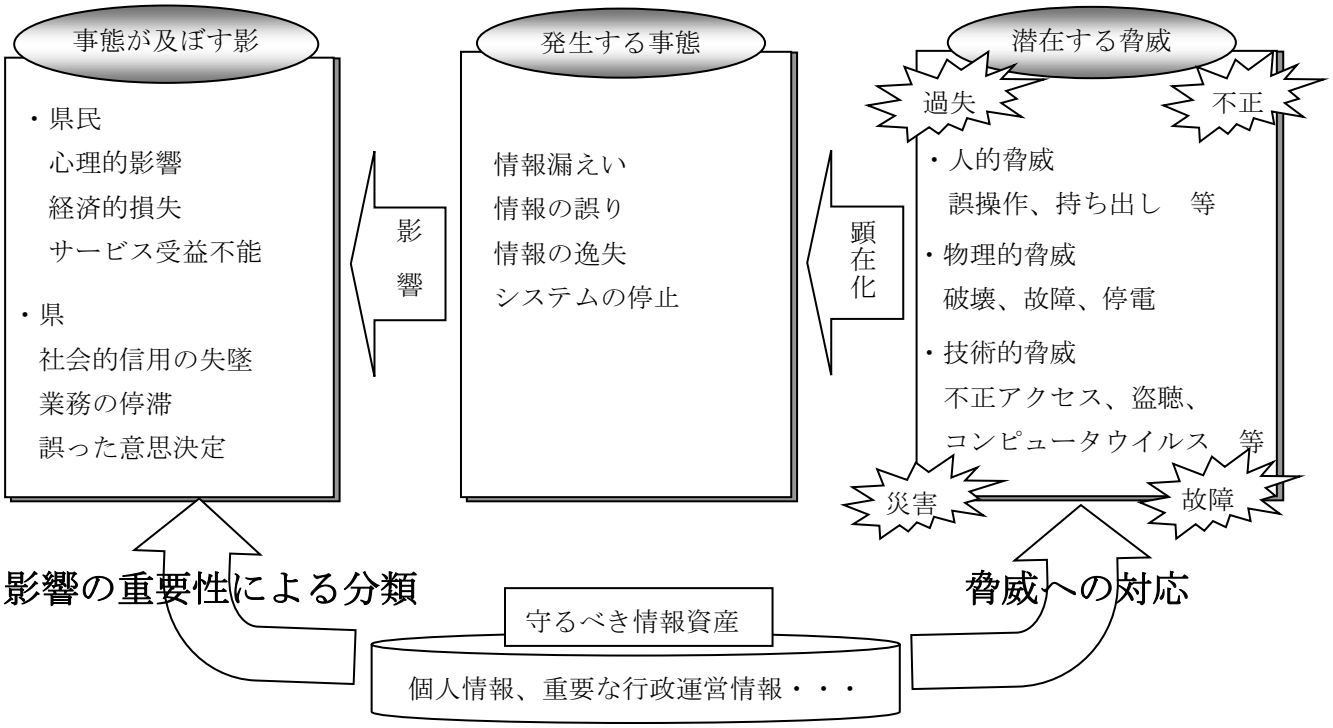
（ア）情報セキュリティ管理者及び情報システム管理者（以下「情報セキュリティ管理者等」という。）は、所管のコンピュータ、周辺機器等を管理する職員等を定め、誰がどのコンピュータ等を管理するのか明確にしなければならない。

（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。

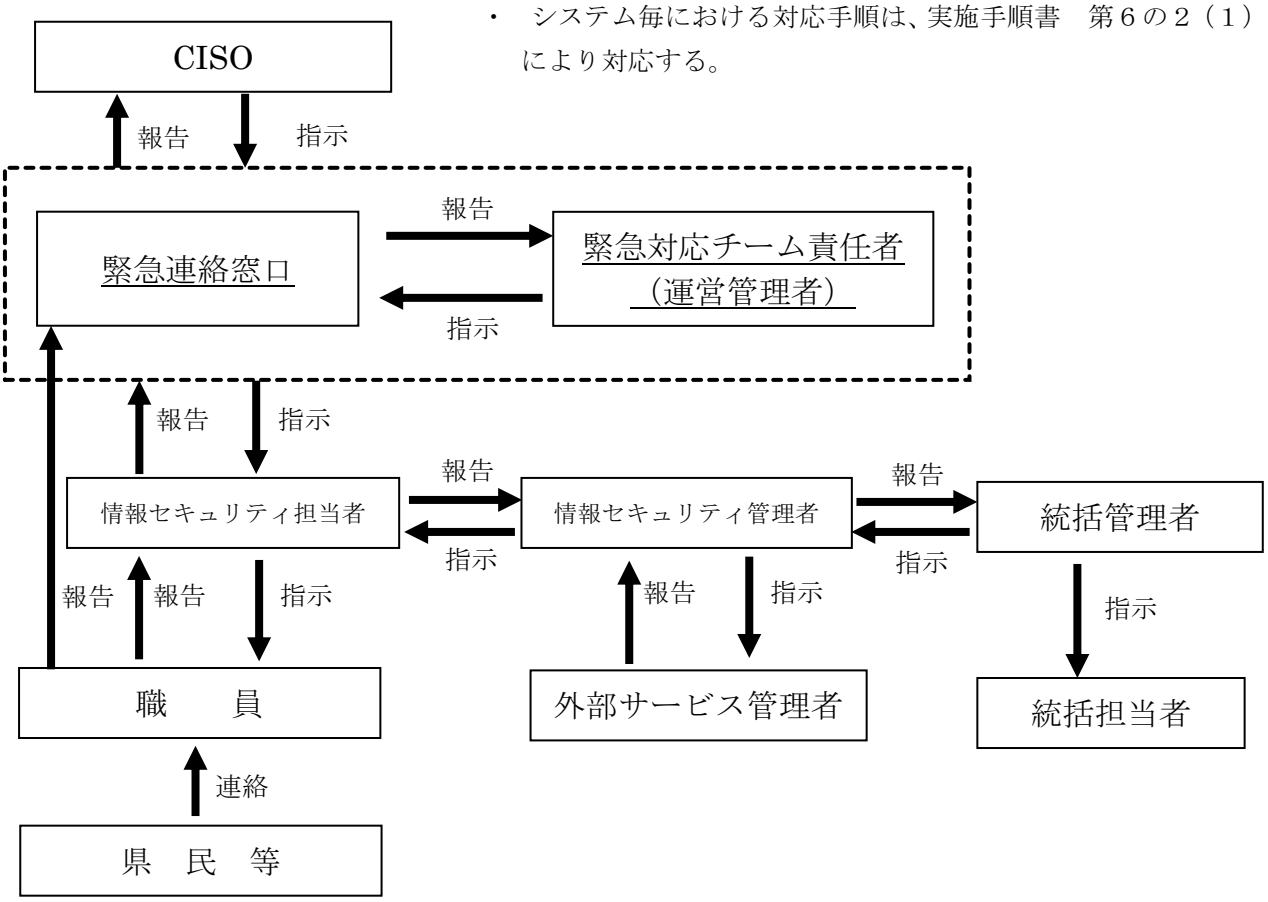
③ 統括管理者は、情報セキュリティ管理者から情報セキュリティインシデントの報告を受けた場合、必要に応じて、情報セキュリティ管理者及び統括担当者に指示を行うものとする。

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。