**令和７年度経済産業省デジタルプラットフォーム構築事業**

**（中小企業等経営強化法に基づく経営力向上計画申請プラットフォームの改修・保守運用業務）**

**調達仕様書（案）**

中小企業庁事業環境部企画課

目次

[１ 調達案件の概要 3](#_Toc173499843)

[(1) 調達件名 3](#_Toc173499844)

[(2) 調達の背景 3](#_Toc173499845)

[(3) 調達目的及び調達の期待する効果 3](#_Toc173499846)

[(4) 業務・情報システムの概要 3](#_Toc173499847)

[(5) 契約期間 5](#_Toc173499848)

[(6) 作業スケジュール 5](#_Toc173499849)

[２ 情報システムに求める要件 5](#_Toc173499850)

[(1) インタフェース要件 6](#_Toc173499851)

[(2) データ定義 6](#_Toc173499852)

[(3) 認証機能要件 6](#_Toc173499853)

[(4) 規模・拡張性 6](#_Toc173499854)

[(5) 利用者数、アクセス数及びアクセス方式 6](#_Toc173499855)

[３ 作業の実施内容 7](#_Toc173499856)

[(1) プラットフォームの保守・運用 7](#_Toc173499857)

[(2)プラットフォームの改修 9](#_Toc173499858)

[(3)システムの引継ぎ 10](#_Toc173499859)

[(4)認定事業者等へのアンケート調査及び分析 11](#_Toc173499860)

[(5)成果物 11](#_Toc173499861)

[４ 作業の実施体制・方法 13](#_Toc173499862)

[(1)作業要員に求める資格等の要件 13](#_Toc173499863)

[(2) 作業の実施場所 14](#_Toc173499864)

[５ プロジェクトの管理 14](#_Toc173499865)

[(1) プロジェクト計画に関する事項 14](#_Toc173499866)

[(2) 定例会等の実施 14](#_Toc173499867)

[６ 作業の実施に当たっての留意事項 15](#_Toc173499868)

[(1) 情報セキュリティ 15](#_Toc173499869)

[(2)機密保持、資料の取扱い 15](#_Toc173499870)

[(3)個人情報の取扱い 17](#_Toc173499871)

[(4)法令等の遵守 17](#_Toc173499872)

[(5)標準ガイドラインの遵守 18](#_Toc173499873)

[(6)契約金額内訳及び情報資産管理標準シートの提出 18](#_Toc173499874)

[７ 成果物の取扱いに関する事項 18](#_Toc173499875)

[(1) 知的財産権の帰属 18](#_Toc173499876)

[(2) 契約不適合責任 19](#_Toc173499877)

[(3) 検収 20](#_Toc173499878)

[８ 入札参加資格に関する事項 20](#_Toc173499879)

[(1) 競争参加資格 20](#_Toc173499880)

[(2) 受注実績等 20](#_Toc173499881)

[９ 附属文書 21](#_Toc173499882)

[情報セキュリティに関する事項 22](#_Toc173499883)

[情報取扱者名簿及び情報管理体制図 32](#_Toc173499884)

[法人インフォメーションとの連携 34](#_Toc173499885)

[中小企業支援プラットフォームとの連携 35](#_Toc173499886)

1. 調達案件の概要
2. 調達件名

令和７年度経済産業省デジタルプラットフォーム構築事業（中小企業等経営強化法に基づく経営力向上計画申請プラットフォームの改修・保守運用業務）

1. 調達の背景

平成２８年に創設された中小企業等経営強化法に基づく経営力向上計画は、国が定める事業分野別指針に沿って人材育成、コスト管理等のマネジメントや設備投資など経営力を向上させる計画であるが、特定事業者等は本計画を作成し、業種ごとの各主務大臣（各省庁の地方支分部局長等）に申請し、認定を受けることで、取得設備に関する即時償却等の税制措置や金融支援措置等を受けることができる。令和６年４月末現在、約１７万者が経営力向上計画の認定を受けている。

中小企業庁は、平成３０年度にプラットフォームを構築し、申請者（ただし、提出先を経済産業局（沖縄経済産業部を含む。）のみとする申請を行う者に限る。）が、Ｗｅｂ画面上で計画申請に係る必要事項を入力した申請書を印刷したものに押印して申請できる計画申請電子化システム（試行版）の運用を平成３１年１月に開始した。その後、令和元年度に本格運用用のプラットフォームを構築し、電子申請対応をする省庁が所管する業種のみの事業者はＷｅｂ画面上で計画申請に係る必要事項を入力すれば電子申請が可能となり、電子申請対応をしない省庁が所管する業種の事業者はプラットフォームで申請書を作成できる現行システムの運用を令和２年４月に開始した。

経済産業省宛ての申請については、電子化の推進により、現在、約７割が電子申請となっている。また関係省庁へも電子申請率を増加させるべく働きかけており、警察庁、金融庁、総務省、文部科学省、厚生労働省、農林水産省、国土交通省及び環境省が現行システムを利用した電子申請に対応している。

1. 調達目的及び調達の期待する効果

本事業では、事業者のニーズや制度の利用状況を踏まえつつ、現行システムの保守・運用及び改修を行うことで、経営力向上計画の申請手続き等の電子化をさらに進めることにより、形式的なミスの軽減を図り、経営力向上計画を作成・申請する特定事業者等の作業負担を軽減することや、経済産業局等の審査事務の効率化・迅速化を図ることを目的とする。

1. 業務・情報システムの概要

プラットフォームは、経営力向上計画の申請者が、法人共通認証基盤（ＧビズＩＤ）で取得したＩＤ、パスワードを利用してログインすることができ、経営力向上計画の申請書の必要記載事項（※）を入力して申請することが可能である。

※申請書の必要記載事項：中小企業等経営強化法及び関係政省令（中小企業等経営強化法施行令、中小企業等経営強化法施行規則及び経営力向上に関する命令）並びにその他関連文書（経営力向上計画策定の手引き等）で定められたもの。

プラットフォームは、以下の機能と連携可能である。

①ＧビズＩＤの提供する機能等：

<https://gbiz-id.go.jp/top/system_guide/system_guide.html>参照

②法人インフォメーションとの連携：別添３参照

③中小企業支援プラットフォームとの連携：別添４参照

経営力向上計画プラットフォームの全体概要は図１のとおり。

（図１）経営力向上計画プラットフォームの全体概要



経営力向上計画の申請及び認定の内容は、プラットフォームのデータベースに蓄積することができる。申請者が変更申請を行う場合、プラットフォームのデータベースに蓄積された情報を利用することを可能とする機能を備えている。

経営力向上計画の適切な運用を実施する上の関係者は表１のとおり。

（表１）経営力向上計画の適切な運用を実施する上の関係者

|  |  |
| --- | --- |
| 関係者 | 関係性 |
| ①特定事業者等 | ・経営力向上計画の申請主体 |
| ②中小企業庁事業環境部企画課（以下「企画課」という。） | ・経営力向上計画制度の執行に関し、各経済産業局及び関係省庁のとりまとめ |
| ③経済産業局 | ・計画申請の受付、審査及び認定・過去の認定情報の検索、閲覧及び抽出・経営力向上設備（Ｂ類型）、デジタル化設備（Ｃ類型）、経営資源集約化に資する設備（Ｄ類型）等に係る投資計画の確認書の発行・報告書の受領 |
| ④関係省庁（地方局を含む。） | ・計画申請の受付、審査及び認定・過去の認定情報の検索、閲覧及び抽出 |
| ⑤関係工業会 | ・経営力向上設備等の生産性向上要件証明書の発行 |
| ⑥認定経営革新等支援機関 | ・申請者が計画を作成する際の支援 |
| ⑦市町村、各都道府県税事務所及び税務署 | ・申請者が計画認定に伴う税制措置を利用する場合、認定書等を受領 |

1. 契約期間

令和７年４月１日から令和８年３月３１日まで

1. 作業スケジュール

作業スケジュールは次のとおり想定している。

（図２）　作業スケジュール

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ４月 | ５月 | ６月 | ７月 | ８月 | ９月 | 10月 | 11月 | 12月 | １月 | ２月 | ３月 |
| プラットフォームの保守・運用 |  |  |  |  |  |  |  |  |  |  |  |  |
| プラットフォームの改修 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 | 　 |
| 認定事業者等へのアンケート調査及び分析 |  |  |  |  |  |  |  |  |  |  |  |  |

1. 情報システムに求める要件
2. インタフェース要件

法人インフォメーション等の連携するシステムのＡＰＩ要件によって他のシステムと連携することを視野に入れること。

1. データ定義

データ定義については、中小企業庁が提示する中小事業者データの項目を参照の上、企画課と協議をし、決定すること。

1. 認証機能要件

ＧビズＩＤでユーザー認証を行うこと。

1. 規模・拡張性

プラットフォームの規模、拡張性要件は表２のとおり。

なお、本事業は現在運用しているプラットフォームを引き続き運用するものであるが、電子申請の認知度向上等により、業務量、ユーザー数及びアクセス数が想定より増加した場合にも、対応できるプラットフォームを提案すること。

（表２）プラットフォームの業務処理量想定（令和７年度）

|  |  |  |
| --- | --- | --- |
| 項目 | 単位時間当たり処理件数 | 補足 |
| 定常時 | ピーク時 |
| サイトへの訪問者数 | 409人/1日 | ３月の営業日526件/1日 |  |
| ページビュー数 | 25,210件/1日 | ３月の営業日30,257件/1日 |  |
| 申請書作成数 | 69件/1日 | ３月の営業日85件/1日 |  |

1. 利用者数、アクセス数及びアクセス方式

本プラットフォームで想定される利用者（ユーザー）数、同時アクセス数等は表３のとおり。

（表３）申請電子化ユーザー数、アクセス数等（令和７年度）

|  |  |  |  |
| --- | --- | --- | --- |
| 利用者 | 利用者数 | 利用時間帯 | アクセス方式 |
| 一般ユーザー | 不特定多数 | 365日24時間 | インターネット |
| 中企庁、経産局及び他省庁（地方局を含む。）のプラットフォーム運用担当者等 | 500 | 365日24時間 | インターネット |

1. 作業の実施内容
2. プラットフォームの保守・運用

ＧビズＩＤとの連携により、特定事業者等が固有のＩＤを利用して、オンライン上で、申請書の作成のみならず、申請を行うことができる本プラットフォームを引き続き保守・運用する。

作業は、「デジタル・ガバメント推進標準ガイドライン」（2024年（令和６年）5月31日改定）（以下、「標準ガイドライン」という。）第３編第９章「運用及び保守」に準拠して実施すること。

運用保守状況に合わせ、運用保守計画書等の作成・更新を行うこと。

①審査担当者のサポート

企画課の指示に基づき、審査担当者等からの操作の質問に対するサポート及び操作トラブルへの対処並びにデータ訂正等のデータベース操作等を行う。

発生時から対応完了までを２営業日程度とする。

②システム稼働確認及び障害発生時の対応

（ア）プラットフォームが正常に稼働することを確認する。

（イ）プラットフォームは、申請者からの申請受付機能等は年末年始、メンテンナンス期間を除き、２４時間３６５日稼動する。

（ウ）プラットフォームで障害が発生した場合に、一次解析、原因解析、問題の解決等の一連の作業を行う。

（エ）プラットフォームのバックアップを管理するとともに、データ破損等の不慮の事態等が発生した場合には、バックアップデータからのリストアップ作業を行う。

③ＷＥＢサイト及びメールアドレスの管理並びにドメイン及びサーバ証明書の維持管理

プラットフォームの既存の事業者窓口ＷＥＢサイト及びプラットフォームから申請者や審査担当者へ自動送信されるメールアドレスの管理を行うとともに、ドメイン及びサーバ証明書の更新作業を実施すること。

④ライセンスの準備等

プラットフォームはSalesforce.com 上で構築されているが、「令和６年度経済産業省デジタルプラットフォーム構築事業（中小企業等経営強化法に基づく経営力向上計画申請プラットフォームの改修・保守運用・調査事業）（以下「令和６年度事業」という。）」の受注者から、本プラットフォームに係るSalesforce.comの環境・組織の引き継ぎを受け、令和７年４月１日以降も引き続き運用することとする。

ライセンスは、「２(4)規模・拡張性」に基づいた表４のアカウント種別等を用意すること。また中小企業庁が運営するミラサポｐｌｕｓ、ミラサポＣＯＮＮＥＣＴ等からＡＰＩ接続でアクセスするためのライセンスも用意すること。加えて、正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要な証跡を取得すること。

（表４）アカウント種別、アカウント数、ログイン数

|  |  |  |  |
| --- | --- | --- | --- |
|  | アカウント種別 | アカウント数 | ログイン数 |
| 1 | Lightning Platform - Unlimited Edition (Administrator) | 1 |  |
| 2 | Lightning Platform Plus - Unlimited Edition | 500 |  |
| 3 | Customer Community - Unlimited Edition - Logins |  | 13,000/月平均 |
| 4 | Additional 20 Objects for Customer Community |  | 13,000/月平均 |
| 5 | Event Monitoring | 1 |  |
| 6 | Field Audit Trail | 1 |  |

⑤プラットフォームの操作方法等に関する問合せ窓口の運用

特定事業者等に向けた申請電子化システム及び簡易版経営力向上報告機能の操作方法他に関する問合せ窓口を開設する。問合せ窓口の要件は以下のとおり。

ア　問合せ窓口の開設期間：令和７年４月１日～令和８年３月３１日

イ　問合せ対応時間：９：３０～１７：００（土日祝日及び年末年始（１２月２９日から1月３日まで）を除く）

ウ　問合せ手段：電話及びメール

エ　問合せ件数：最大５００件/月を想定。問合せに適切に応じるとともに、問合せの内容に応じて、改善要望の整理、報告を行う。

⑥ミラサポＣＯＮＮＥＣＴＡＰＩに関する保守・運用

「中小企業庁関連事業データ利活用ポリシー」を踏まえて、令和７年４月以降に経済産業局等のみに電子申請された経営力向上計画の（ア）認定書及び（イ）申請書における連携対象となっている項目について、ミラサポＣＯＮＮＥＣＴと円滑にデータ共有できるよう、ミラサポＣＯＮＮＥＣＴＡＰＩの保守・運用を行うこと。また、必要に応じて、ミラサポコネクト開発事務局と連携すること。

なお、想定外の事態が発生した場合には、適正な対処法を企画課に相談すること。

⑦クラウドのバージョンアップ対応

プラットフォームであるSalesforce.comのバージョンアップについて、事前検証作業および修正確認作業の上、本番環境への適切なバージョンアップ作業を行う。

⑧引継ぎ資料の作成

本案件終了後に次の運用・保守事業者に速やかな引継ぎを行えるよう、引継ぎ資料の作成・更新を行うこと。

(2)プラットフォームの改修

利便性向上や制度改正に対応するためにプラットフォームの機能等を改修する。

受注者は、改修要件を満たすための詳細設計を行い、成果物について当省の承認を得ること。

受注者は、改修内容に合わせ、単体テスト、結合テスト及び総合テストについて、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載したテスト計画書を作成し、当省の承認を得ること。

受注者は、設計工程の成果物及びテスト計画書に基づき、アプリケーションプログラムの改修、テストを行うこと。

なお、改修にあたっては、マニュアルの作成又は企画課が提供する既存マニュアルの修正を併せて行う。また改修の際は、必要に応じて、経済産業局及び関係省庁（以下「一部特定事業者等」という。）におけるテスト試行の支援、（１）⑤において設置する窓口等に寄せられた一部特定事業者等からの意見の受付・集約、システム等への反映等を行う。

改修項目は以下を予定しているが、制度改正や不具合対応などにより内容が増減することもありうる。

* + 1. 電子認定省庁の追加

追加した省庁が所管する申請について、事業者が入力した情報から認定書を自動生成し、事業者が、Experience CloudサイトであるプラットフォームからPDFファイルとしてダウンロードできるようにする。

ダウンロードされた場合、履歴を作成する。

申請が認定された際には、事業者に通知するメールを送信する。

追加した各省庁の認定書の固有の仕様に対応した機能を実装する。

* + 1. 所得拡大報告書画面の廃止

プラットフォームから、所得拡大促進税制の上乗せ措置に関連する画面・機能を削除する。

必要に応じて関連データのクレンジング作業等を実施し、他のデータ全体との整合性の保持や品質の確保をする。

* + 1. 発電設備等の報告書の接受機能追加

審査者が、報告書の入力画面で入力された発電設備等の報告書に関する情報を閲覧できるようにする。

関連するファイルが添付された場合、それを閲覧できるようにする。

また、事業者が入力した情報から報告書を自動生成し、審査者が審査画面上からPDFファイルとしてダウンロードできるようにする。

入力内容に不備がある場合には、事業者に対して補正の指示を出し、メールで通知することができるようにする。

* + 1. 発電設備等の報告書の入力画面追加

プラットフォーム上で、事業者が発電設備等の報告書に関する情報を入力することができるようにする。

仕様上必要であれば、ファイルの添付ができるようにする。

* + 1. 変更申請時の変更箇所表示機能追加

審査者が審査に利用する画面において、変更前申請と変更後申請との入力の変更部分を一覧表示する画面を新規に追加する。

* + 1. 変更申請時の前回申請書自動添付機能追加

変更申請時に直近の申請書を添付する画面でデータを連携させる。

* + 1. その他法令改正等による改修

各種法令改正（内容・時期は令和７年度内に適宜決定する）が確定してから、１カ月程度の開発期間でリリースできる体制を維持する。

(3)システムの引継ぎ

①Salesforce.comの環境・組織の引き継ぎにあたっては、セキュリティに係る漏洩に留意の上、引き継ぎに係る責任範囲・方法について受託者で検討を行い、令和６年度事業の受注者及び中小企業庁の承認を受けること。また、引継ぎに係る内容について令和６年度事業の受注者と協議・調整が必要となる場合は、本調達の事業者が主導のもと調整を行うこと。合意に係る調整責任及び引き継ぎに関する費用は本調達の事業者が負担すること 。

②令和８年度事業の受注者にシステム環境を引き継ぐことを想定し、以下の条件に同意すること。

・Salesforceの組織譲渡について、Salesforce社、令和７年度事業の受注者、令和８年度事業の受注者との間で結ばれる三者間契約に応じる。

③令和８年度事業において、本プラットフォームをSalesforce以外に移転する場合、Salesforce組織設定情報、登録データの抽出作業を実施すること。

④受注者は、他の運用事業者が本情報システムの運用を受注した場合には、次期運用事業者に対し、作業経緯、残存課題等についての引継ぎを行うこと。

(4)認定事業者等へのアンケート調査及び分析

①アンケート調査の実施

認定事業者等に対して、１回程度アンケートを行う。具体的な方法は以下の通り。

・アンケート対象：約１２万事業者（回答率目標：２割以上）

・アンケート方法：電子メール等を利用し、郵送は行わないこと。

・アンケート内容：経営力向上計画の申請（新規・変更）のためのプラットフォームの機能等についてのニーズや利用状況やその他の中小企業施策の利用状況等。

・アンケート方法：令和６年度事業のアンケート票などを参照の上、企画課に提案し、協議を行うこと。アンケート調査の設問数は全体で１回あたり50～80問程度を想定。

　　 　・アンケート送付先：企画課が提供する経営力向上計画の申請時に記載されている連絡先（メールアドレス）を使用すること。

②アンケート調査の分析

　　　　上記①のアンケート結果を取りまとめ、プラットフォームの機能及び電子申請をより使いやすくし、普及促進していくことにつなげるための分析や、その他の中小企業政策の利用状況についての評価等を行う。

(5)成果物

納入成果物は、以下のとおりとする。なお、納入成果物の詳細及び編集方法並びに納入期限等はこの仕様書の定めのあるほかについては、当省の担当職員と受注者が別途協議の上決定するものとする。また、以下に含まれていない場合であっても、当省の担当職員及び受注者が必要と認める場合はこの限りでない。

1. 調査報告書
2. 調査報告書電子媒体（ＣＤ－Ｒ、またはＤＶＤ－Ｒ） １式
	* 調査報告書、調査で得られた元データ、委託調査報告書公表用書誌情報（様式１）、二次利用未承諾リスト（様式２）を納入すること。
	* 調査報告書については、PDF形式に加え、機械判読可能な形式のファイルも納入すること。
	* 調査で得られた元データについては、機械判読可能な形式のファイルで納入することとし、特に図表・グラフに係るデータ（以下「Excel等データ」という。）については、Excel形式等により納入すること。
	* なお、様式１及び様式２はExcel形式とする。

（イ）調査報告書電子媒体（ＣＤ－Ｒ、またはＤＶＤ－Ｒ） ２式（公表用）

* + 調査報告書及び様式２（該当がある場合のみ）を一つのPDFファイル（透明テキスト付）に統合したもの、並びに公開可能かつ二次利用可能なExcel等データを納入すること。
	+ セキュリティ等の観点から、当省と協議の上、非公開とするべき部分については、削除するなどの適切な処置を講ずること。
	+ 調査報告書は、オープンデータ（二次利用可能な状態）として公開されることを前提とし、当省以外の第三者の知的財産権が関与する内容を報告書に盛り込む場合は、①事前に当該権利保有者の了承を得、②報告書内に出典を明記し、③当該権利保有者に二次利用の了承を得ること。二次利用の了承を得ることが困難な場合等は、下記の様式２に当該箇所を記述し、提出すること。
	+ 公開可能かつ二次利用可能なExcel等データが複数ファイルにわたる場合、１つのフォルダに格納した上で納入すること。

◆各データのファイル名については、調査報告書の図表名と整合をとること。

◆Excel等データは、オープンデータとして公開されることを前提とし、当省以外の第三者の知的財産権が関与する内容を含まないものとすること。

 ※調査報告書電子媒体の具体的な作成方法の確認及び様式１・様式２のダウンロードは、下記URLから行うこと。

　　 <https://www.meti.go.jp/topic/data/e90622aj.html>

1. 以下のドキュメントを納入すること。
2. プロジェクト計画書（契約締結後10日営業日以内）
3. 運用保守計画書（契約締結後10日営業日以内）
4. テスト計画書（契約締結後10日営業日以内）
5. テスト結果報告書（事業期間終了時まで）
6. 運用報告書（事業期間終了時まで）
7. システム構成図（事業期間終了時まで）
8. 基本設計書（事業期間終了時まで）
9. 詳細設計書（事業期間終了時まで）
10. ソースプログラム（事業期間終了時まで）
11. ログ情報（事業期間終了時まで）
12. 操作マニュアル（システム改修時）
13. 引き継ぎ資料（事業期間終了１ヶ月前まで）
14. 納入場所は以下のとおりとする。

東京都千代田区霞が関一丁目３番１号

　　　　　中小企業庁事業環境部企画課

1. 作業の実施体制・方法

(1)作業要員に求める資格等の要件

以下の要件を満たす者を配置した体制とし、本業務の作業体制表を提出すること。作業体制には、作業責任者、個人情報取扱責任者及び作業担当者の氏名及び所属、担当作業、指揮命令系統、情報セキュリティ対策に係る管理・連絡体制並びに連絡先を記載すること。

ア　作業責任者と個人情報取扱責任者を各々１名ずつ選任すること。

イ　作業責任者は、100人月規模以上の政府系情報システムの設計・開発の作業責任者としての経験を３件以上有すること。

ウ　作業責任者は、情報処理技術者試験制度の「プロジェクトマネージャ」試験の合格者若しくはＰＭＰ（Project Management Professional）の有資格者であること。

エ　チームリーダは、本システムの構成や仕様と類似するSalesforceシステムの設計・構築業務に関し、リーダとして２件以上の経験を有すること。

オ　開発メンバは、本システムの構成や仕様と類似するSalesforceシステムの設計・構築業務に関し、メンバとしての経験を有すること。

カ　本作業を担当する従事者の中に、Salesforceの資格を取得または以下のSalesforce開発経験を有する者を１名以上含めること。

1. 単一Salesforce組織内でオブジェクト数100以上の設計・構築業務
2. Salesforce組織から複数システムへのデータ連携の設計・構築業務。特にユーザー追加や権限管理は他システムから連携されるデータに応じて実行する実績など
3. 不特定ユーザーに対するSalesforce Customer Community のアカウント発行とマイページの設計・構築業務
4. Salesforce セキュリティツールであるイベントモニタリング、項目監査履歴の導入と運用
5. 作業の実施場所

ア　本業務の作業場所及び作業に当たり必要となる設備、備品及び消耗品等につい

ては、受注者の責任において用意すること。また、必要に応じて担当部署が現地確

認を実施することができるものとする。

イ　作業場所の選定にあたっては、経済産業省情報セキュリティ対策基準を遵守の上、当省の承認を得ること。

ウ　運用・保守業務において監視等拠点を経済産業省外に設ける場合は、上記規程を遵守の上、個人情報や機密情報等のデータを当省外から取得できないよう対策を講じること。

1. プロジェクトの管理
2. プロジェクト計画に関する事項

受注者は、契約締結後１０営業日以内に作業体制とともに作業内容及びスケジュール等について記載したプロジェクト計画書を策定し、当省担当職員に提出した上で、その承認を受けること。

受注者が作成するプロジェクト計画書には、マスタスケジュール、体制、開発方針の他、進捗管理、課題管理、変更管理、リスク管理、コミュニケーション管理、情報セキュリティ管理の各方法に加え、受注者が有効なプロジェクト管理を行うために有効と思われるものについて、当省担当職員受注者と検討し決定した項目について記すものとする。

作業体制には、システム開発作業責任者、システム開発作業に係る個人情報取扱責任者及びシステム開発作業担当者の氏名及び所属、担当作業の内容、指揮命令系統、情報セキュリティ対策に係る管理・連絡体制並びに連絡先を明記しなければならない。

1. 定例会等の実施

ア　受注者は、定例会を原則隔週開催するとともに、業務の進捗状況を作業実施要領に基づき報告すること。

　　　　イ　担当部署から要請があった場合、又は、受注者が必要と判断した場合、必要資料を作成の上、定例会とは別に会議を開催すること。

　　　　ウ　受注者は、会議終了後、3日以内（行政機関の休日（行政機関の休日に関する法律（昭和63年法律第91号）第１条第１項各号に掲げる日をいう。）を除く。）に議事録を作成し、担当部署の承認を得ること。

1. 作業の実施に当たっての留意事項
2. 情報セキュリティ

①受注者は本事業で知り得た情報を適切に管理するため、次の履行体制を確保し、発注者に対し「情報セキュリティを確保するための体制を定めた書面（情報管理体制図）」及び「情報取扱者名簿」（氏名、個人住所、生年月日、所属部署、役職等が記載されたもの）別添２（様式）を契約前に提出し、担当課室の同意を得ること（住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当課室から求められた場合は速やかに提出すること。）。

なお、情報取扱者名簿は、委託業務の遂行のため最低限必要な範囲で情報取扱者を掲載すること。

（確保すべき履行体制）

契約を履行する一環として契約相手方が収集、整理、作成等した一切の情報が、経済産業省が保護を要さないと確認するまでは、情報取扱者名簿に記載のある者以外に伝達又は漏えいされないことを保証する履行体制を有していること。

②本事業で知り得た一切の情報について、情報取扱者以外の者に開示又は漏えいしてはならないものとする。ただし、担当課室の承認を得た場合は、この限りではない。

③①の情報セキュリティを確保するための体制を定めた書面又は情報取扱者名簿に変更がある場合は、予め担当課室へ届出を行い、同意を得なければならない。

④国から提供した資料又は国が指定した資料の取扱い（返却・削除等）については、担当職員の指示に従うこと。

⑤情報セキュリティに関し、他の項に定めるもののほか、別添１「情報セキュリティに関する事項」に従うこと。

(2)機密保持、資料の取扱い

1. 担当部署から経済産業省情報セキュリティ管理規程、経済産業省情報セキュリティ管理基準等の説明を受けるとともに、本業務に係る情報セキュリティ要件を遵守すること。
2. 本業務に係る情報セキュリティ要件は次のとおりである。
3. 発注した業務以外の目的で利用しないこと。
4. 当省が開示した情報、契約履行過程で生じた納入成果物及び本作業の履行上知り得た一切の事項について、いかなる場合にもこれを当省が開示することを認めていない第三者に開示又は漏えいしてはならない。
5. 情報の開示を受けるにあたっては、開示する情報の内容、範囲、期限、開示を受けたものによる管理方法、使用後の措置を当省と協議の上取り決めること。
6. 情報の開示を受けるにあたっては、「機密保持体制表」を作成し、当省の了承を得ること。
7. 本作業を実施する上で、開示を受けた情報、作成及び出力した一切の資料については、当省の了承を得ずに本作業の作業場所以外に持ち出さないこと。
8. 上記の開示又は漏えい防止、当省の了承を得ることについては、本作業の業務期間終了後も同様とする。
9. 受注者は、情報セキュリティインシデントが発生するなどの万一の事故があった場合に直ちに報告する義務や*、*受注者の責に起因するセキュリティインシデントでの損害に対する賠償等の責任を負うこと。
10. 当省が提供する本作業に関連する文書等については、当省と協議の上、決定した場所に保管し、原則として、契約期間終了時までに返却又は裁断・溶解等の処分を行うこと。
11. 適切な措置が講じられていることを確認するため、遵守状況の報告を求めることや、必要に応じて発注者による実地調査が実施できること。
12. 本作業で作成したプログラム及びデータは事前に許可した機器やディレクトリのみに格納すること。
13. 本作業で作成したプログラム、データ及びその他本作業の履行上発生した納入成果物については、当省の許可なしに、作業実施場所から外部に持ち出さないこと。
14. 本作業で作成したプログラム、データ及びその他本作業の履行上発生した納入成果物については、当省の許可なしに、外部からアクセスできる状態におかないこと。
15. 電子媒体によって運用するプログラム、データ及び文書等については、ウィルスチェックを実施すること。
16. 異なる業者間でのデータ等の授受は、原則として、当省の了承を得ること。また、授受にあたっての連絡及び調整は、原則として、当省が行う。
17. 会議を実施するためのWeb会議サービスやファイル授受のためのオンラインストレージサービスを利用する際には、当省の指定するサービスを利用する等、事前に担当部署の了承を得ること。
18. 上記以外に、別紙1「情報セキュリティに関する事項」に基づき、作業を行うこと。

(3)個人情報の取扱い

1. 個人情報（生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。以下同じ。）の取扱いに係る事項について経済産業省と協議の上決定し、書面にて提出すること。なお、以下の事項を記載すること。
2. 個人情報の取扱いに関する責任者が情報管理責任者と異なる場合には、個人情報の取扱いに関する責任者等の管理体制
3. 個人情報の管理状況の検査に関する事項（検査時期、検査項目、検査結果において問題があった場合の対応等）
4. 本業務の作業を派遣労働者に行わせる場合は、労働者派遣契約書に秘密保持義務など個人情報の適正な取扱いに関する事項を明記し、作業実施前に教育を実施し、認識を徹底させること。なお、受注者はその旨を証明する書類を提出し、当省の承認を得た上で実施すること。
5. 個人情報を複製する際には、事前に担当部署の承認を得ること。なお、複製の実施は必要最小限とし、複製が不要となり次第、その内容が絶対に復元できないように破棄・消去を実施すること。なお、受注者は廃棄作業が適切に行われた事を確認し、その保証をすること。
6. 受注者は、本業務を履行する上で個人情報の漏えい等安全確保の上で問題となる事案を把握した場合には、直ちに被害の拡大を防止等のため必要な措置を講ずるとともに、担当部署に事案が発生した旨、被害状況、復旧等の措置及び本人への対応等について直ちに報告すること。
7. 個人情報の取扱いにおいて適正な取扱いが行われなかった場合は、本業務の契約解除の措置を受けるものとする。

(4)法令等の遵守

受注者は、本件に係る各種計画及び方針、並びに関連する各種法令を遵守すること。

(5)標準ガイドラインの遵守

　本作業の実施に当たっては、原則として「デジタル・ガバメント推進標準ガイドライン」等に記載された事項を遵守すること。

<https://www.digital.go.jp/resources/standard_guidelines/>

また、今後契約期間中に当該文書が改定された場合には、それに従うこととするが、より良い作業の進め方について提案がある場合には、担当職員に提案、協議の上、当該提案に基づき実施してもよい。

(6)契約金額内訳及び情報資産管理標準シートの提出

1. 受注者は、標準ガイドライン別紙２「情報システムの経費区分」に基づき区分等した契約金額の内訳が記載されたエクセルの電子データを契約締結後速やかに提出すること。
2. 受注者は、当省が定める時期に情報資産管理標準シートを提出すること。
3. 受注者は、当省が指定する様式について、当省が定める時期に提出すること。
4. 成果物の取扱いに関する事項
5. 知的財産権の帰属

ア　本業務における成果物の原著作権及び二次的著作物の著作権（著作権法第21条から第 28条に定める全ての権利を含む。）は、請負者が本事業の実施の従前から権利を保有していた等の明確な理由によりあらかじめ権利譲渡不可能と示されたもの以外は、全て主管課に帰属するものとする。

イ　主管課は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改変等し、及びそれらの利用を第三者に許諾することができるとともに、任意に開示できるものとする。

ウ　また、受注者は、成果物について、自由に複製し、改変等し、及びこれらの利用を第三者に許諾すること（ 以下「複製等」という。） ができるものとする。

ただし、成果物に第三者の権利が帰属するときや、複製等により主管課がその 業務を遂行する上で支障が生じるおそれがある旨を契約締結時までに通知したときは、この限りでないものとし、この場合には、複製等ができる範囲やその方法等について協議するものとする。

エ　納品される成果物に第三者が権利を有する著作物（以下「既存著作物等」という。）が含まれる場合には、受注者は、当該既存著作物等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を行うこと。この場合、本業務の受注者は、当該既存著作物の内容について事前に主管課の承認を得ることとし、主管課は、既存著作物等について当該許諾条件の範囲で使用するものとする。

なお、本仕様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の原因が専ら主管課の責めに帰す場合を除き、受注者の責任及び負担において一切を処理すること。この場合、主管課は係る紛争等の事実を知ったときは、受注者に通知し、必要な範囲で訴訟上の防衛を受注者に委ねる等の協力措置を講じるものとする。

オ　本件に関する権利（著作権法第21条から第28条に定める全ての権利を含む。）及び成果物の所有権は、主管課から受注者に対価が完済されたとき受注者から主管課に移転するものとする。

カ　受注者は主管課に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。

キ　受注者は使用する画像、デザイン、表現等に関して他者の著作権を侵害する行為に十分配慮し、これを行わないこと。

1. 契約不適合責任
2. 発注者は、業務が完了した後でも、その成果物もしくは役務行為の成果が種類、品質又は数量に関して本契約の内容に適合しない（以下、「契約不適合」という。）ときは、受注者に対して相当の期間を定めて催告し、その契約不適合の履行の追完をさせることができる。
3. 前項の規定により種類又は品質に関する契約不適合に関し履行の追完を請求するには、契約不適合の事実を知った時から１年以内に受注者に通知することを要する。ただし、受注者が、本業務の成果物もしくは役務行為の成果を発注者に引き渡した時において、その契約不適合を知り、又は重大な過失によって知らなかったときは、この限りでない。
4. 受注者は、本業務の成果物もしくは役務の成果について、契約不適合のある場合、速やかに、履行を追完すること。
5. 前項の規定により、追完を行うときには、不適合の原因と追完の方法、追完を行った場合の影響について当省に提示し、了承を得ること。
6. 受注者は、当省が了承した計画にもとづいて、調査及び必要な修補又は履行の追完を実施するとともに設計書、マニュアル等の関連する納入成果物も併せて修正の上、提出すること。
7. 受注者が前アの期間内に履行の追完をしないときは、発注者は、受注者の負担にて第三者に履行の追完をさせ、又は契約不適合の程度に応じて受注者に対する対価の減額を請求することができる。ただし、履行の追完が不能であるとき、受注者が履行の追完を拒絶する意思を明確に表示したとき、本契約の履行期限内に履行の追完がなされず本契約の目的を達することができないとき、そのほか発注者が第１項の催告をしても履行の追完を受ける見込みがないことが明らかであるときは、発注者は、受注者に対し、前アの催告をすることなく、発注者の負担において直ちに第三者に履行の追完をさせ、又は対価の減額を請求することができる。
8. 検収
9. 本業務の受注者は、「３．（５）成果物」に記載の本仕様書に基づく契約の目的物について、納品期日までに主管課に内容の説明を実施し検収を受けること。
10. 検収の結果、成果物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について主管課に説明を行った上で、指定された日時までに再度納品すること。
11. 入札参加資格に関する事項
12. 競争参加資格

ア　予算決算及び会計令第70条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。

イ　公告日において令和4・5・6年度全省庁統一資格の「役務の提供等」の「A」、「B」、「C」又は「D」の等級に格付けされ、競争参加資格を有する者であること。

ウ　各省各庁から指名停止又は一般競争入札資格停止若しくは営業停止を受けていない者であること。

エ　入札に参加を希望する者は、本調達の仕様を理解するため、各種資料等を閲覧しなければならない。資料の閲覧に係る手続き等については、機密情報閲覧に関する誓約書を提出すること。

1. 受注実績等

ア　応札者は、過去3年以内に、本業務と同種の業務、あるいは類似業務を実施した実績を有すること。

イ　応札者は、同規模（利用者数約10,000人以上）及びそれ以上の政府系情報システムにおける運用・保守実績を有すること。

ウ　応札者は、Salesforceのコンサルティングパートナーもしくは再販パートナーの認定を受けた事業者であること。

1. 附属文書

(1)別添１　情報セキュリティに関する事項

(2)別添２　情報取扱者名簿及び情報管理体制図

(3)別添３　法人インフォメーションとの連携

(4)別添４　中小企業支援プラットフォームとの連携

以　上

（別添１）

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。

【情報セキュリティ関連事項の確保体制および遵守状況の報告】

1) 受注者（委託契約の場合には、受託者。以下同じ。）は、契約締結後速やかに、情報セキュリティを確保するための体制並びに以下2)～17)に記載する事項の遵守の方法及び提出を求める情報、書類等（以下「情報セキュリティを確保するための体制等」という。）について、経済産業省（以下「当省」という。）の担当職員（以下「担当職員」という。）に提示し了承を得た上で確認書類として提出すること。ただし、別途契約締結前に、情報セキュリティを確保するための体制等について担当職員に提示し了承を得た上で提出したときは、この限りでない。また、定期的に、情報セキュリティを確保するための体制等及び対策に係る実施状況（「情報セキュリティに関する事項の遵守の方法の実施状況報告書」（様式））を紙媒体又は電子媒体により報告すること。加えて、これらに変更が生じる場合は、事前に担当職員へ案を提出し、同意を得ること。

なお、報告の内容について、担当職員と受注者が協議し不十分であると認めた場合、受注者は、速やかに担当職員と協議し対策を講ずること。

【情報セキュリティ関連規程等の遵守】

2) 受注者は、「経済産業省情報セキュリティ管理規程（平成18･03･22シ第1号）」、「経済産業省情報セキュリティ対策基準（平成18･03･24シ第1号）」及び「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（令和５年度版）」(以下「規程等」と総称する。)を遵守すること。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。

3) 受注者は、当省又は内閣官房内閣サイバーセキュリティセンターが必要に応じて実施する情報セキュリティ監査、マネジメント監査又はペネトレーションテストを受け入れるとともに、指摘事項への対応を行うこと。

【情報セキュリティを確保するための体制】

4) 受注者は、本業務に従事する者を限定すること。また、受注者の資本関係・役員の情報、本業務の実施場所、本業務の全ての従事者の所属、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を担当職員に提示すること。なお、本業務の実施期間中に従事者を変更等する場合には、事前にこれらの情報を担当職員に再提示すること。

5) 受注者は、本業務を再委託（業務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。）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、1)から17)まで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、1)の確認書類には再委託先に係るものも含むこと。

【情報の取扱い】

6) 受注者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）の取扱いには十分注意を払い、当省内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に担当職員の許可を得ること。なお、この場合であっても、担当職員の許可なく複製してはならない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明すること。

7) 受注者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体）について、担当職員の許可なく当省外で複製してはならない。また、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明すること。

8) 受注者は、本業務を終了又は契約解除する場合には、受注者において本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）を速やかに担当職員に返却し、又は廃棄し、若しくは消去すること。その際、担当職員の確認を必ず受けること。

9) 受注者は、契約期間中及び契約終了後においても、本業務に関して知り得た当省の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。

なお、当省の業務上の内容を外部に提供する必要が生じた場合は、提供先で当該情報が適切に取り扱われないおそれがあることに留意し、提供の可否を十分に検討した上で、担当職員の承認を得るとともに、取扱上の注意点を示して提供すること。

【情報セキュリティに係る対策、教育、侵害時の対処】

10) 受注者は、本業務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業務にかかわる従事者に対し実施すること。

11) 受注者は、本業務の遂行において、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。

【クラウドサービス】

12) 受注者は、本業務を実施するに当たり、民間事業者等が不特定多数の利用者に対して提供する、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスを利用する場合には、これらのサービスで要機密情報を取り扱ってはならず、2)に掲げる規程等で定める不正アクセス対策を実施するなど規程等を遵守すること。

13) 受注者は、本業務を実施するに当たり、利用において要機密情報を取り扱うものとしてクラウドサービスを調達する際は、「政府情報システムのためのセキュリティ評価制度（ISMAP）」のISMAPクラウドサービスリスト又はISMAP-LIUクラウドサービスリストから調達することを原則とすること。

14) 受注者は、前2項におけるクラウドサービスの利用の際は、提供条件等から、利用に当たってのリスクの評価を行い、リスクが許容できることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。

【セキュアな情報システム（外部公開ウェブサイトを含む）の構築・運用】

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。

①各工程において、当省の意図しない変更や機密情報の窃取等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、具体的な管理手順や品質保証体制を証明する書類等を提出すること。

②情報システムや機器等に意図しない変更が行われる等の不正が見つかったときに、追跡調査や立入検査等、当省と連携して原因を調査し、排除するための手順及び体制を整備していること。これらが妥当であることを証明するため書類を提出すること。

③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。 また、以下を含む対策を行うこと。

（a）不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。

（b）不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成すること。

（c）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、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。

（d）不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。

（e）EDRソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討すること。

④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、他の事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容を含めること。

⑤サポート期限が切れた、又は本業務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こと、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。

⑥受注者自身（再委託先を含む。）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。

⑦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等の当省外向けシステムを構築又は運用する場合には、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」を使用すること。

⑧外部に公開するウェブサイトを構築又は運用する場合には、以下の対策を実施すること。

・サービス開始前および、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。

・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。

⑨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。

【アプリケーション・コンテンツの情報セキュリティ対策】

16) 受注者は、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。

①提供するアプリケーション・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。

（a）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。

（b）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。

（c）提供するアプリケーション・コンテンツにおいて、当省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などして確認すること。

②提供するアプリケーション・コンテンツが脆弱性を含まないこと。

③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。

④電子証明書を用いた署名等、提供するアプリケーション・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、政府認証基盤（ＧＰＫＩ）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。

⑤提供するアプリケーション・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、ソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更をＯＳ、ソフトウェア等の利用者に要求することがないよう、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。

⑥当省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などの機能がアプリケーション・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アプリケーション・コンテンツに組み込む場合は、当省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アプリケーション・コンテンツに掲載すること。

17) 受注者は、外部に公開する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、ウェブアプリケーションの構築又は更改時においてはサービス開始前に、運用中においてはウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合に、「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。

様式

令和 年 月 日

中小企業庁事業環境部企画課長　殿

住　　　　　所

　　　 名　　　　　称

　　　　　　　　　代 表 者 氏 名

情報セキュリティに関する事項の遵守の方法の実施状況報告書

　情報セキュリティに関する事項１）の規定に基づき、下記のとおり報告します。

記

１．契約件名等

|  |  |
| --- | --- |
| 契約締結日 |  |
| 契約件名 |  |

２．報告事項

|  |  |  |
| --- | --- | --- |
| 項目 | 確認事項 | 実施状況 |
| 情報セキュリティに関する事項２） | 本業務全体における情報セキュリティの確保のため、「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」（令和５年度版）、「経済産業省情報セキュリティ管理規程」（平成１８・０３・２２シ第１号）及び「経済産業省情報セキュリティ対策基準」（平成１８･０３･２４シ第１号）（以下「規程等」と総称する。）に基づく、情報セキュリティ対策を講じる。 |  |
| 情報セキュリティに関する事項３） | 経済産業省又は内閣官房内閣サイバーセキュリティセンターが必要に応じて実施する情報セキュリティ監査、マネジメント監査又はペネトレーションテストを受け入れるとともに、指摘事項への対応を行う。 |  |
| 情報セキュリティに関する事項４） | 本業務に従事する者を限定する。また、受注者の資本関係・役員の情報、本業務の実施場所、本業務の全ての従事者の所属、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を担当職員に提示する。なお、本業務の実施期間中に従事者を変更等する場合には、事前にこれらの情報を担当職員に再提示する。 |  |
| 情報セキュリティに関する事項５） | 本業務の一部を再委託する場合には、再委託することにより生ずる脅威に対して情報セキュリティに関する事項１）から１７）までの規定に基づく情報セキュリティ対策が十分に確保される措置を講じる。 |  |
| 情報セキュリティに関する事項６） | 本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）の取扱いには十分注意を払い、経済産業省内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に経済産業省の担当職員（以下「担当職員」という。）の許可を得る。なお、この場合であっても、担当職員の許可なく複製しない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明する。 |  |
| 情報セキュリティに関する事項７） | 本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体）について、担当職員の許可なく経済産業省外で複製しない。また、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明する。 |  |
| 情報セキュリティに関する事項８） | 本業務を終了又は契約解除する場合には、受注者において本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）を速やかに担当職員に返却し、又は廃棄し、若しくは消去する。その際、担当職員の確認を必ず受ける。 |  |
| 情報セキュリティに関する事項９） | 契約期間中及び契約終了後においても、本業務に関して知り得た経済産業省の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。なお、経済産業省の業務上の内容を外部に提供する必要が生じた場合は、提供先で当該情報が適切に取り扱われないおそれがあることに留意し、提供の可否を十分に検討した上で、担当職員の承認を得るとともに、取扱上の注意点を示して提供する。 |  |
| 情報セキュリティに関する事項１０） | 本業務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業務にかかわる従事者に対し実施する。 |  |
| 情報セキュリティに関する事項１１） | 本業務の遂行において、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。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。 |  |
| 情報セキュリティに関する事項１２） | 本業務を実施するに当たり、民間事業者等が不特定多数の利用者に対して提供する、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスを利用する場合には、これらのサービスで要機密情報を取り扱ってはならず、「情報セキュリティに関する事項２）」に定める不正アクセス対策を実施するなど規程等を遵守する。 |  |
| 情報セキュリティに関する事項１３） | 本業務を実施するに当たり、利用において要機密情報を取り扱うものとしてクラウドサービスを調達する際は、「政府情報システムのためのセキュリティ評価制度（ISMAP）」のISMAPクラウドサービスリスト又はISMAP-LIUクラウドサービスリストから調達することを原則とすること。 |  |
| 情報セキュリティに関する事項１４） | 情報セキュリティに関する事項１２）及び１３）におけるクラウドサービスの利用の際は、提供条件等から、利用に当たってのリスクの評価を行い、リスクが許容できることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。 |  |
| 情報セキュリティに関する事項１５） | 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。（１）各工程において、当省の意図しない変更や機密情報の窃取等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、具体的な管理手順や品質保証体制を証明する書類等を提出すること。（２）情報システムや機器等に意図しない変更が行われる等の不正が見つかったときに、追跡調査や立入検査等、当省と連携して原因を調査し、排除するための手順及び体制を整備していること。これらが妥当であることを証明するため書類を提出すること。（３）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。また、以下を含む対策を行うこと。①不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。②不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成すること。③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、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。④不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。⑤EDRソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討すること。（４）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、他の事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容を含めること。（５）サポート期限が切れた又は本業務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こと、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。（６）受注者自身（再委託先を含む。）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。 （７）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等の当省外向けシステムを構築又は運用する場合には、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」を使用すること。（８）外部に公開するウェブサイトを構築又は運用する場合には、以下の対策を実施すること。・サービス開始前および、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。・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。・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。（９）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。 |  |
| 情報セキュリティに関する事項１６） | 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。（１）提供するアプリケーション・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提供するアプリケーション・コンテンツにおいて、当省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などして確認すること。（２）提供するアプリケーション・コンテンツが脆弱性を含まないこと。（３）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。（４）電子証明書を用いた署名等、提供するアプリケーション・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、政府認証基盤（ＧＰＫＩ）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。（５）提供するアプリケーション・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、ソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更をＯＳ、ソフトウェア等の利用者に要求することがないよう、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。（６）当省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などの機能がアプリケーション・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アプリケーション・コンテンツに組み込む場合は、当省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アプリケーション・コンテンツに掲載すること。 |  |
| 情報セキュリティに関する事項１７） | 外部公開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。）に従う。また、ウェブアプリケーションの構築又は改修時においてはサービス開始前に、運用中においてはウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合に、「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。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。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には、その指示に従う。 |  |

記載要領

１．「実施状況」は、情報セキュリティに関する事項２）から１７）までに規定した事項について、情報セキュリティに関する事項１）に基づき提出した確認書類で示された遵守の方法の実施状況をチェックするものであり、「実施」、「未実施」又は「該当なし」のいずれか一つを記載すること。「未実施」又は「該当なし」と記載した項目については、別葉にて理由も報告すること。

２．上記に記載のない項目を追加することは妨げないが、事前に経済産業省と相談すること。

（この報告書の提出時期：定期的（契約期間における半期を目処（複数年の契約においては年１回以上））。）

（別添２）

情報取扱者名簿及び情報管理体制図

①情報取扱者名簿

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 氏名 | 個人住所 | 生年月日 | 所属部署 | 役職 | パスポート番号及び国籍（※４） |
| 情報管理責任者（※１） | Ａ |  |  |  |  |  |  |
| 情報取扱管理者（※２） | Ｂ |  |  |  |  |  |  |
| Ｃ |  |  |  |  |  |  |
| 業務従事者（※３） | Ｄ |  |  |  |  |  |  |
| Ｅ |  |  |  |  |  |  |
| 再委託先 | Ｆ |  |  |  |  |  |  |

（※１）受託事業者としての情報取扱の全ての責任を有する者。必ず明記すること。

（※２）本事業の遂行にあたって主に保護すべき情報を取り扱う者ではないが、本事業の進捗状況などの管理を行うもので、保護すべき情報を取り扱う可能性のある者。

（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※４）日本国籍を有する者及び法務大臣から永住の許可を受けた者（入管特例法の「特別永住者」を除く。）以外の者は、パスポート番号等及び国籍を記載。

（※５）住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当課室から求められた場合は速やかに提出すること。

②情報管理体制図

（例）

情報取扱者

【情報管理体制図に記載すべき事項】

・本事業の遂行にあたって保護すべき情報を取り扱う全ての者。（再委託先も含む。）

・本事業の遂行のため最低限必要な範囲で情報取扱者を設定し記載すること。

（別添３）

法人インフォメーションとの連携

法人インフォメーションとの連携の概要

電子申請の入力時等において、操作者の入力作業を簡素化するため、法人の基本情報を当省が保有する法人インフォメーションシステムから取り込み、自動的に表示(プレプリント) することを想定している。

法人インフォメーションが、外部システムに法人データを提供するAPI及びデータについて以下に記す。



法人インフォメーションから取得できるデータ

本 API を用いることで、法人の法人番号、名称、住所（商業登記の情報）といった基本的な情報に加え、補助金、調達、表彰、届出認定（各府省庁から提供のあったもの）といった各種の活動に関する情報を検索・取得することが可能である。各情報は RDF データとして表現されており、REST を用いた検索・取得が可能である。

参照・検索API

1. 利用者は、アクセストークン発行画面からアクセストークンを取得する。
2. 利用者は、入手したトークンを利用するアプリケーションに設定する。
3. アプリケーションは、アクセストークンを用いて法人インフォメーションAPIをコールする。

法人インフォメーションから取得するデータ項目、APIの仕様書

法人インフォメーションから取得するデータ項目、API仕様については、以下から取得できる最新のデータ項目、インタフェース仕様に従うこと。

* REST：情報提供REST　API

　　　　https://hojin-info.go.jp/hojin/swagger-ui.html

 (別添４)

中小企業支援プラットフォームとの連携

１）中小企業支援プラットフォームとの連携の概要

　　２０２０年４月より中小企業向けの行政手続における電子申請は中小企業支援プラットフォーム（仮）に統合する方針であるところ、各サービスと中小企業支援プラットフォームの連携の概要について記す。

（中小企業支援プラットフォームイメージ図）



2) 連携内容

　ア) ポータルサイトと電子申請サイトのURL連携

各電子申請サイトはポータルサイトとなる「ミラサポｐｌｕｓ」からＵＲＬリンクでページ遷移できるようにする。

　各電子申請サイトにおいて検索機能等を有する場合、検索結果、照会画面等を固有のＵＲＬで表示できるようにし、また検索条件をＵＲＬパラメータに設定できるようにすること。

1. サイトデザインの統一

　中小企業向け電子申請サイトであることが視覚的にも認識できるようサイトデザインを「ミラサポｐｌｕｓ」のデザインに極力合わせること。サイトデザインの調整に当たっては、スタイルガイドを中小企業庁担当者より受領し、スタイルガイドを適用するページを中小企業庁担当者と調整の上、決定すること。