

山口県インターンシップ推進協議会ホームページリニューアル実業務仕様書

本仕様書は、山口県(以下、「委託者」という。)と受託者との間で契約する山口県インターンシップ推進協議会ホームページリニューアル業務の委託について適用する。

1 背景

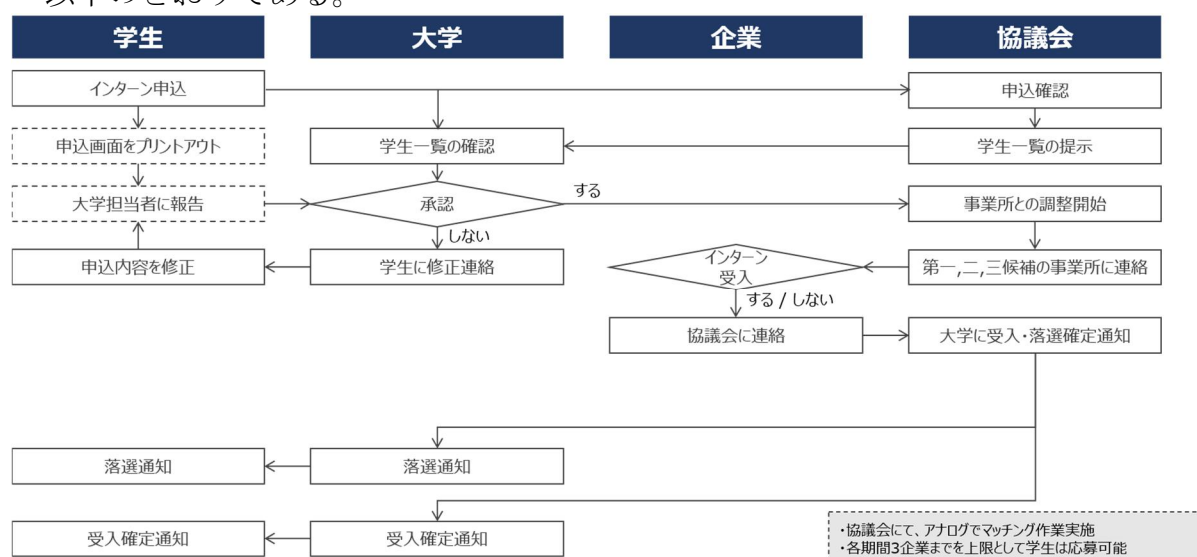
現行の山口県インターンシップ推進協議会(以下、「協議会」という。)のホームページでは、情報の構成や申込みまでの導線が分かりにくく、学生が企業に関心を持っても申込みに至らないケースが生じている。

(参考：現行ホームページ URL : <https://www.y-internship.com/>)

また、申込受付後のマッチング業務については、管理システムと手作業・帳票を併用した運用となっており、業務負担が大きいことから、募集期間の確保や迅速なマッチングの面で課題を抱えている。

2 現行のマッチング業務フロー

本事業で構築する「マッチング支援ツール」が対象とする現在の業務フローは以下のとおりである。



- (1) 申込み (学生) : 学生がホームページ上のフォームから、希望する企業や実習時期等を入力し、1～4件程度のマッチングが成立するよう申込みを行う。
- (2) 大学承認 (各大学担当者) : 申込みを保存すると申込者リストに登録される。協議会から学生の所属大学へ、適格性の確認・承認を依頼し、大学が承認を行う。
- (3) マッチング調整 (協議会) : 大学の承認が得られた学生について、協議会が企業側の受入枠と照らし合わせ、調整を行う。
- (4) 受入可否確認 (企業) : マッチング候補となった学生について、協議会から企業へ受入の打診を行い、企業が受入の可否を判断する。
- (5) 結果通知 (協議会) : マッチングが確定した後、協議会から大学へ、大学から学生へ結果を通知する。

現在、これらの工程における「大学への承認依頼」「企業への打診」「各所への結果通知」及び進捗管理の多くを、メールや Excel、手作業による帳票作成で行っており、本業務によってこれらを一元管理・効率化することを目指す。

3 現行システムの状況

現行システムの規模及び稼働環境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インフラ構成、セキュリティ対策、及びデータ移行計画を提案すること。

(1) システム構成・インフラ環境

サーバー環境(本番用)：さくらのレンタルサーバ ビジネス(共用サーバー)

サーバー環境(バックアップ用)：さくらのレンタルサーバ スタンダード

ディスク容量：本番 600GB(使用量 7.72GB) /バックアップ 300GB(使用量 6.24GB)

導入 CMS：WordPress 5.0.22

(2) 利用状況及びトラフィック統計

総ページ数：固定ページ 29 ページ(投稿記事を除く)

平均月間アクセス数(直近1年間)：約 13,200 PV / 約 1,900 ユーザー

最大アクセス集中時期：5月(インターンシップ募集開始時期等)

ピーク時月間アクセス数：約 51,000 PV(平常時の約4倍)

(3) 蓄積データ量(データ移行の参考値)

企業情報登録件数：557 件

学生情報登録件数：973 件

投稿記事数(お知らせ等)：5 件

データベースサイズ：本番約 11.7 MB/バックアップ 6.41MB

4 事業の目的

本事業は、単なるデザイン刷新に留まらず、学生の行動プロセスに即した UI/UX の再設計を行うことにより、学生が県内企業を知り、比較・理解し、安心して申込みに至る環境を整備するとともに、県内企業の認知向上及びマッチング率の向上を図ることを目的として、新たなホームページを構築するものである。

あわせて、申込受付後のマッチング業務についても見直しを行い、協議会における進捗管理を効率化するため、申込受付後のマッチング業務を支援するツール(以下、「マッチング支援ツール」という。)を整備し、インターンシップ推進事業全体の円滑な実施を図る。

5 本事業における基本的な考え方

本業務において構築するホームページ及びマッチング支援ツールは、学生・大学・企業・協議会間におけるインターンシップ申込みおよび受入れ調整業務を一元的・効率的に実施し、協議会が行うインターンシップ推進事業全体を円滑に実施するための基盤として位置付ける。

(1) 利用者区分

本ホームページ及びマッチング支援ツールの利用者は、学生、大学担当者、企業担当者、協議会(運営管理者)の4者とする。

(2) ホームページに関する考え方

本ホームページは、「探す・理解する・安心する(不安や迷いを解消する)・申し込む」という学生の行動プロセスを一貫して支援し、不安や迷いを感じる

ことなく次の行動へ進める UI/UX 設計を重視するとともに、企業の情報登録が簡便に行えるようにする。

各画面において、利用者が「今どの段階にいるのか」、「次に何をすべきか」を直感的に理解できる構成とする。

(2) マッチング支援ツール及び運営に関する考え方

学生による申込み受付後の業務は、大学担当者による確認・承認、企業とのマッチング調整を経て結果を通知する業務フローである。

なお、協議会は学生の申込み内容、企業とのマッチング調整において、学生、大学、企業に助言を行っているため、この業務が可能な機能を盛り込むこと。

また、構築後は協議会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、特定の事業者依存しない構成とする。

(3) 閲覧環境に関する考え方

本ホームページは、学生が主にスマートフォンから閲覧・利用することを想定し、デバイスやブラウザの違いによらず、支障なく閲覧・利用できる閲覧環境の確保に配慮した設計とする。

(4) 最低限仕様及び積極提案の位置付け

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。

6 委託契約期間

契約締結日から令和9年3月31日まで

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。

- ア ホームページ全体の企画・構成設計・デザイン制作
- イ UI/UX 設計（学生の行動・心理を踏まえた導線設計を含む）
- ウ システム構築・実装（ホームページ本体）
- エ マッチング支援ツールの企画・設計・新規開発
- オ 現行ホームページに付随する管理機能の見直し及び再整備
- カ テスト及び動作確認（ホームページ及びマッチング支援ツール）
- キ 本番環境への公開
- ク 納品・引継対応（協議会の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 本ホームページ公開後の継続的な運営・更新業務（協議会が主体となって実施することを想定）
- イ 本ホームページ公開後の保守・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、次年度以降に必要な保守運用費用（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（契約金額）には含まないものとする。

8 機能要件

(1) ホームページ

【必須機能】

- ア トップページから直感的に利用可能な企業検索機能
(学年、実施期間、体験内容等の条件による検索・絞り込みを想定)
- イ 募集中企業が一目で分かる企業一覧表示
- ウ 企業詳細ページの作成（企業概要や体験内容が理解しやすい情報構成）
全社共通となる標準項目と各社固有の情報を補足できる自由記述（備考欄）などマッチング精度向上に向けた提案を含めること。なお、協議会も編集可能な権限や、協議会による公開前に企業担当者へ助言できる機能を有すること。
- エ 企業詳細ページから直接申込可能な一体的導線設計
ただし、学生による企業の申込は、同一期間で上限 10 社までと制限し、マッチング精度が高まる提案とすること。
- オ 入力負担を軽減した申込フォーム
- カ スマートフォン利用を前提とした UI 最適化
- キ AI 等デジタル技術を活用した企業レコメンド機能
学生が申込時に入力する自己 PR や志望理由等の自由記述情報について、生成 AI 等を用いて整理・分析することにより、学生の志向や関心に基づいてインターンシップ応募企業のレコメンド機能を有すること。
加えて、学生が特定の企業で就業体験を申し込む際（申込前又は申込完了直後を想定）に、当該企業と類似する条件（例：業種、実施時期、体験内容、地域等）に基づき、追加候補となり得る県内企業を複数社提示すること。
その他、学生や企業担当者の入力負担軽減や利便性向上に資する適切なタイミングでのレコメンドについても、提案に含めること。
提示にあたっては、学生の選択肢拡充及び県内企業の認知度向上に資するよう配慮すること。

(2) マッチング支援ツール

【目的】

協議会における申込受付後の学生・企業のマッチング作業を省力化し、進捗管理を効率化することを目的とする。

本ツールは、各利用者が、それぞれの権限に応じて当該情報を確認・操作できることを想定する。

【必須機能】

(共通)

- ア 利用者権限
 - ・利用者区分（学生、大学担当者、企業担当者、協議会）ごとのログイン機能

- イ 進捗管理画面
 - ・申込み・大学承認・調整・確定・通知までの各ステータスについて、進捗状況を表示（各利用者は権限に応じたステータス閲覧のみ可能とする）
- ウ 通知
 - ・マッチング結果の通知機能
 - ・作業する必要がある場合の通知機能
 （学生）
- ア 申込み・結果状況確認
 - ・自身の行った申込み及びマッチング結果を確認できる機能
 - ・複数のマッチング成立を希望している場合は、期間が重複しない機能
 （大学担当者）
- ア 承認・差戻し
 - ・学生申込み時の承認／差戻し機能（必要に応じてコメント等を付与できること）
- イ 申込み状況確認
 - ・学生の申込状況を集約した一覧画面において、自大学の学生の申込状況を確認できる機能
 （企業担当者）
- ア 受入れ可否選択
 - ・大学承認済みの申込みに対する受入れ可否選択機能
- イ 申込み状況確認
 - ・学生の申込状況を集約した一覧画面において、自社への学生の申込状況を確認できる機能
 （協議会）
- ア 管理
 - ・全体進捗の一覧管理
 - ・企業の受入枠、受入条件、回答状況等の管理
 - ・学生の申込み内容、企業担当者の受入れ選択に対し助言できる機能
- イ 補助・管理機能
 - ・学生・大学・企業・進捗状況単位での検索・抽出
 - ・データ出力機能（CSV 等）
 - ・履歴管理（操作ログ等）

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あたっては、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 本ホームページは、学生が主にスマートフォンから閲覧・利用することを想定し、PC 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スデザインとすること。
- ウ 対応ブラウザについては、一般的に広く利用されている最新バージョン（Google Chrome、Microsoft Edge、Safari 等）を対象とし、特定のブラウザや旧バージョンに依存しない構成とすること。

（２）セキュリティと安全性

- ア 本ホームページ及びマッチング支援ツールの構築・運用にあたっては、

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」及び山口県情報セキュリティポリシー（※詳細は山口県ホームページにて公開中の最新版を参照のこと）を遵守し、個人情報保護及びセキュリティ確保に万全を期すこと。

イ 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講じること。

ウ 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、受託者の責任において速やかに改善策を図ること。

エ 障害又はインシデント発生時には、速やかに委託者へ報告し、指示に基づき対応すること。

オ データについては、定期的なバックアップを実施し、障害発生時に速やかな復旧が可能な体制を確保すること。

（3）システム性能と拡張性

ア 本ホームページは、利用者がストレスなく閲覧・操作できるよう、ページ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。

イ 募集開始時や締切直前など、一時的にアクセスが集中する状況を考慮し、同時アクセスが発生した場合においても、通常の利用に支障が生じない性能を確保すること。

ウ 将来的な機能追加・改修を想定した拡張性を確保すること。

（4）公開に向けたドメイン・移行作業

ア 本ホームページの公開にあたっては、現行ドメイン（y-internship.com）を継続して使用すること。

イ 新システムへの切り替えに伴うサーバー移行作業及びDNS設定変更作業は、協議会と協議の上、受託者が主体となって実施すること。

ウ サイト構造の変更に伴い、主要な既存ページから新ページへの適切なリダイレクト設定（301リダイレクト等）を行い、ユーザーの利便性と検索エンジン（SEO）の評価を維持すること。

（5）インターンシップ後のフォロー

ア 山口県インターンシップ推進協議会にて定める就業体験実施要領（<https://www.y-internship.com/wp-content/uploads/2025/03/outline2025.pdf>）を踏まえ、インターンシップ終了後のフォロー施策についても、可能であれば本業務の提案に含めること。

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

本ホームページ及びマッチング支援ツールは、構築後、協議会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

（1）受託者は、本ホームページ及びマッチング支援ツールの構築完了後（令和9年2月末を目途とする）、令和9年3月を試行運用及び習熟期間とし、管理方

- 法、更新手順、システム構成等について操作マニュアルを作成し、十分な説明及び引継ぎを行うものとする。
- (2) この期間中に発見された軽微な修正や設定変更については、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

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。

13 スケジュール

本業務は、契約締結後、速やかに着手するものとし、概ね次の工程及び時期を目安として実施すること。

ただし、各工程の内容については、本業務の規模及び目的に応じた範囲で実施するものとする。

なお、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、協議の上決定する。また、進捗状況により変更が必要となった場合は、委託者及び受託者が協議の上、これを変更する。

	8月	9月	10月	11月	12月	1月	2月	3月
要件定義								
サイト設計								
デザイン作成								
テンプレート作成								
システム設計								
システム構築								
データ移行								
テスト・運用調整								
完成								
仮運転（試行運用）								
操作研修								
本番公開準備・引継ぎ								

※令和9年3月は、次年度の本番運用に向けた試行運用・操作習熟期間とする。本格的な稼働開始は令和9年4月1日を予定している。

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。

- (1) 試行運用開始前（令和9年2月末日）までに提出するもの

- ア システム設計書一式（システム概要、基本設計書、詳細設計書等）
- イ 操作マニュアル及び引継ぎ資料（緊急時の対応手順等を含む）

- (2) 業務完了時（令和9年3月末日）までに提出するもの

- ア システム関連データ一式（本番稼働時のプログラムソースコード、デザインデータ等）

- イ ウェブアクセシビリティ試験結果報告書
- ウ Webアプリケーション脆弱性診断結果報告書
- エ 業務完了報告書

15 実施体制

業務を円滑に遂行するため、委託者及び関係機関との連携・調整を行う実施体制を構築すること。

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) 委託業務の性格上、利用者の個人情報を取り扱うことから、受託者はこの業務に従事する職員に対して守秘義務を課すこと。この守秘義務は、この業務終了後においても同様とすること。
- (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

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 及びレベル AA 全て。（詳細は「山口県目標達成基準」（別紙 1）のとおり）

3 対象範囲

本業務で制作するウェブサイト (<https://www.y-internship.com/>) 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、「a) 全てのウェブページを選択する場合」にある方法を用いて、試験を実施すること。

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

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) 利用者認証を経し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られ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ун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と呼び出した場合 (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ун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。

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ト脆弱性 (意図しないリダイレクト)
16	クローラへの耐性

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、甲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ことを問わず、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。