令和５年度～令和６年度経済産業省基盤情報システム更改に係るGSS移行及び独自調達システム等の調達支援業務
調達仕様書（案）

経済産業省

令和５年ｘ月

目次

1　件名

令和５年度～令和６年度経済産業省基盤情報システム更改に係る GSS 移行及び独自調達システム等の調達支援業務

2　事業の背景及び目的

経済産業省（以下「当省」という。）では当省職員による業務の効率化、高度化を進めるために職員が使用する PC とネットワーク環境（LAN）である経済産業省基盤情報システム（以下「基盤情報システム」という。）を構築、運用しており、当省の行政事務遂行において必要不可欠なものとなっている。

現行の第７期の経済産業省基盤情報システムサービス（以下、「第７期システム」という。）は、令和４年２月に更改し運用しているところであるが、IT 技術の進歩や機器の耐用年数を考慮し４年後の令和７年度後半のシステム更改を予定している。

次の第８期基盤情報システム（以下、「第８期システム」という。）への更改にあたっては、「デジタル社会の実現に向けた重点計画」（令和４年６月７日閣議決定）により、デジタル庁が整備するガバメントソリューションサービス（以下、「GSS」という。）へ移行するとされていることから、GSS へ移行することを前提としつつ、利用する職員の柔軟な働き方に対応し、働きがいが高まる基盤情報システムの実現を目標としている。また、GSS を利用することによる費用削減も最大限追及する方針としている。

第８期システムへの更改を行うにあたっては、当省の基盤情報システムが求めるサービスと、GSS で提供しているサービスの差異があることから、GSS への移行に向けた設定の検討と独自に調達・構築する個別のシステム（以下、「独自調達システム」という。）の仕様検討等、双方の作業を調整しつつ平行に進める必要がある。

これらの作業を実施するには、技術的専門性が要求されるため、専門的知識を有する第三者の支援が不可欠であるため、本調達仕様書に基づいて、専門的知識を有する第三者を本業務実施業者として調達するものである。

3　成果物納入

(1) 納入物

本業務における納入物とその提出時期及び納入期限は下表のとおり。納入物ごとの提出時期までに提出し、当省の大臣官房情報システム室等の職員（以下「担当職員」という。）による確認を受け、最終版を各年度の最終納入期限までに納入しなければならない。なお、下表に示す提出時期は目安であるため、請負者は落札後速やかに、自らが提案したスケジュールに応じた各納入物の提出予定日を確定し、担当職員の承認を得ること。

表１　納入物一覧

項番	納入物	提出時期 （目安）	最終納入期限
1	業務実施計画書	契約日から 10 営業日以内	令和６年３月末
2	情報提供依頼資料案	令和５年９月中旬	
3	資料提供招請実施結果報告書	令和５年 12 月下旬	
4	業務実施結果報告書（中間報告）	令和６年３月下旬	
5	費用積算書（GSS 及び独自調達）	令和６年３月下旬	
6	調達仕様書案・要件定義書案	令和６年６月上旬	令和７年３月末
7	提案依頼書案・技術審査項目案	令和６年７月下旬	
8	意見招請に対する意見への対応案	令和６年８月下旬	
9	技術審査結果報告書	令和７年１月上旬	
10	システム管理支援業務に係る業務要求仕様書・費用積算書・提案依頼書案・技術審査項目案	令和７年３月下旬	
11	業務実施結果報告書（最終報告）	令和７年３月下旬	

(2) 納入方法

納入物の最終納入に当たっては、担当職員の承認を得た内容を電子媒体に格納し、担当職員が指示する場所に納入すること。また、納入物の内容について担当職員から変更の指示があった場合には、速やかに対応すること。

4　本調達に係る関係者

第７期システム及び第８期システムに関係する事業者、当省の関係者及び他省庁等を含めた関係者を下表のとおり想定している。本業務の請負者は、関係者と積極的にコミュニケーションを図りながら業務を遂行すること。

表２　本調達に係る関係者

関係者	該当する機関・部署及び事業者名	契約期間
プロジェクト責任者	経済産業省業務改革課情報システム室長	－
PJMO	経済産業省業務改革課情報システム室、 特許庁総務部総務課	－
第７期システム提供事業者	日本電気株式会社 株式会社 JECC	令和３年４月～ 令和８年１月
第７期システム運用管理事業者	NEC フィールディング株式会社	令和３年 10 月～ 令和８年１月
ガバメントソリューションサービス主管	デジタル庁	－

5　業務内容

(1) 本プロジェクトの管理

ア　業務実施計画書作成

請負者は契約締結日から１０営業日以内に業務実施計画書を提出し、担当職員の承認を得ること。

イ　管理・報告

請負者は本プロジェクトに関する進捗及び課題等を適切に管理し、担当職員に対して定期的に進捗状況の報告や課題に関する協議等を行うための会議体を設けること。なお、会議体の開催頻度は、プロジェクトの状況に応じて週次もしくは隔週を想定しており、具体的な開催スケジュールは担当職員と調整の上、決定すること。また、本会議体を開催後３営業日以内に議事録を作成し、当省へ提出すること。

ウ　基盤情報システムのプロジェクト計画書更新支援

請負者は、第８期システムへの更改に向け、基盤情報システムのプロジェクト計画書を本作業での検討状況に応じて更新すること。更新にあたっては、「デジタル・ガバメント推進標準ガイドライン」（https://www.digital.go.jp/resources/standard_guidelines/）（以下「標準ガイドライン」という。）に準拠すること。なお、基盤情報システムのプロジェクト計画書は当省ＰＭＯやデジタル庁等からの求めに応じて随時提出する必要が生じることから、担当職員から要望があった場合には速やかに更新を行い、承認を得ること。

エ　中間報告の実施

請負者は令和６年３月下旬を目途に、令和５年度の業務実施結果を中間報告として報告すること。中間報告では、それまでの検討状況や成果物等を取りまとめて、報告すること。

オ　最終報告の実施

請負者は令和７年３月下旬を目途に、本業務に関する最終報告を実施すること。最終報告では、それまでに実施した業務の実施結果を整理するとともに、令和７年度の第８期システムの設計・構築工程に携わる担当職員及び支援事業者に向けた引継ぎ事項等を取りまとめて、報告すること。

(2) 資料提供招請実施支援

ア　情報提供依頼書案の作成

第８期システムの構築・移行に向けては、令和４年度及び令和５年度に各１回ずつ、計２回の資料提供招請を実施することを予定している。請負者は令和４年度に実施した資料提供招請における依頼内容及び分析結果、GSSとの仕様調整及び各独自調達システムの仕様検討状況を踏まえ、令和５年度の資料提供招請において使用する情報提供依頼資料案を作成し、当省の承認を得ること。

なお、資料提供招請の実施に当たり、当省内外の関係者への説明を実施することから、説明資料の作成等を支援すること。

イ　説明会等支援

資料提供招請の公告後、説明会や事業者からの質問回答を実施することを想定しているため、請負者はその対応を支援すること。

ウ　実施結果分析

請負者は各事業者からの提供資料についてその内容を整理し、第８期システムの想定構成やコスト、更改に向けたスケジュール等への影響を分析した上で、資料提供招請実施結果報告書として取りまとめて、報告すること。

(3) ガバメントソリューションサービス（GSS）の仕様調整

ア　デジタル庁との調整支援

第８期システムで GSS を利用可能なサービスについては、デジタル庁と GSS への移行に向けた調整を進めていく必要があるため、デジタル庁との定例打合せを設けることを予定している。請負者はその定例打合せに参加し、デジタル庁との各種調整について支援すること。

イ　移行方法検討

請負者は GSS への移行に向けて、利用する機能や運用、組織範囲などの移行対象範囲を明確にした上で、それぞれのサービスに係る移行方式や移行スケジュールを検討し、GSS 移行方針書案として取りまとめること。

ウ　仕様調整支援

GSS に係る調達仕様書及び要件定義書はデジタル庁にて作成されるが、そのためには当省からデジタル庁への各種情報提供や仕様調整が必要になることから、請負者は当省の関係組織や関係事業者と協力して必要な情報の収集や仕様検討を支援すること。

なお、仕様調整にあたっては、当省の第７期システムでの独自機能（カスタマイズ機能）の移行可能性を検討すること。

エ　コスト試算支援

GSS に係る予算はデジタル庁にて一括計上される見込みであるが、そのためには当省からの情報提供が必要になることから、請負者は GSS 移行に係る費用を積算し、予算要求時に求められる積算根拠資料等を作成し、当省の対応を支援すること。なお、費用積算に当たっての作業分担については当省及びデジタル庁と十分に認識を合わせた上で、漏れの無いように留意すること。

オ　移行計画作成支援

GSS への移行に向けては、令和７年度に GSS 受託事業者等と協力して移行を実施することになるため、本業務の請負者はその準備として、現行業務からの変更点を整理した上で、職員への教育及び訓練等に係る移行作業計画案を取りまとめること。

(4) 当省が独自に用意するシステムの調達支援

ア　調達仕様書案及び要件定義書案の作成

第８期システムで必要とするサービスのうち、GSS を利用しないサービスについては当省にて調達することから、請負者は令和４年度に実施した１回目の資料提供招請と、本業務期間中に

実施する２回目の資料提供招請の結果を踏まえ、調達に向けた要件を検討し、調達仕様書案及び要件定義書案として取りまとめること。

なお、現時点で想定している独自調達システムは、個別の業務システム用サーバリソース、外部公開用 Web システム、データ連携基盤、システム管理支援、その他新規機能等があるので、令和 4 年度に実施している「経済産業省基盤情報システムに係るフィージビリティスタディ調査業務」の報告書を確認し、目的や要件を理解すること。

要件定義に当たっては、当省内の関係者を参加者とする各種ワーキンググループを開催し、また必要に応じて関係者へ個別にヒアリングを行うなどして、業務や機能、非機能に係る要件を整理し、次期システムのコンセプトとの整合性を勘案し、以下の点に留意しつつ調達仕様書案及び要件定義書案に反映すること。また、不確定要素のある案件についてはリスク要因を明らかにすること。

A) 設計・構築等の役務要件については、第７期システムの設計・構築作業の振り返り結果を踏まえた留意事項を整理した上で、調達仕様書案等に反映すること

B) 第８期システムが備えるべき基本的な機能要件を整理した上で、システム機能構成図を作成すること。また、大まかなシステム構成を検討し、ハードウェア構成図、ソフトウェア構成図、ネットワーク構成図を作成すること。

C) 重複した機能（サービス）が入らないようにすること。

D) スケジュール管理、課題管理及びリスク管理等のプロジェクト活動の品質が向上される内容にすること。

E) 第８期システムの特性に合うように、ガイドラインのテーラリングを行ったうえで、遵守すべきプロセスや成果物を定義すること。

F) 構築事業者から目的に沿わない提案、設計を極力防止するため、第８期システムの利用方法や運用方法を検討し、ユースケース図及び業務要件を作成すること。その際、エンドユーザでユースケースが異なる場合には、それぞれについて作成すること。

G) 構築事業者が調達後にタスクの考慮漏れによるスケジュールの遅延等が発生しないような記載の工夫を行うこと。

H) GSS、構築事業者、システム管理事業者、当省各者の役割分担及び責任分界を明確にすること。

I) 第８期システムの調達において、各成果物の品質基準を向上させるような記載の工夫を行うこと。特に、第７期システムからの切替えにおいて、経済産業行政事務処理に影響を及ぼさないようにするために、性能要件の基準を明記するなどの工夫を行うこと。

J) 必要な性能要件が確保されるよう、性能の目標値や目標値を測定する際の条件（業務量、アクセス量、データ量等）を明確に定め、実運用時を想定した性能設計がなされるようにすること。

K) 実運用を想定したテスト要件の明確化及び性能に係る早期の検証に係る要件の定義がなされるようにすること。

L) その他第８期システムの構築・運用等にあたり想定しうる問題を検討し、問題を抑止する工夫をした記載内容とすること。

イ　コスト試算支援

当省で調達するサービスについては、当省で予算要求を実施することから、請負者は調達仕様書案等に基づき全ての費用を積算し、予算要求時に求められる積算根拠資料等を作成し、当省の対応を支援すること。

ウ　調達手続き支援

当省独自に調達するサービスの調達手続きに係る意見招請や入札の実施に当たり、当省内外の関係者への説明が求められることから、請負者はその説明資料の作成を支援すること。

また、意見招請や入札に係る以下の作業を実施すること。

① 意見招請支援

事業者からの質問や意見の内容を確認し、回答案を作成すること。また、意見招請後に仕様書の修正が必要な場合は、修正案を作成すること。

② 技術審査支援

請負者は、技術審査会を実施するために必要な運用要領や技術審査マニュアルなどの資料を担当職員と調整の上、作成するとともに、各業務の外部専門家による技術審査について、５回程度（仕様書・審査概要説明、提案内容説明、提案者へのヒアリング、とりまとめ、予備）開催される審査会の運営を行い、当該外部専門家及び省内関係者に対して各社提案に関する十分な説明及び質疑対応を行い、外部専門家及び省内関係者の合意を得た上で、各社提案に対する評価を取りまとめること。

(5) システム管理支援業務の調達支援

ア　調達仕様書案及び要件定義書案の作成

GSS の運用管理については、デジタル庁が用意するヘルプデスク等を利用するが、独自調達システムは、職員からの問い合わせ窓口や、システム稼働監視等のシステム管理も独自に実施する。また、当省職員の利便性を考慮し、問合せは GSS の件も一次受けして GSS の窓口へ転送するなど、独自システムと窓口を一本化したいと考えている。請負者は GSS と独自システムが混在する環境下での、適切なシステム管理体制を検討し、調達仕様書案及び要件定義書案として取りまとめること。

要件定義に当たっては、当省内の関係者を参加者とする各種ワーキンググループを開催し、また必要に応じて関係者へ個別にヒアリングを行うなどして要件定義書に反映すること。

イ　コスト試算支援

システム管理支援業務については、当省で予算要求を実施することから、請負者は調達仕様書案等に基づき全ての費用を積算し、予算要求時に求められる積算根拠資料等を作成し、当省の対応を支援すること。

ウ　調達手続き支援

システム管理支援業務の調達手続きに係る意見招請の実施に向け、当省内外の関係者への説明が求められることから、請負者はその説明資料の作成を支援すること。

(6)　情報資産管理標準シートの提出等

請負者は、本事業の実施に係る以下の資料を当省に提出すること。

① 契約金額内訳

デジタル・ガバメント推進標準ガイドラインの「別紙２　情報システム経費区分」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 情報資産管理標準シートの提出

情報資産管理標準シートを、デジタル庁から作業依頼のある時期（原則毎年度末）に、提出すること。

(7)　その他

GSS へ移行する範囲及び、独自調達システムの範囲は今後の検討、調整の中で変化する場合がある。その場合は担当職員と協議のうえで、作業内容の見直しを行うこと。

6　全体スケジュール案

本業務は令和５年度及び令和６年度の複数年度において実施する業務である。第８期システム調達において想定している全体スケジュール案を以下に示す。なお、本スケジュールは現時点での想定であり、今後の調査業務における検討状況や外部との調整状況によりスケジュールが変更になる可能性があるため、請負者はその可能性を十分に理解したうえで、状況の変化に対して柔軟に対応すること。

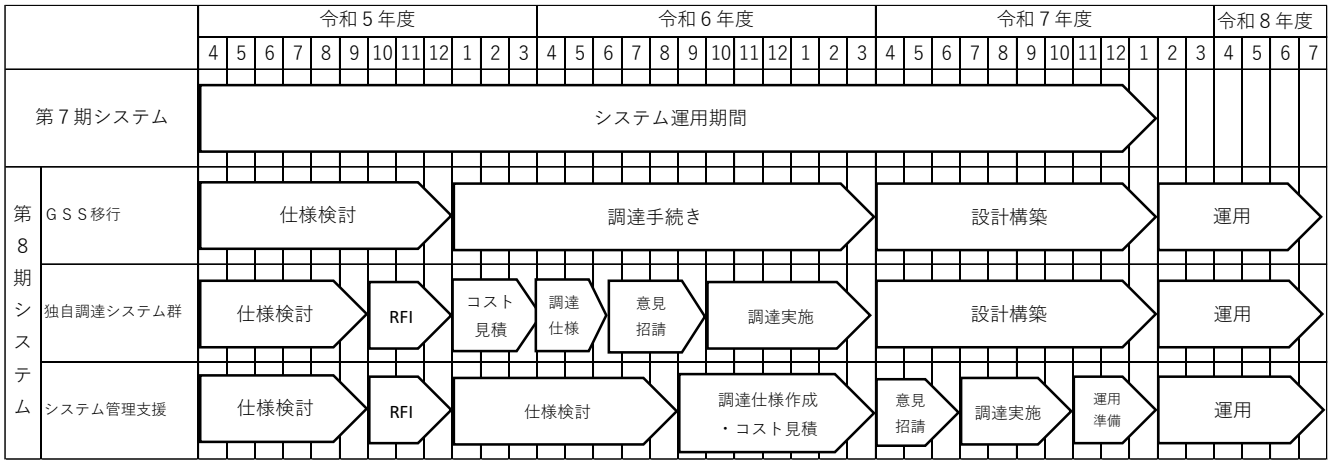


図２　全体スケジュール案

7　契約期間

契約締結日から令和７年３月３１日(月)までとする。

8　請負者の要件

(1) 業務実績

請負者は直近３年程度の間に以下の業務実績を有し、これを証明すること。

① 2,000 人以上のユーザが利用する基盤情報系システム（例：AD、DNS、Proxy、Web、Mail 等の IT インフラ。）に係る調査業務もしくは要件定義業務、調達支援業務を累計３件以上遂行した実績

② 中央省庁等の公共機関におけるパブリッククラウドサービスを利用する情報システムに係る調査業務もしくは要件定義業務、調達支援業務を遂行した実績

(2) マネジメントシステム

請負者はマネジメントシステムに係る以下の要件を充足し、これを証明すること。

① 品質マネジメントシステムの規格である「JIS Q 9001」（登録活動範囲が情報処理に関するもの）の認証取得事業者であること。または、これと同等の能力を有していること。

② 情報セキュリティマネジメントシステムの規格である「ISO27001（JIS Q 27001）/ISMS 適合性評価制度」の認証取得事業者であること。または、これと同等の能力を有していること。

9　作業の実施体制

(1) 実施体制

請負者は、本業務の実施に当たり、プロジェクト全体を管理する業務責任者を１名配置すること。また、本業務の実施に当たり必要となる専門性を定義した上で、それらの専門性を有する業務従事者を３名以上配置すること。

(2) 業務責任者

業務責任者には以下の資格及び要件を有している者を配置し、これを証明すること。

① 経済産業大臣が認定する情報処理技術者（プロジェクトマネージャ）、米国ＰＭＩ認定のＰＭＰ（Project Management Professional）のいずれかの資格を有すること。

② ＰＭＢＯＫ第６版または第７版をＰＤＵ（Professional Development Units）対象の研修受講により理解していること。

③ プロジェクトの責任者として、基盤情報系システムに係る調査業務もしくは要件定義業務、調達支援業務、設計・構築業務、工程管理支援業務のいずれかの業務を遂行した実績を累計３件以上有していること。

④ プロジェクトの責任者として、中央省庁等の公共機関における情報システムに係る調査業務もしくは要件定義業務、調達支援業務、設計・構築業務、工程管理支援業務のいずれかの業務を遂行した実績を累計３件以上有していること。

(3) 業務従事者

業務従事者には以下の要件を有している者を１名以上配置し、これを証明すること。

① 情報処理技術者試験制度の「システムアーキテクト」試験の合格者又はこれらと同等の技

術水準を満たしていること。

② プロジェクトの責任者またはリーダーなど一定以上の責任を有する立場として、基盤情報系システムに係る調査業務もしくは要件定義業務、調達支援業務、設計・構築業務、工程管理支援業務のいずれかの業務を遂行した実績を有していること。

③ パブリッククラウドサービスを利用する情報システムに係る調査業務もしくは要件定義、調達支援業務のいずれかの業務を遂行した実績を有していること。

(4) 資料閲覧

業務責任者を担当する予定の者は、第７期システムの要求仕様書一式、令和 4 年度に実施している「経済産業省基盤情報システムに係るフィージビリティスタディ調査業務」の報告書、ガバメントソリューションサービス関連資料を提案書の提出締切日の前日までに閲覧すること。

10 機密保持

① 本仕様書に基づく作業の実施中はもとより、作業の実施後も、基盤情報システムの構成及び機器等に関する技術、知識及びその他本調達を履行する上で、知り得た情報を第三者に開示、漏えい又は本調達の遂行目的以外の目的で利用しないこと。また、そのために必要な措置を講ずること。

② 当省及びデジタル庁が提供する資料は、原則、作業実施場所以外への持ち出しを禁止する。ただし、担当職員の承認を得た場合に限り貸し出しを行うが、本調達の遂行中は請負者が適切な管理を実施し、また、適切な時点で担当職員又は資料提供元に返却又は抹消等を行い復元不可能な状態にすること。また、当該資料の複写及び第三者への提供はしないこと。

③ 当省及びデジタル庁が提供した情報を第三者に開示することが必要である場合は、事前に担当職員と協議の上、承認を得ること。

④ 請負者の責に起因する情報セキュリティインシデントが発生する等の万一の事故があった場合は、直ちに担当職員に報告すること。また、事故による損害が生じた場合は賠償等の責任を負うことがある。

⑤ 機密保持や資料の取扱いについて適切な措置が講じられていることを確認するため、遵守状況の報告及び当省による実施調査を求めることがあるため、請負者はこれに応じること。

11 情報管理体制

(1) 情報管理体制

① 請負者は、本業務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、当省に対し「情報取扱者名簿」（氏名、住所、生年月日、所属部署、役職等が記載されたもの）及び「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)」（別紙１）を契約前に提出し、担当職員の同意を得ること。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、契約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請負者が収集、整理、作成等した一切の情報が、当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 本業務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、担当職員の承認を得た場合はこの限りではない。

③ ①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、予め担当職員へ届出を行い、同意を得なければならない。

(2) 履行完了後の情報の取扱い

当省及びデジタル庁から提供した資料又は当省及びデジタル庁が指定した資料の取扱い（返却・削除等）については、担当職員に確認すること。

12 下請負

当省の許可なく、本業務の一部又は全部を第三者（下請負先）に請け負わせてはならない。ただし、当省が許可した場合には、契約上請負者に求められる水準と同等の情報セキュリティ水準を、下請負先においても確保すること。また、請負者は、下請負先が実施する情報セキュリティ対策及びその実施状況について報告すること。

また、本業務の一部を第三者に請け負わせる場合、請け負わせることにより生ずる脅威に対して情報セキュリティを十分に確保するため、以下の事項を下請負先に担保させること。

① 下請負先に提供する情報の下請負先における目的外利用の禁止
② 下請負先における情報セキュリティ対策の実施内容及び管理体制
③ 本業務の実施に当たり、下請負先企業又はその従業員、再下請負先、若しくはその他の者による意図せざる変更が加えられないための管理体制
④ 下請負先の資本関係・役員等の情報、本業務の実施場所、下請負事業従事者の所属・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提供
⑤ 情報セキュリティインシデントへの対処方法
⑥ 情報セキュリティ対策その他の契約の履行状況の確認方法
⑦ 情報セキュリティ対策の履行が不十分な場合の対処方法
⑧ 情報セキュリティ監査の受入れ

13 契約不適合責任

請負者は、以下の契約不適合責任を負うものとする。契約不適合責任期間は、当省による検収後１年間とする。

① 本作業にて納入する全ての納入物について、契約不適合責任を負う。
② 納入物に契約不適合があった場合には、本調達の請負者の負担と責任において関連する納入物を修正の上、提出する。

14 知的財産権の帰属

① 本業務に当たり作成・変更・更新されるドキュメント類及びプログラム等の著作権（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、請負者が本調達の実施前から権利を保有していた等の明確な理由により、予め提案書にて権利譲渡不可能と示されたもの以外は、全て当省に帰属するものとする。

② 本調達に当たり発生した権利については、請負者は著作者人格権を行使しないものとする。

③ 本調達に当たり発生した権利については、今後、二次的著作物が作成された場合等であっても、請負者は原著作権の著作権者としての権利を行使しないものとする。

④ 本調達に当たり作成・変更・修正されるドキュメント類及びプログラム等に第三者が権利を有する著作物が含まれる場合、請負者は当該著作物の使用に必要な費用負担や使用許諾契約に係る一切の手続きを行うこと。この場合は、事前に当省へ報告し、承認を得ること。

⑤ 本調達に当たり第三者が有する知的所有権を利用する場合は、請負者の責任において解決すること。

15　その他

① 業務の実施に当たっては、速やかに実施体制表を作成し、担当職員の了解を得ること。実施体制表には、プロジェクトに参画する者の氏名、所属、担当業務、指揮命令系統及び連絡先を記載すること。なお、実施体制表を変更する場合は、あらかじめ、担当職員の了解を得ること。

② 本作業に係る作業工程を細分化した WBS を作成し、作業工程毎に成果物又は工程完了の基準を定め、担当職員の承認を得ること。

③ 是正措置を講じても進捗の遅れが改善されず、本作業の納期までの完了が達せられないと認められる場合は、当省は本契約の解除事項とすることができるものとする。

④ 当省の業務時間内（平日 8:30～18:15）においては担当職員から連絡が受けられる環境を整備すること。

⑤ 請負者は、本仕様書「５　業務内容」の業務を実施するに当たり、各種製品及び機能等に関する情報収集を行う際には、標準化された技術を用いた複数の製品・サービス又はソリューションを対象として情報収集を行うこと。

⑥ 請負者は、業務遂行上不明な点がある場合、速やかに担当職員に質問し、不明点を解消すること。

⑦ 請負者は、担当職員と日本語で円滑なコミュニケーションが可能で、かつ良好な関係が保てること。

⑧ 請負者は、情報セキュリティに関して以下に掲げる事項を遵守すること。

(ｱ) 請負者は、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(ｲ)～(ﾂ)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、担当職員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」（別紙２））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、担当職員と請負者が協議し不十分であると認めた場合、請負者は、速やかに担当職員と協議し対策を講ずること。

(ｲ) 請負者は、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。

(ｳ) 請負者は、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。

(ｴ) 請負者は、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。

(ｵ) 請負者は、本業務を終了又は契約解除する場合には、請負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。

(ｶ) 請負者は、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。

(ｷ) 請負者は、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) 請負者は、「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３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。

(ｹ) 請負者は、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。

(ｺ) 請負者は、本業務に従事する者を限定すること。また、請負者の資本関係・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。

(ｻ) 請負者は、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、上記(ｱ)から(ｺ)まで及び(ｼ)から(ﾂ)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、ｱ)の確認書類には再委託先に係るものも含むこと。

(ｼ) 請負者は、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、請負者自身（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。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。

(ｽ) 請負者は、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。

(ｾ) 請負者は、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、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。

(ｿ) 請負者は、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、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。

(ﾀ) 請負者は、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。

(i) 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。

(ii) 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。

(iii) 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。

(iv) 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。

(v) 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。

(vi) 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。

(ﾁ) 請負者は、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、画一的な約款や規約等への同意のみで利用可能となる外部サービス（ソーシャルメディアサービスを含む）を利用する場合には、これらのサービスで要機密情報を扱ってはならず、(ｸ)に掲げる規程等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こと。なお、請負者は、本契約を実施するに当たり、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）」において登録されたサービスから調達することを原則とすること。

(ﾂ) 請負者は、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。

(i) 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。

(a) 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。

(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、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。

(ii) 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。

(iii) 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。

(iv) 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、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。

(v) 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、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、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。

(vi) 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、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。

⑨ 当省に提出する納入物の記載項目については、担当職員の了解を得ること。

⑩ 請負者は、担当職員が常時契約履行に関する調査を行える体制とすること。

⑪ 当省が適切な支援が期待できないと判断した場合、業務責任者を含む業務従事者の変更を依頼することがある。そのような場合には、本業務に影響しないよう配慮すること。

⑫ 本業務の円滑な遂行を実現するため、必要な時に積極的に調整等を実施すること。また、積極的に問題や課題の早期発見に努め、主体的かつ迅速に、その解決に取り組むこと。

⑬ 本業務に関係する調達案件への入札制限

本業務の請負者（下請負先を含む。）及びその関連事業者（「財務諸表等の用語、様式及び作成方法に関する規則」（昭和 38 年大蔵省令第 59 号）第 8 条に規定する親会社及び子会社、同一の親会社をもつ会社並びに委託先事業者等の緊密な利害関係を有する事業者をいう。以下同じ。）については、透明性及び公正性の観点の確保並びに相互牽制の観点から、第８期システムの設計・構築、サービス提供を実施する調達案件及びシステム管理業務を実施する調達案件への入札に参加することはできない。

16 特記事項

① 本調達は、令和５年度の予算成立を条件とする。

② 本調達の受注後に本仕様書の内容の一部について変更を行おうとする場合、その変更の内容、

理由等を明記した書面をもって当省へ申し入れを行うこと。双方の協議において、その変更内容が軽微（契約額、納期に影響を及ぼさない）かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が記名捺印することによって変更を確定する。

（別紙１）

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						
下請負先	F						

（※1）受注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。

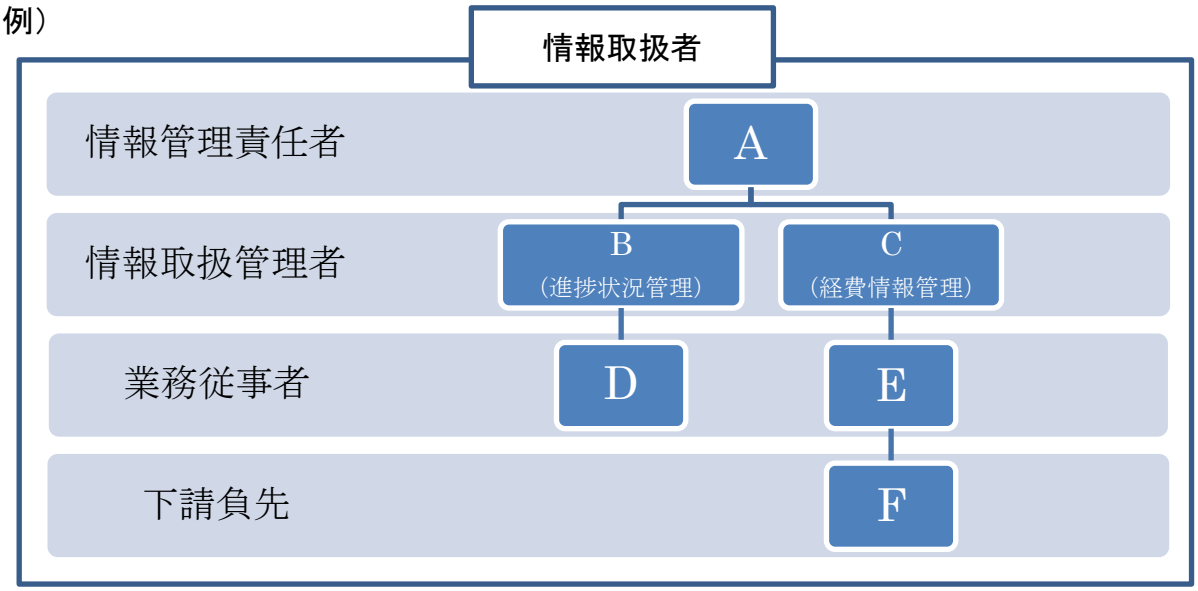
（※3）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※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。（下請負先も含む。）

・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。

別紙2

令和　　年　　月　　日

経済産業省大臣官房情報システム室長　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

15.⑧情報セキュリティに関する事項(ｱ)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(ｲ)	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(ｳ)	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(ｴ)	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(ｵ)	本業務を終了又は契約解除する場合には、請負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、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(ｶ)	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(ｷ)	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(ｸ)	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3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 (ケ)	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 (コ)	本業務に従事する者を限定する。また、請負者の資本関係・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 (サ)	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(ア)から(コ)まで及び(シ)から(ツ)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 (シ)	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、請負者が管理責任を有するサーバ等を利用する場合には、当該ウェブサイト又は当該サーバ等で利用する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。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。	
情報セキュリティに関する事項 (ス)	本業務の実施に当たって、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。 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。	
情報セキュリティに関する事項 (セ)	ウェブサイト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、ウェブサイト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。	
情報セキュリティに関する事項 (ソ)	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、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。	
情報セキュリティに関する事項 (タ)	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。 (i) 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。 (ii) 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。 (iii) 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。 (iv) 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。 (v) 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。 (vi) 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 (チ)	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、画一的な約款や規約等への同意のみで利用可能となる外部サービス（ソーシャルメディアサービスを含む）を利用する場合には、これらのサービスで要機密情報を扱ってはならず、(ク)に掲げる規程等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こと。なお、本業務を実施するに当たり、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）」において登録されたサービス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 (ツ)	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。 (i) 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、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。 (ii) 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。 (iii) 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。 (iv) 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、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。 (v) 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、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、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。 (vi) 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、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。	

記載要領

1. 「実施状況」は、情報セキュリティに関する事項(イ)から(ツ)までに規定した事項について、15.⑧情報セキュリティに関する事項(ア)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、事前に当省と相談すること。

（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））。）