独立行政法人国立高等専門学校機構
女子学生向けキャリア形成支援 Web サイト
構築・保守及びコンテンツ制作業務
一式　仕様書

令和５年８月

独立行政法人国立高等専門学校機構

１．件名

独立行政法人国立高等専門学校機構女子学生向けキャリア形成支援 Web サイト
構築・保守及びコンテンツ制作業務　一式

２．業務範囲

本委託作業の業務範囲は次のとおりとする。

（１） Web ページの構築（Web ページ用サーバの用意も含む）
（２） コンテンツ制作
（３） 保守管理
（４） その他

３．契約期間

契約締結日から令和８年３月３１日までとする。
期間内のスケジュールについては以下のとおりとする。

（１） Web ページの構築（サーバの用意含む）及びコンテンツ制作
　　契約締結日から令和６年１月３１日までに行うこと。
（２） 保守管理業務
　　Web サイト構築完了日から令和８年３月３１日まで行うこと。

４．本業務の目的

４－１．概要

OECD(2021.09)のデータによると、高等教育機関に入学した学生のうち、理系分野に占める女性の割合は OECD 加盟国の中で日本が最も低く、「ロールモデルが少ない」など女子学生のキャリア形成に関する問題が多いことから、現役女子学生・OG のネットワークの形成や高等専門学校（以下、「高専」とする）OG の卒業後のキャリア形成の可視化を行う Web サイトを構築し、女子学生のキャリア形成を支援するとともに、活躍する現役女子学生・OG の姿を発信して、女子学生獲得（女性技術者の増加）へつなげることを目的としている。

４－２．基本方針

受注者は以下の項目を十分に理解した上で業務を実施すること。

（１）高専 OG の活躍を通じロールモデルを見せることで、女子学生のキャリア選択に役立てるものとする。
（２）今学んでいることがどう将来につながっているかを伝え、キャリア形成を支援するものとする。
（３）現役学生が活躍している OG との交流を通じて不安を解消し、より充実した高専生活を送れるものとする。

（4）現役女子学生だけでなく、入学者を増やすコンテンツにつなげるものとする。
（5）卒業・修了した高専 OG 情報のデータをできるだけ多く集約し、出身高専や学科、卒業年度等で検索できるものとする。
（6）掲載している OG 情報は、キャリアの更新に合わせ随時、国立高等専門学校機構（以下、「機構」とする）及び OG 自身が編集できるものとする。
（7）Web サイト運用開始後、機構において、大きな費用負担なく維持管理ができるものとする。

５．要求要件

５－１．サーバの用意と Web サイトの構築について（基本的要件）

（1） 「４．本業務の目的」を満たすサイトの構成・デザインの提案・作成を行うこと。その際、Web サイト全体で統一化されたデザインにすること。また、トップページの他、第２階層以下のページについてもデザインを提示すること。なお、想定しているサイトの構成例「（資料１）サイトマップ」を参照のこと。【必須】【優れている場合加点】
（2） レスポンシブ Web デザインであること。スマートフォンからアクセスがあった場合は、スマートフォン用ページが開き、PC（タブレット）からアクセスがあった場合は、PC 用ページが開くようにする。スマートフォンからのアクセスを考慮して、デザイン・レイアウトのためにフレームやテーブルを用いないものとする。【必須】
（3） 高専関係者のみが閲覧できる情報と一般に公開できる情報を切り分け、表示できるものとすること。【必須】
（4） JIS X 8341-3:2016 のウェブアクセシビリティ適合レベル A 以上に配慮して作成されていること。【必須】
（5）年間 250 万円未満で継続して、「５－３．保守管理について」の記載事項と同様の保守管理が行えること。【必須】
（6） OG 情報の編集は、随時 OG 自身が行うことを想定している。CMS 機能の導入等、OG 自身が編集作業を行える仕組みとすること。【必須】
（7）OG 情報の編集がされたとき、承認しなければ編集内容が反映されない仕組みとし、承認を行うための管理用アカウントを用意すること。また、管理用ライセンスアカウントの追加発行等に対応すること。【必須】
（8）OG 情報の検索機能は高専関係者等、任意のユーザのみが利用できる仕組みにすること。【必須】
（9） 「４．本業務の目的」を満たす有益な提案があれば、提案すること。【任意】【優れている場合加点】
（１０）令和６年１月３１日までに、サイトマップ等 Web サイトの構成情報を電子デー

タで納入すること。【必須】

（１１）Web サイトの運用マニュアルを Word もしくは PowerPoint 形式で編集可能な電子ファイルで令和６年１月３１日までに１部、納入すること。

なお、運用マニュアルには以下のものを含めることとする。【必須】

①　管理マニュアル

・サイトマップ

・管理者機能(アカウントの作成・管理方法)

・コンテンツの修正・公開方法

②　ユーザ（情報登録者向け）マニュアル

・情報登録するコンテンツの入力・編集方法

(文字入力、画像貼り付け、その他注意すべきこと)

※ユーザマニュアルは利用者が分かり易いように、図付きの構成とすること。

５－２．コンテンツ制作および Web サイトの管理・運用について【必須】

（１）　「４. 本業務の目的」を踏まえた上で、以下のコンテンツの提案・制作をすること。

【優れている場合加点】

・「(資料２）高専 OG 情報」に記載されている指示を満たすコンテンツ

・チャットスペース等、現役女子学生同士や高専 OG と交流が図れるコンテンツ

（２）　インタビュー記事や動画等の新規コンテンツの追加を想定したものであること。

（３）　（２）で例示したコンテンツの追加や各種情報の修正・変更等について、随時対応できること。

（４）　「６－１．対応ブラウザ」に挙げる Web ブラウザソフトで操作できるものであること。

（５）　プラグインを利用する場合はその予定のプラグイン一覧を提示すること。

（６）　更新履歴・承認履歴を管理できること。

（７）　YouTube 等にアップロードした動画をページに埋め込んで、動画のインライン再生ができること。

（８）　高専関係者のみが閲覧できる情報等にアクセス可能なユーザの管理ができること。

５－３．保守管理について【必須】

（１）保守管理体制

保守に関する責任者及び担当者を定め、保守管理体制図として提出すること。

（２）障害対応

Web サイトに障害が発生した場合、速やかに復旧作業を実施し、機構へ対応内容を報告すること。なお、復旧には自動復旧システムを使っても差し支えないものとする。

障害発生後の平日（国民の祝日に関する法律第３条に規定する休日及び１２月２９日

～１月３日の年末年始を除く月～金曜日）の 9 時～17 時の時間内に状況の把握、影響範囲の調査を行い、速やかに機構への報告及び再発防止に努めること。

（３）Web ページのデザインの軽微な変更

Web ページのデザインの軽微な変更(ボタンの追加・画像の位置変更・プラグイン追加 等)に対応すること。なお、機構からの変更要求が軽微か否かについては都度機構と受注者にて協議することとする。

（４）ユーザ管理

高専関係者のみが閲覧できる情報等にアクセス可能なユーザ情報の登録・修正・削除等の管理を行うこと。

（５）問い合わせ対応

Web サイトに係る機構からの以下の項目に関連する質問及び相談に真摯に対応すること。また、質問及び相談に対する回答は、対面もしくは、オンライン会議、電話、電子メールにて行うこと。

なお、問い合わせ対応時間帯は原則として平日（国民の祝日に関する法律第３条に規定する休日及び１２月２９日～１月３日の年末年始を除く月～金曜日）の 9 時～17 時とする。

(ア) ページの作成・更新に関する相談、支援

(イ) 各種不具合の原因、対策の調査

(ウ) Web サイト運用改善及び問題解決に有効な技術の調査、助言

(エ) デザインの簡易な修正・更新

(オ) 機構の指示に基づく指定コンテンツの更新

（６）業務完了報告書の提出

Web サイトの稼働状況、発生した障害の内容と対応状況等を記載した保守管理業務報告書を毎月末作成し、翌月初めに機構に提出すること。機構は提出された同報告書により検収を行うものとする。

（７）本業務を履行する上で、サーバや有料のプラグイン等の外部サービスを利用するために発生する費用は保守の費用に含めること。

５－４．セキュリティ要件【必須】

「別紙 情報セキュリティに関する事項」を遵守すること。

６．その他

６－１．対応ブラウザ【必須】

次に示す Web ブラウザにおいて、閲覧者及び機構担当者が適切に Web サイトを利用できること。なお、タブレット端末はパソコン用デザインを表示させ、各最新 OS の標準ブラウザ最新版で正しく表示できること。

	OS	ブラウザ
Web ブラウジング	Windows MacOS Android iOS	Edge FireFox Safari Google Chrome

６－２．著作権の帰属【必須】

（１） 入札時の提出物を除き、本件で作成されたドキュメント、データに関する一切の著作権（著作権法第 27 条及び第 28 条の権利を含む）は、受注者又は第三者が本件契約前から保有していた著作権又はフリー素材の著作権を除き、機構に帰属するものとする。

（２） 本件で作成されたドキュメント、データに関する一切の著作権について、機構又は機構が指定する第三者に対し、著作者人格権（公表権、氏名表示権、同一性保持権）を行使しない。

（３） 本件で作成されたドキュメント、データに第三者が権利を有する著作物（以下、「既存著作物」という。）が含まれる場合には、受注者は当該既存著作物の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続きを行うこと。また、著作権関係の紛争が生じた場合、受注者の責任において一切を処理するものとする。

６－３．第三者からの権利侵害【必須】

本仕様書に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争等が生じた場合は、当該紛争の原因が専ら機構の責に帰す場合を除き、受注者の責任、負担において一切を処理すること。

この場合、機構は係る紛争等の事実を知った時は、受注者方に通知し、必要な範囲で訴訟上の防衛を受注者方に委ねる等の協力措置を講じるものとする。

６－４．実績【任意】

以下の実績について、リスト（任意様式）をもって示すこと。【優れている場合加点】

・女性活躍推進を目的とした企画の運営実績。

・学生向けキャリア支援サイトの運営実績。

６－５．ワークライフバランス【任意】

女性の職業生活における活躍の推進に関する法律に基づく認定企業（えるぼし認定企業）、次世代育成支援対策推進法に基づく認定企業（くるみん認定企業等）及び、青少年の雇用の促進等に関する法律に基づく認定企業（ユースエール認定企業）については加

点するので、認定されていることが確認できる書面の写しを提出すること。【優れている場合加点】

６－６．疑義に関する協議

仕様書に記載されていない事項、法令により義務付けられている事項及びその他の事項についても、業務上当然必要な事項については、本業務の範囲に含まれるものとする。

なお、疑義が生じた場合には、機構と受注者で協議して定める。それにより、追加業務等が発生する場合は、契約係を通して発注するので、受注者はそれ以外の者からの発注や依頼を受け付けないこと。

以上

サイトマップ

■ WEBサイト

トップページ
・サイト概要
・ピックアップ情報

高専OG情報
出身高専や学科、卒業年度等での検索機能。
※登録ユーザと一般閲覧者で表示内容を変える

各OG情報ページ
キャリアの更新に合わせて、随時更新できる仕組みとする。

交流コンテンツ
現役女子学生同士や高専OGと交流が図れるコンテンツ
※登録ユーザのみ参加可能

登録ユーザー関連コンテンツ
※高専OG、現役女子学生がユーザ登録可能
・ユーザ登録、ログイン
・ユーザ登録情報の更新

その他、提案コンテンツや必要とされるページ、機能 等

利用

登録・更新

掲載情報等を管理

■ 管理機能

管理画面　※機構担当者及び保守担当者のみアクセス可能
・ユーザ管理
・コンテンツ管理
・その他、必要とされる機能

女子学生向けキャリア形成支援Webサイト　サイトマップ

WEBサイト	
トップページ	サイトの概要、ピックアップ情報、各コンテンツへのリンクなど
高専OG情報	出身高専や学科、卒業年度等での検索機能 登録ユーザと一般閲覧者で表示内容を変える 詳細は別紙「（資料１）高専OG情報」を参照
各OG情報ページ	集約したOGの情報を掲載 登録ユーザと一般閲覧者で表示内容を変える
交流コンテンツ	現役女子学生同士や高専OGと交流が図れるコンテンツ
登録ユーザー関連コンテンツ	※高専OG、現役女子学生がユーザ登録可能 ・ユーザ登録、ログイン ・ユーザ登録情報の更新 ・OG情報の登録・更新（OGのみ） ・交流コンテンツの利用　等
その他	提案コンテンツや必要とされるページ、機能 等

管理機能	
管理画面	※機構担当者及び保守担当者のみアクセス可能
ユーザ管理	
コンテンツ管理	
その他	必要とされる機能

（資料２）

高専ＯＧ情報

卒業・修了した高専 OG 情報のデータをできるだけ多く集約し、高専関係者等、任意のユーザのみが出身高専や学科、卒業年度等で情報を検索・表示できるものとするが、一般の閲覧者も個人が特定されない程度の情報（学科と職種、キャリアパスのみ等）を検索・表示できるものとする。

また、集約した情報は、キャリアの更新に合わせて、機構担当者の負担なく、随時更新できる仕組みとする。

〇集約するデータについては以下のとおりとする。【必須】

・氏名(※)
・ニックネーム
・顔写真（アイコン含む）
・連絡先（メールアドレス・電話番号）(※)
・出身高専名
・出身学科名（コース・専攻等含む）
・卒業・修了年度
・卒業・修了時の進路選択（進学・就職）
・現在までのキャリアパス（進路選択がわかるように）
（例）・高専本科卒→大学編入学(〇〇学科)→大学院進学（〇〇専攻）→就職（研究開発部門）
・高専本科卒→高専専攻科進学（〇〇コース）→大学院進学（〇〇専攻博士課程〇年）
・高専本科卒→就職（製造部門）→品質管理部門リーダー
・現在の職種（業種）
・現住所（都道府県のみ）
・現役学生に向けたメッセージ
（※）氏名、連絡先については、Web ページでは非公開を想定。

〇以下に例示するような内容も集約できるものとする。

・研究内容
・部活動・サークル等
・高専時代の一番の思い出
・高専時代にがんばったこと
・高専での学びとの共通点
・今の仕事内容（役職・ポジション含む）
・趣味
・SNS などのアカウント情報

〇検索項目については以下のとおりとする。【必須】

・出身高専
・出身学科（コース・専攻等含む）
・卒業・修了年度
・卒業・修了時の進路選択（進学・就職）
・現在の職種（業種）
・現住所

別紙

情報セキュリティに関する事項

以下の事項について遵守すること。

1. 受注者は、一般社団法人情報マネジメントシステム認定センター、公益財団法人日本適合性認定協会、もしくはその他認定機関により認定された審査登録機関による ISO/IEC27001 又は JIS Q 27001 または、一般財団法人日本情報経済社会推進協会からプライバシーマーク制度によるプライバシーマーク（JISQ15001）の認証を受けていること。
2. 受注者は、本事業に使用するソフトウェア、電子計算機等に係る脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じるとともに、契約期間中にこれらの対策に関する情報セキュリティ教育を本事業にかかわる従事者に対し実施すること。
3. 受注者は、本作業の遂行において、情報セキュリティが侵害され又はそのおそれがある場合の対処方法について担当職員に提示すること。また、情報セキュリティが侵害され又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従うこと。
4. 受注者は、情報セキュリティの確保を目的とした体制を整備し契約締結後速やかに機構に提示すること。報告する体制には、以下の情報を含めること。また、体制が変更になった場合は速やかに機構へ報告を行うこと。
   (ア) 受注者の資本関係・役員等の情報
   (イ) 本事業の実施場所
   (ウ) 本事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報
5. 受注者は、本サービスにおける情報セキュリティ対策が適切に履行されていることを、定期的に書面にて機構に提出すること。また、情報セキュリティ対策が不十分だったことが判明した場合、受注者の責において適切な対策を講ずること。
6. 受注者は、情報セキュリティインシデントが起こった際の対応手順を、応札時に機構に提示すること。
7. 情報セキュリティインシデント発生時には必要に応じて機構の情報セキュリティ監査を受け入れるとともに、指摘事項への対応を行うこと。
8. 受注者は、政府機関等のサイバーセキュリティ対策のための統一基準群（「政府機関等のサイバーセキュリティ対策のための統一規範」、「政府機関等のサイバーセキュリティ対策の運用等に関する指針」、「政府機関等のサイバーセキュリティ対策のための統一基準」及び「政府機関等の対策基準策定のためのガイドライン」の総称）（以下、これらを総称して「統一基準群」という。）を踏まえた情報セキュリティ対策を実施

する。また、契約締結時に規程等が改正されている場合は、改正後の規程等を遵守すること。

9. 受注者は、外部公開ウェブサイト（以下「ウェブサイト」という。）を構築又は運用するプラットフォームとして、受注者自身（再委託（事業の一部を第三者に委託することをいい、外注及び請負を含む。以下同じ。）先を含む。）が管理責任を有するサーバ等を利用する場合には、ＯＳ、ミドルウェア等のソフトウェアの脆弱性情報を収集し、セキュリティ修正プログラムが提供されている場合には業務影響に配慮しつつ、速やかに適用を実施すること。また、ウェブサイト構築時においてはサービス開始前に、運用中においては年１回以上、ポートスキャン、脆弱性検査を含むプラットフォーム診断を実施し、脆弱性を検出した場合には必要な対策を実施すること。
10. 受注者は、ウェブサイト上のウェブアプリケーションの構築又は改修を行う場合には、独立行政法人情報処理推進機構が公開する最新の「安全なウェブサイトの作り方」（以下「作り方」という。）に基づくこと。また、構築又は改修したウェブアプリケーションのサービス開始前に、「作り方」に記載されている脆弱性の検査等（ウェブアプリケーション診断）を実施し、脆弱性を検出した場合には必要な対策を実施すること。併せて、「作り方」のチェックリストに従い対応状況を確認し、その結果を記入したチェックリストを担当職員に提出すること。なお、チェックリストの結果に基づき、担当職員から指示があった場合は、それに従うこと。
11. 受注者は、ウェブサイト上のウェブアプリケーションの構築又は改修を行う場合には、以下の脆弱性を含めないこと。
    (ア) SQL インジェクション脆弱性
    (イ) OS コマンドインジェクション脆弱性
    (ウ) ディレクトリトラバーサル脆弱性
    (エ) セッション管理の脆弱性
    (オ) アクセス制御欠如と認可処理欠如の脆弱性
    (カ) クロスサイトスクリプティング脆弱性
    (キ) クロスサイトリクエストフォージェリ脆弱性
    (ク) クリックジャッキング脆弱性
    (ケ) メールヘッダインジェクション脆弱性
    (コ) HTTP ヘッダインジェクション脆弱性
    (サ) eval インジェクション脆弱性
    (シ) レースコンディション脆弱性
    (ス) バッファオーバーフロー及び整数オーバーフロー脆弱性
    (セ) サーバサイドリクエストフォージェリ（SSRF）脆弱性
12. 受注者は、ウェブサイトを構築又は運用する場合には、インターネットを介して通信する情報の盗聴及び改ざんの防止並びに正当なウェブサーバであることを利用者が確

認できるようにするため、TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講じること。なお、必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること。

13. 受注者は、ウェブサイトを構築する場合、公開が終了したコンテンツをサーバから自動削除する機能を設けること。

14. 受注者は、ウェブサイト又は電子メール送受信機能を含むシステムを構築又は運用する場合には、原則、政府機関のドメインであることが保証されるドメイン名「.go.jp」（以下「政府ドメイン名」という。）を使用すること。なお、政府ドメイン名を使用しない場合には、第三者による悪用等を防止するため、事業完了後、一定期間ドメイン名の使用権を保持すること。

15. 受注者は、情報システム（ウェブサイトを含む。以下同じ。）の設計、構築、運用、保守、廃棄等（電子計算機、電子計算機が組み込まれた機器、通信回線装置、電磁的記録媒体等のハードウェア又はソフトウェア（以下「機器等」という。）の調達を含む場合には、その製造工程を含む。）を行う場合には、以下を実施すること

(ア) 機構等の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。

(イ) 本調達に係る機器等の開発におけるライフサイクルにおいて、不正な変更が加えられない管理がなされていること。また、機構が求めた場合、管理体制の確認に応じること。

(ウ) 不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。

(エ) 情報セキュリティ対策による情報システムの変更内容について、担当職員に速やかに報告すること。また、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等、他の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を含めること。

(オ) サポート期限が切れた又は本事業の期間中にサポート期限が切れる予定がある等、サポートが受けられないソフトウェアの利用を行わない及びその利用を前提としないこと。また、ソフトウェアの名称・バージョン・導入箇所等を管理台帳で管理することに加え、サポート期限に関するものを含むソフトウェアの脆弱性情報を収集し、担当職員に情報提供するとともに、情報を入手した場合には脆弱性対策計画を作成し、担当職員の確認を得た上で対策を講ずること。

(カ) 電子メール送受信機能を含む場合には、ＳＰＦ（Sender Policy Framework）等のなりすましの防止策を講ずるとともに、SMTPによるサーバ間通信のTLS（SSL）化やS/MIME等の電子メールにおける暗号化及び電子署名等により保護すること。

(キ) アクセスログ、認証ログ、システムログ、システムへのログイン履歴及び操作ログについて１年以上保持すること。また、機構担当者から依頼があった場合に、これを提供すること。

16. システムに投入された情報は災害や情報セキュリティインシデント等に備え、復元可能な形で、システムから物理的かつ論理的に隔離された場所に保管すること。
17. システムの利用者、管理者等の全てのアカウントに対して多要素認証の利用を強制すること。
18. 本システムでパスワードを使用する場合、高専機構パスワードに準拠したものとすること。
19. 受注者は、本事業を実施するに当たり、約款による外部サービスやソーシャルメディアサービスを利用する場合には、それらサービスで要機密情報を扱わないことや不正アクセス対策を実施する等規程等を遵守すること。
20. 受注者は、ウェブサイトの構築又はアプリケーション・コンテンツ（アプリケーションプログラム、ウェブコンテンツ等の総称をいう。以下同じ。）の開発・作成を行う場合には、利用者の情報セキュリティ水準の低下を招かぬよう、以下の内容も含めて行うこと。

(ア) 提供するウェブサイト又はアプリケーション・コンテンツが不正プログラムを含まないこと。また、そのために以下を含む対策を行うこと。

① ウェブサイト又はアプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。

② アプリケーションプログラムを提供する場合には、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認すること。

③ 提供するウェブサイト又はアプリケーション・コンテンツにおいて、機構外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、ＨＴＭＬソースを表示させる等して確認すること。

(イ) 提供するウェブサイト又はアプリケーションが脆弱性を含まないこと。

(ウ) 実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラム形式でコンテンツを提供しないこと。

(エ) 電子証明書を用いた署名等、提供するウェブサイト又はアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをウェブサイト又はアプリケーション・コンテンツの提供先に与えること。なお、電子証明書を用いた署名を用いるときに、UPKI の利用が可能である場合は、UPKI により発行された電子証明書を用いて署名を施すこと。

(オ) 提供するウェブサイト又はアプリケーション・コンテンツの利用時に、脆弱性が

存在するバージョンのＯＳやソフトウェア等の利用を強制する等の情報セキュリティ水準を低下させる設定変更を、ＯＳやソフトウェア等の利用者に要求することがないよう、ウェブサイト又はアプリケーション・コンテンツの提供方式を定めて開発すること。

(カ) 機構外へのアクセスを自動的に発生させる機能やサービス利用者その他の者に関する情報が本人の意思に反して第三者に提供される等の機能がウェブサイト又はアプリケーション・コンテンツに組み込まれることがないよう開発すること。ただし、必要があって当該機能をウェブサイト又はアプリケーション・コンテンツに組み込む場合は、機構外へのアクセスが情報セキュリティ上安全なものであることを確認した上で、他のウェブサイト等のサーバへ自動的にアクセスが発生すること、サービス利用者その他の者に関する情報が第三者に提供されること及びこれらを無効にする方法等が、サービス利用者において容易に確認ができるよう、担当職員が示すプライバシーポリシー等を当該ウェブサイト又はアプリケーション・コンテンツに掲載すること。

21. 受注者は、サプライチェーン・リスクの要因となる脆弱性を発生させない又は増大させないための管理体制を構築すること。また、契約締結後速やかに情報セキュリティの確保を目的とした体制を整備し、機構に提示すること。報告する体制には、以下の情報を含めること。また、体制が変更になった場合は速やかに機構へ報告を行うこと。

(ア) 管理体制図

(イ) 受注者の資本関係・役員等の情報

(ウ) 事業の実施場所

(エ) 事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報

22. 受注者は、機構がサプライチェーン・リスクに係る情報セキュリティインシデントを認知した場合又はその疑いが生じた場合に、必要に応じて業務内容、作業プロセス又は成果物を立ち入り検査等で機構が確認することを了承すること。

23. 本業務において機構がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、リスク低減対策等、機構と迅速かつ密接に連携し提案の見直しを図ること。

24. 受注により知り得た全ての情報について守秘義務を負うものとし、これを第三者に漏らし、又は他の目的に使用しないこと。

25. 受注により知り得た情報については、契約期間はもとより、契約終了後においても第三者に漏らしてはならない。

26. 正当な理由があってやむを得ず第三者に開示する場合、書面によって事前に機構の承諾を得ること。また、情報の厳重な管理を実施すること。

27. 受注者は、業務完了後、本件に係る情報を返却または抹消し、そのことを機構に書面

で報告すること。

28. 機構が提供した資料は、原則として全て複製禁止とすること。但し、業務上やむを得ず複製する場合であって、事前に書面にて機構の許可を得た場合はこの限りではない。なお、この場合にあっても使用終了後はその複製を機構本部に返納又は焼却・消去する等適切な措置をとり、機密を保持すること。
29. 機器のリースを行う場合、機器の返却後、機器における電磁的記憶媒体の全ての情報を抹消すること。また、そのことを書面で報告すること。
30. 運用・保守業務においてセキュリティ対策により、システムに変更を行った場合は、速やかに機構に報告すること。
31. クラウドサービスとして提供される場合、経済産業省による「政府情報システムのためのセキュリティ評価制度（ISMAP)」に登録されたサービスであること。もしくは、本サービスが、経済産業省が定める ISMAP-LIU（ISMAP for Low-Impact Use）に登録されていること。
32. サービスの準拠法は日本の法律であること。また、管轄裁判所を日本国内の裁判所とすること。
33. サービスにおいて、本校の情報は国内のみで取り扱われること。
34. 本案件に係る情報は、日本法令のみが適用される環境のみで取り扱うこと。
35. 受注者は本業務を自ら履行するものとし、本業務の全部を第三者に委託、又は請け負わせてはならない。ただし、本業務の一部を第三者に委託する場合であり、かつ、機構に書面によって外部委託の詳細を提出し許可された場合は、この限りではない。なお第三者委託を許可された場合であっても、受注者は契約による責任を免れることはできない。
36. 受注者は、本事業を再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記 1. ～34. の措置の実施を契約等により再委託先に担保させること。また、4.の確認書類には再委託先に係るものも含むこと。

その他、遵守すべきガイドライン等

1. デジタル・ガバメント推進標準ガイドライン
   https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/8a3b6203/20230331_resources_standard_guidelines_guideline_01.pdf
2. 「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」
   https://www.nisc.go.jp/pdf/policy/general/SBD_manual.pdf
3. 政府機関の情報セキュリティ対策のための統一基準群

(ア)政府機関の情報セキュリティ対策のための統一規範
https://www.nisc.go.jp/pdf/policy/general/kihanr5.pdf
(イ)政府機関等の情報セキュリティ対策のための統一基準
https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf
(ウ)政府機関等の対策基準策定のためのガイドライン
https://www.nisc.go.jp/pdf/policy/general/guider5.pdf
4. サイバーセキュリティ 2023
https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023.pdf
5. 安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity/about.html
6. OWASP Japan | OWASP Foundation
https://owasp.org/www-chapter-japan/