

令和8年度「環境価値認証制度等整備事業費（J-クレジット制度推進のための地域支援事業 四国経済産業局）」に係る企画競争募集要領

令和8年4月24日
四国経済産業局
資源エネルギー環境部
資源エネルギー環境課

四国経済産業局（以下「当局」という。）では、令和8年度「環境価値認証制度等整備事業費（J-クレジット制度推進のための地域支援事業 四国経済産業局）」を実施する委託先を、以下の要領で広く募集します。

なお、委託契約に係るルールを一部改正し、令和5年10月16日（月）より運用を開始しています。「委託事業事務処理マニュアル」を含め、関係資料の内容を承知の上で応募してください。

1. 事業の目的

J-クレジット制度とは、中小企業等の再エネ・省エネ設備の導入や適切な森林管理による温室効果ガス排出削減量や吸収量をクレジットとして国が認証する制度であり、2025年2月18日に閣議決定された地球温暖化対策計画において定めた2030年度目標である累計1500万t-CO₂の認証目標に向けて制度運営を行っています。

J-クレジットの創出は、現状、民間企業が自主的かつ積極的にプロジェクト登録とクレジット認証を実施する動きはあるものの、排出量取引制度等、今後の需要拡大の機運が高まっていることから、大幅な供給量拡大が求められています。そのため、これまで以上に効果的かつ確実なJ-クレジットの認証を促す必要があります。

しかしながら、

- ① J-クレジットの売り先、売却益が見込めず、事業計画を立てることが難しい
- ② 認証までモニタリング期間など一定の時間を要し追加的な作業が発生する
- ③ 認証までモニタリング期間における企業内の方針転換や担当者の異動等の事情により、登録を躊躇、登録したにもかかわらず認証に結び付きにくい点も課題となっております。

以上を踏まえ、四国管内（徳島県、香川県、愛媛県、高知県）において、J-クレジットの確実な登録・認証を促し、クレジット供給量の増加に繋げるとともに、地域活性化のためのJ-クレジット創出・活用支援を実施することとします。

2. 事業の内容

以下に掲げるものについて、事業内容を具体的に提案してください。

(1) 地域密着型の新規プロジェクトの登録支援

四国経済産業局管内において、新規プロジェクトの登録を促進するためには、地域に密着したクレジットの登録を丁寧に支援していくことが重要である。そのため、地域密着型の新規プロジェクトの登録に向けた支援を行う。支援対象事業者や支援条件は、Jークレジット制度事務局の支援内容と整合をとること。

下記配点を参考に、プロジェクト登録支援を行い、令和8年度または令和9年度に登録が見込める案件について、四国経済産業局に件数の報告を行う。その合計は6pt以上となるよう努める。なお、支援の結果、令和8年度または令和9年度中の登録が難しい場合は、その要因について四国経済産業局に情報共有を行うこと。

事業提案にあたっては、過年度の登録支援状況とその実績、令和8年度の実施方針（登録支援が見込まれるプロジェクトの概要や想定件数等）について記載すること。

(1件当たりの配点)

- | | |
|---------------|-----|
| ①プログラム型プロジェクト | 6pt |
| ②通常型プロジェクト | 3pt |

①プログラム型プロジェクト

プログラム型プロジェクトの運営・管理者になり得る四国局管内の金融機関、コンサル、大企業、地方自治体等にアプローチを行い、プログラム型プロジェクトの登録に向けた書類作成支援（書類作成代行は行わず、将来的にはプロジェクト実施者が自立してクレジット創出の手続きが行えるよう、書類作成のアドバイス、相談対応等）を行う。

②通常型のプロジェクト

例えば、今後、森林分野の吸収系クレジットの需要拡大が見込まれることや四国管内でのポテンシャルもあることから、四国局管内の森林分野のプロジェクト登録に向けた書類作成支援を行う。そのために金融機関、自治体や森林分野に係る事業を実施している事業者等に対し、Jークレジット制度の提案を行い、クレジットの創出に意欲のある事業者に対して、プロジェクトの登録に向けた書類作成支援を行う。

(2) クレジット認証に向けたフォローを含む相談対応等

前年度登録支援を行ったプロジェクトについて継続的に相談対応することや、既に登録されているプロジェクト等について事業者の置かれた状況について確認・相談対応を行い、認証申請への後押しをする他、要請に応じてJ-クレジット認証委員会への申請を前提とした書類作成のアドバイスを行う。支援対象事業者や支援条件は、J-クレジット制度事務局の支援内容と整合を取る。取り組みは、精査の上整理し、内容と件数について報告を行う。

また、J-クレジットの登録と認証支援に係る問い合わせ等に限らず、購入等についての相談・質問等に対応し、要望に応じて管轄地域の自治体や業界団体等が主催する勉強会及びセミナーで講師対応等を行う。

講師対応予定回数：1回程度

事業提案にあたっては、相談体制や過年度の認証支援状況とその実績、令和8年度の実施方針（可能な範囲で相談対応・認証支援を行っている、または見込まれるプロジェクトの概要や件数等）について記載すること。

(3) 地域のJ-クレジット創出・活用の促進に寄与する支援・取り組みの実施

① J-クレジット制度説明会の周知

J-クレジットの創出・活用・流通に関するJ-クレジット制度の認知度向上、活性化を目的とした制度説明会をJ-クレジット制度事務局にて開催するため、地域内への周知を行う。

② 制度の普及啓発及び案件組成を目的とした個別訪問等

J-クレジット制度の普及促進、クレジットの供給量拡大や需要の掘り起こし等に繋げるため、四国管内の自治体や企業等へ個別訪問等（先方の状況に応じてオンライン対応も可）を行い、ヒアリングや制度説明等を行う。

訪問等目標件数：8件程度

事業提案にあたっては、アプローチ予定の自治体や企業等の概要、アプローチの方向性等について記載すること。

3. 事業実施期間

契約締結日～令和9年3月17日（水）

4. 応募資格

応募資格：次の要件を満たす企業・団体等とします。

本事業の対象となる申請者は、次の条件を満たす法人とします。

- ① 日本に拠点を有していること。
- ② 本事業を的確に遂行する組織、人員等を有していること。

- ③ 本事業を円滑に遂行するために必要な経営基盤を有し、かつ、資金等について十分な管理能力を有していること。
- ④ 予算決算及び会計令第70条及び第71条の規定に該当しないものであること。
- ⑤ 経済産業省からの補助金交付等停止措置又は指名停止措置が講じられている者ではないこと。
- ⑥ 過去3年以内に情報管理の不備を理由に経済産業省との契約を解除されている者ではないこと。

なお、コンソーシアム形式による申請も認めますが、その場合は幹事法人を決めていただくとともに、幹事法人が事業提案書を提出して下さい。(ただし、幹事法人が業務の全てを他の法人に再委託することはできません。)

5. 契約の要件

- (1) 契約形態：委託契約（概算契約）
- (2) 採択件数：1件
- (3) 予算規模：5,690千円（消費税及び地方消費税を含む）を上限とします。
なお、最終的な実施内容、契約金額については、当局と調整した上で決定することとします。
- (4) 成果物の納入：事業報告書の電子媒体（PDF形式）を当局に納入すること。
- (5) 委託金の支払時期：委託金の支払いは、原則として、事業終了後の精算払となります。

※本事業に充てられる自己資金等の状況次第では、事業終了前の支払い（概算払）も可能ですので、希望する場合は個別にご相談ください。

- (6) 支払額の確定方法：事業終了後、事業者より提出いただく実績報告書に基づき原則として現地調査を行い、支払額を確定します。
支払額は、契約金額の範囲内であって実際に支出を要したと認められる費用の合計となります。このため、全ての支出には、その収支を明らかにした帳簿類及び領収書等の証拠書類が必要となります。また、支出額及び内容についても厳格に審査し、これを満たさない経費については、支払額の対象外となる可能性もあります。

6. 応募手続き

(1) 募集期間

募集開始日：令和8年4月24日（金）

募集締切日：令和8年5月29日（金）17時必着

(2) 説明会の開催

開催日時：令和8年5月11日（月）14時～15時

開催方法：オンライン（Microsoft Teams を使用）

説明会への参加を希望する方は、「13. 問い合わせ先」へ連絡先（社名、担当者氏名、電話番号、メールアドレス）を令和8年5月7日（木）12時までに登録してください。ご登録いただきましたメールアドレスに参加 URL 等をご連絡します。（事前にテスト連絡をさせていただく場合があります。）

「Microsoft Teams」が利用できない場合は、概要を共有させていただきますので、その旨を連絡していただくとともに連絡先を登録してください。

(3) 応募書類

① 以下の書類を電子媒体（PDF 形式）で（4）により提出してください。

- ・申請書（様式1）
- ・企画提案書（様式2及び別紙の「支出計画」）
- ・申請受理票（様式3）
- ・申請者（提案企業・団体）に関する概要票（様式4）

② 提出された応募書類は本事業の採択に関する審査以外の目的には使用しません。なお、応募書類は返却しません。

③ 応募書類等の作成費は経費に含まれません。また、選定の正否を問わず、応募書類の作成費用は支給されません。

④ 企画提案書に記載する内容については、今後の契約の基本方針となりますので、予算額内で実現が確約されることのみ表明してください。なお、採択後であっても、申請者の都合により記載された内容に大幅な変更があった場合には、不採択となることがあります。

(4) 応募書類の提出先

応募書類はメールにより「13. 問い合わせ先」に記載の E-mail アドレスに提出してください。

※資料に不備がある場合は、審査対象となりませんので、記載要領等を熟読の上、注意して記入してください。

7. 審査・採択について

(1) 審査方法

採択にあたっては、第三者の有識者で構成される委員会で審査を行い決定します。なお、応募期間締切後に、必要に応じて提案に関するヒアリングを実施します。

(2) 審査基準

以下の審査基準に基づいて総合的な評価を行います。

- ① 申請者としての適格性について
- ア. 4. の応募資格を満たしているか。
 - イ. 事業全体の企画及び立案並びに根幹に関わる執行管理部分について、再委託(委託業務の一部を第三者に委託することをいい、請負その他委託の形式を問わない。以下同じ。)を行っていないか。
 - ウ. 事業費総額に対する再委託費の割合が50%を超えないか。超える場合は、相当な理由があるか(「再委託費率が50%を超える理由書」を作成し提出すること)。
- ② 提案事業の実施内容・方法・スケジュールについて
- ア. 事業内容が全て提案されており、また、その内容が事業の目的に合致しているか。
 - イ. 提案事業の実施内容・方法・スケジュールが具体的に示されており、また、その実現性が高いか。
 - ウ. 提案事業において、実施方針(支援先の想定等)が充実しており、その費用対効果が高いか。また、必要となる経費・費目を過不足無く考慮し、適正な積算が行われているか。
- ③ 提案事業を実施する体制・基盤について
- ア. 当該事業を効果的に遂行するために必要なネットワークを保有しているか。
 - イ. 四国地域での広域で事業を実施出来る体制が取られているか。
 - ウ. 当該事業を行うのに適切な財政基盤、一般的な経理処理能力を有しているか。
 - エ. 欠員等が生じた際に、事業遂行が円滑にいく体制が取られているか。
 - オ. 適切な情報管理体制が確保されているか。また、情報取扱者以外の者が情報に接することがないか。
- ④ 過去の実績・業務処理能力について
- ア. 過去に当事業と同様の支援事業を受託した事業者にあつては、支援実績が十分であるか。
 - イ. 業務従事予定者が、以下の(i)～(iii)に記載する内容等について、知見・業務実績を有しているか。
 - (i) 国内クレジット制度、J-クレジット制度
 - (ii) 中小企業等の温室効果ガス排出削減対策及び温室効果ガス排出削減量の算定
 - (iii) 省エネ診断や省エネ量の測定等の省エネ関連事業
 - ウ. 業務従事予定者の経歴・所持資格・業務実績等が、当該業務遂行の前提素養・キャリアとして十分であるか。
- ⑤ 事業遂行上の独自提案等について
- ア. 提案事業において、独自の提案や事業効果を高めるための独創的な工夫がなされているか。
- ⑥ ワーク・ライフ・バランス等の推進について

ア. ワーク・ライフ・バランス等の推進企業（団体）であるか。

(3) 採択結果の決定及び通知について

採択された申請者については、当局のホームページで公表するとともに、当該申請者に対してその旨を通知します。

8. 契約について

(1) 採択された申請者について、国と提案者との間で委託契約を締結することになります。なお、採択決定後から委託契約締結までの間に、当局との協議を経て、事業内容・構成、事業規模、金額などに変更が生じる可能性があります。

契約書作成に当たっての条件の協議が整い次第、委託契約を締結し、その後、事業開始となりますので、あらかじめご承知おきください。また、契約条件が合致しない場合には、委託契約の締結ができない場合もありますのでご了承ください。

契約条項は、基本的には以下の内容となります。

○概算契約書

https://www.shikoku.meti.go.jp/02_soshikiinfos/04_kaikei/koukoku/download/files/r8gaisan_format.pdf

また、委託事業の事務処理・経理処理につきましては、経済産業省の作成する委託事業事務処理マニュアルに従って処理していただきます。

https://www.meti.go.jp/information_2/publicoffer/jimusyori_manual.html

なお、契約締結後、受託者に対し、事業実施に必要な情報等を提供することがありますが、情報の内容によっては、守秘義務の遵守をお願いすることがあります。

(2) 再委託比率が50%を超える場合

- ・総額に対する再委託の割合が50%を超えないか。超える場合は、相当な理由があるか（「再委託費率が50%を超える理由書」を作成し提出すること）。
- ・再委託を行う場合、グループ企業との取引であることのみを選定理由とした調達は、原則、認めない（経済性の観点から、相見積りを取り、相見積りの中で最低価格を提示した者を選定すること）。
- ・提案書等において再委託費率が50%を超える理由書を添付した場合には、経済産業省で再委託内容の適切性などを確認し、落札者に対して、契約締結までに履行体制を含め再委託内容の見直しの指示をする場合がある。

<事業類型>

- I. 多数の事業者を管理し、その成果を取りまとめる事業
(主に海外法人等を活用した標準化や実証事業の取りまとめ事業)
- II. 現地・現場での作業に要する工数の割合が高い事業

(主に海外の展示会出展支援やシステム開発事業)

Ⅲ. 多数の事業者の協力が必要となるオープン・イノベーション事業

(主に特定分野における専門性が極めて高い事業)

9. 経費の計上

(1) 経費の区分

本事業の対象とする経費は、事業の遂行に直接必要な経費及び事業成果の取りまとめに必要な経費であり、具体的には以下のとおりです。

経費項目	内容
I. 人件費	事業に従事する者の直接作業時間に対する人件費
II. 事業費	
旅費	事業を行うために必要な国内出張及び海外出張に係る経費
会場費	事業を行うために必要な会議、講演会、シンポジウム等に要する経費（会場借料、機材借料及び茶菓料（お茶代）等）
謝金	事業を行うために必要な謝金（会議・講演会・シンポジウム等に出席した外部専門家等に対する謝金、講演・原稿の執筆・研究協力等に対する謝金等）
備品費	事業を行うために必要な物品（ただし、1年以上継続して使用できるもの）の購入、製造に必要な経費
(借料及び損料)	事業を行うために必要な機械器具等のリース・レンタルに要する経費
消耗品費	事業を行うために必要な物品であって備品費に属さないもの（ただし、当該事業のみで使用されることが確認できるもの。）の購入に要する経費
印刷製本費	事業で使用するパンフレット・リーフレット、事業成果報告書等の印刷製本に関する経費
補助職員人件費	事業を実施するために必要な補助員（アルバイト等）に係る経費
その他諸経費	事業を行うために必要な経費のうち、当該事業のために使用されることが特定・確認できるものであって、他のいずれの区分にも属さないもの 例) 通信運搬費（郵便料、運送代、通信・電話料等） 光熱水料（電気、水道、ガス。例えば、大規模な研究施設等について、専用のメータの検針により当該事業に使用した料金が算出できる場合） 設備の修繕・保守費

	翻訳通訳、速記費用 文献購入費、法定検査、検定料、特許出願関連費用等
Ⅲ. 再委託費・外注費	受託者が直接実施することができないもの又は適当でないものについて、他の事業者にも再委託するために必要な経費 ※改正前の委託事業事務処理マニュアルにおける経費項目である「外注費」と「再委託費」のことを言う。
Ⅳ. 一般管理費	委託事業を行うために必要な経費であって、当該事業に要した経費としての抽出、特定が困難なものについて、委託契約締結時の条件に基づいて一定割合の支払を認められた間接経費

(2) 直接経費として計上できない経費

- ・建物等施設に関する経費
- ・事業内容に照らして当然備えているべき機器・備品等(机、椅子、書棚等の什器類、事務機器等)
- ・事業実施中に発生した事故・災害の処理のための経費
- ・その他事業に関係のない経費

10. 情報管理体制

- (1) 受託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)様式5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、四国経済産業局が保護を要し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。

- (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、予め担当課室へ届出を行い、同意を得なければならない。

1 1. 履行完了後の情報の取扱い

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。業務日誌を始めとする経理処理に関する資料については適切に保管すること。

1 2. その他

- (1) 本委託事業において、業務情報を取り扱う場合又は業務情報を取り扱う情報システムやウェブサイトの構築・運用等を行う場合、別記「情報セキュリティに関する事項」を遵守し、情報セキュリティ対策を実施してください。

- (2) 事業終了後、提出された実績報告書に基づき、原則、現地調査を行い、支払額を確定します。支払額は、委託契約額の範囲内で、事業に要した費用の合計となります。調査の際には、全ての費用を明らかにした帳簿類及び領収書等の証拠書類が必要となります。当該費用は、厳格に審査し、事業に必要と認められない経費等については、支払額の対象外となる可能性もあります。

- (3) 委託事業の事務処理・経理処理につきましては、経済産業省の作成する委託事業事務処理マニュアルに従って処理していただきます。

https://www.meti.go.jp/information_2/publicoffer/jimusyori_manual.html

① 再委託、外注に関する体制等の確認（提案要求事項の追加等）

- ・事業全体の企画及び立案並びに根幹に関わる執行管理について再委託を行っていないか。なお、「委託事業事務処理マニュアル」上で明示している、本事業における再委託を禁止している「事業全体の企画及び立案並びに根幹に関わる執行管理業務」については以下の通り。

【事業全体の企画及び立案並びに根幹に関わる執行管理業務】

- ・事業内容の決定（実施手段・方法、対象者、スケジュール、実施体制）
- ・再委託・外注先の業務執行管理（再委託・外注内容の決定、進捗状況の管理方法及び確認、成果及び結果のとりまとめ方法、とりまとめ）
- ・報告書（構成及び作成、再委託・外注先の内容のとりまとめ）

② 一般管理費率の算出基礎の見直し

（一般管理費＝（人件費＋事業費）（再委託・外注費を除く）×一般管理費率）

- (4) 委託費を不正に使用した疑いがある場合には、経済産業省より落札者に対し必要

に応じて現地調査等を実施する。また、事業に係る取引先（再委託先、外注（請負）先以降も含む）に対しても、必要に応じ現地調査等を実施するため、あらかじめ落札者から取引先に対して現地調査が可能となるよう措置を講じておくこと。

調査の結果、不正行為が認められたときは、当該委託事業に係る契約の取消を行うとともに、経済産業省から新たな補助金の交付と契約の締結を一定期間（最大36ヵ月）行わないこと等の措置を執るとともに当該事業者の名称及び不正の内容を公表する。

具体的な措置要領は、以下の URL の通り。

https://www.meti.go.jp/information_2/publicoffer/shimeiteishi.html

(5) 「ビジネスと人権に関する行動計画の実施に係る関係府省庁施策推進・連絡会議」

（令和5年4月3日決定）において、政府の実施する公共調達においては、入札する企業における人権尊重の確保に努めるとされたことを受け、当該事業の落札者に対しては「責任あるサプライチェーン等における人権尊重のためのガイドライン」（令和4年9月13日ビジネスと人権に関する行動計画の実施に係る関係府省庁施策推進・連絡会議決定）を踏まえて人権尊重に取り組むよう努めることを求めている。当該ガイドラインの内容を承知の上で、入札をすること。

<https://www.meti.go.jp/press/2022/09/20220913003/20220913003-a.pdf>

(6) 提出された企画提案書等の応募書類及び委託契約書の規定に基づき提出された実績報告書等については、「行政機関の保有する情報の公開に関する法律」（平成11年5月14日法律第42号）に基づき、不開示情報（個人情報及び法人等又は個人の権利、競争上の地位その他正当な利益を害するおそれがあるもの等）を除いて、情報公開の対象となります。なお、開示請求があった場合は、以下に掲げる書類は調整を行わずとも原則開示とし、その他の書類の不開示とする情報の範囲について経済産業省との調整を経て決定することとします。

○原則開示とする書類

・提案書等に添付された「再委託費率が50%を超える理由書」

※不開示情報に該当すると想定される情報が含まれる場合は、当該部分を別紙として分けて作成することとします。別紙について開示請求があった場合には、不開示とする情報の範囲については経済産業省と調整を経て決定することとします。

13. 問い合わせ先

〒760-8512

香川県高松市サンポート3-33

四国経済産業局 資源エネルギー環境部 資源エネルギー環境課

担当者：新川、石橋

E-mail：bzl-cn-shikoku@meti.go.jp

お問い合わせは電子メールでお願いします。電話でのお問い合わせは受付できません。なお、お問い合わせの際は、件名（題名）を必ず「令和8年度環境価値認証制度等整備事業費」としてください。他の件名（題名）ではお問い合わせに回答できない場合があります。

以 上

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及び遵守状況の報告】

- 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」（別紙））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 7 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、当省又は内閣官房国家サイバー統括室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、上記 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、リスクが許容出来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・閉鎖】

- 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

ラ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。

- ・サービス開始前及び、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ずること。

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）、DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication,

Reporting & Conformance) による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。

⑩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は、ドメインに関する情報が正確であることの定期的な確認、当省が指定する期日にドメインの抹消、DNS や CDN 情報の削除、運用環境の削除を行える事業者を選定すること。

また、運用を閉鎖する場合は、終了告知を一定期間行うこと。一定期間の終了告知を終えた後は、ドメインの抹消、DNS や CDN 情報の削除、ドメインへのリンクの削除、SNS を利用していた場合はアカウント削除等、なりすましの防止策を漏れなく講ずること。なお、本事項は、「実施」の場合はその実施内容、「未実施」又は「該当なし」の場合はその理由等を必ず報告すること。

【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に、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に開発すること。ただし、必要があつ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が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つた場合は、それに従うこと。

令和 年 月 日

四国経済産業局〇〇〇課長 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7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国家サイバー統括室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、リスクが許容出来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。	

	<p>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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <ul style="list-style-type: none"> ・サービス開始前及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ずること。 ・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。 <p>(9) 電子メール送受信機能を含む場合には、SPF（Sender Policy Framework）DKIM（DomainKeys Identified Mail）、DMARC（Domain-based Message Authentication, Reporting & Conformance）による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。</p> <p>(10) 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は、ドメインに関する情報が正確であることの定期的な確認、当省が指定する期日にドメインの抹消、DNSやCDN情報の削除、運用環境の削除を行える事業者を選定すること。</p> <p>また、運用を閉鎖する場合は、終了告知を一定期間行うこと。一定期間の終了告知を終えた後は、ドメインの抹消、DNSやCDN情報の削除、ドメインへのリンクの削除、SNSを利用していた場合はアカウント削除等、なりすましの防止策を漏れなく講ずること。</p> <p>なお、本事項は、「実施」の場合はその実施内容、「未実施」又は「該当なし」の場合はその理由等を必ず報告すること。</p>	
<p>情報セキュリティに関する事項 16)</p>	<p>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。</p> <p>(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。</p> <p>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。</p> <p>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</p>	

	<p>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。</p> <p>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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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に、アプリケーション・コンテンツの提供方法を定めて開発すること。</p> <p>(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に開発すること。ただし、必要があつ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。</p>	
<p>情報セキュリティに関する事項 1 7)</p>	<p>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。</p> <p>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つた場合には、その指示に従う。</p>	

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1 7) 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)).)