

仕様書（案）

1. 事業名

令和8年度中小企業等産業公害防止対策調査事業（カンボジア等における公害防止管理
制度支援調査）

2. 事業目的

我が国では、高度経済成長期に産業公害が社会問題化し、国民の不安と批判を招来するとともに産業の健全な発展に支障を及ぼしかねない事態となっていたことを踏まえ、「特定工場における公害防止組織の整備に関する法律」（昭和46年法律第107号）に基づく公害防止管理者の設置を義務づけた。これは、事業者による公害防止体制の整備や積極的な公害防止対策投資、関連する技術開発・普及や人材育成を促し、官民挙げて、各種環境関連法令の遵守を徹底に取り組むことにつながったため、事業者による効率的かつ実効性の高い公害対策が実現された。

こうした経験は、これから経済発展しようとしている新興国に活かすことができるため、第11回日メコン経済大臣会合（令和元年9月）において採択された「メコン産業開発ビジョン2.0」（MIDV2.0）のワークプログラムや日・カンボジア首脳会談（令和7年5月）において合意された経済共創パッケージにおいて公害防止管理制度の支援が登録されている。なお、メコン地域においては、産業界の環境管理に関する知識が不十分なため、環境投資が十分に行われず、環境関連規制も十分に機能しておらず、事業者の公害防止管理体制の構築の検討が解決策の一つとなり得る。

係る観点から、本事業は、MIDV2.0のフォローアップや日・カンボジア経済共創パッケージの履行のために必要となるカンボジア王国等の公害防止管理体制整備支援に関する調査及び日本の公害防止管理者制度の知見並びに経験の共有等を行うことを目的とする。

3. 契約期間

契約締結日から令和9年3月25日（木）

4. 業務内容及び方法

昨年度は、カンボジア王国及びラオス人民民主共和国（以下、「カンボジア等」という）の公害防止管理制度構築に向けて、公害防止管理制度の運用のあり方や講習カリキュラム等を検討するための意見交換を現地及びオンラインにて実施した。また、カンボジア王国においては、日本の公害防止管理制度や同国の制度運営等のための知識習得のため、訪日研修を実施した。ラオス人民民主共和国においては、同国の公害防止管理制度に関する理解の促進等のため、現地でのセミナー等も合わせて実施した。

こうした点を踏まえた本年度の業務内容及び方法は次のとおり。

- (1) メコン地域の公害防止管理実態把握等を通じたM I D V 2. 0のフォローアップ
現地の政府機関、日系企業、関連機関等から得られる情報を元に、調査対象の公害防止に関する法令運用やその人材育成方策の検討に協力し、日本の公害防止管理制度の知見や経験を踏まえた必要な施策を提案する。

調査対象はカンボジア王国及びラオス人民民主共和国を予定。

① カンボジア王国

(A) 現地政府機関等との政策対話を通じた公害防止に関する法令運用協力の支援

(ア) 公害防止体制整備検討対話の実施

- ・現地政府機関等で構成した公害防止体制整備検討対話を実施する。次の項目をテーマとして公害防止に関する法令に基づく講習等の運用等に関する意見交換を行う。その他、必要となる議論テーマ及び参加者等については経済産業省と事前に協議の上、同省の指示に従うこと。
- ・公害防止体制整備検討対話はオンライン又は現地にて対面で2回程度（1回目はオンライン、2回目はオンライン又は現地にて対面を想定）とする。なお、現地にて対面の場合は下記の①（A）（イ）又は（B）のいずれかで合わせて実施することとし、経済産業省と事前に協議の上、同省の指示に従うこと。

（議論テーマ）

- －事業説明及びスケジュールの確認
- －公害防止に関する法令に基づく講習や資格制度の運営等
- －公害防止に関する指導者及び担当者の育成方策等
- －現地政府との間で、令和8年度の調査・協力内容を整理した上で、会議における説明を行うこと。
- －現地政府との間で、令和8年度の調査・協力状況の確認
- －現地政府との間で、令和8年度の調査・協力結果や、制度及び講習の運用のあり方、今後の協力体制等を整理した上で、会議における説明を行うこと。

(イ) ワーキンググループ会議

現地の専門家や技術者等で構成したワーキンググループ（以下、「WG」という）を設置する。WGで実施する内容等は、以下のとおり。

- ・公害防止に関する法令に基づく講習のツールの作成及び講習の運営に関する意見交換等を行う。WGの開催はオンライン及び現地にて対面で2回程度（オンライン及び現地にて対面：各1回程度を想定）とする。
- ・必要に応じて、現地政府機関や大学教授等の学識経験者、現地の事業者等もメンバーに加える。
- ・実施内容については、経済産業省と事前に協議の上、同省の指示に従うこと。

(B) 公害防止に関する法令に基づく講習や資格制度の運営等の支援

公害防止に関する法令に基づく模擬講習等を本年度中に実施予定である。作成した講習教材や開催する模擬講習等について、アドバイス及び改善に向けたフィードバック等をオンライン又は現地にて対面で2回程度（オンライン：1回程度、現地にて対面：1回程度を想定）実施する。また、講習教材の作成に当たり、翻訳（翻訳する資料は、英語からクメール語の翻訳、21,000単語程度を想定。）に伴う支援を行う。実施内容については、経済産業省と事前に協議の上、同省の指示に従うこと。

② ラオス人民民主共和国

(A) 現地政府機関等との政策対話を通じた公害防止に関する法令運用協力の支援

(ア) 公害防止体制整備検討対話の実施

- ・現地政府機関等で構成した公害防止体制整備検討対話を実施する。次の項目テーマとして公害防止に関する法令に基づく講習等の運用等に関する意見交換を行う。その他、必要となる議論テーマ及び参加者等については経済産業省と事前に協議の上、同省の指示に従うこと。
- ・公害防止体制整備検討対話はオンライン2回程度とする。
（議論テーマ）
 - －事業説明及びスケジュールの確認
 - －公害防止に関する法令に基づく講習のフォローアップ等
 - －現地政府との間で、令和8年度の調査・協力内容を整理した上で、会議における説明を行うこと
 - －現地政府との間で、令和8年度の調査・協力状況の確認
 - －現地政府との間で、令和8年度の調査・協力結果や、制度及び講習の運用のあり方、今後の協力体制等を整理した上で、会議における説明を行うこと。

(イ) ワーキンググループ会議

現地の専門家や技術者等で構成したワーキンググループ（WG）を設置する。WGで実施する内容等は、以下のとおり。

- ・講習制度や公害防止に関する法令に基づく講習のフォローアップ等とする。WGの開催はオンライン又は現地にて対面の1回程度とする。なお、現地にて対面の場合は下記の②（B）と合わせて実施することとし、経済産業省と事前に協議の上、同省の指示に従うこと。
- ・必要に応じて、現地政府機関や大学教授等の学識経験者、現地の事業者等もメンバーに加える。
- ・実施内容等については、経済産業省と事前に協議の上、同省の指示に従うこと。

(B) 公害防止に関する法令に基づく講習や資格制度の運営等の支援

公害防止に関する法令に基づく講習や資格制度の運営等が本年度中に実施されることから、現地にて対面1回程度で当該講習や資格制度の運営に係る会議等に立ち合いの上、アドバイス及び改善に向けたフィードバック等の支援を行う。実施内容については、経済産業省と事前に協議の上、同省の指示に従うこと。

③ 留意事項

上記の①及び②について、留意事項は以下のとおり。

- ・(A) 及び (B) の業務において、オンライン会議等を活用したカウンターパート等との協議の機会を設けるにあたり、オンライン会議システムは、Microsoft Teams (又はCisco Webex meetings) を用いることとし、請負者において、カウンターパート等が会議に参加する上での技術的サポートを行うこととする。
- ・(A) 及び (B) の業務において、円滑なコミュニケーションが行えるよう、日本語と現地語との間の通訳を手配すること。なお、日本側の関係者は、経済産業省会議室又は請負者の会議室からオンライン会議に参加する。
- ・(A) 及び (B) の会議等の開催にあたり、カウンターパート等と電子メール等で事前にコンタクトを取り、日程調整や議題設定を行うほか、資料の作成、会場手配、機材準備、関係者への資料事前送付、専門家等への謝金・交通費(実費支給)の支払い等、会議等運営に係る業務は請負者が行うものとする。議題や資料案の作成にあたっては、経済産業省と事前に協議すること。なお、専門家等謝金は、1名あたり14,000円/回を上限とする。
- ・(A) 及び (B) の業務では、制度構築及び講習の実施・運営等に係る詳細な議論が想定されるため、公害防止管理者の有資格者や同制度に精通した者及び現地環境法令の知見を有する者2名以上をもって充てること。
- ・(A) 及び (B) の業務において、やむを得ない事情により実施が難しい場合は、経済産業省と相談の上、同省の指示に従うこと。
 - ・カンボジア王国政府機関 (カウンターパート)
工業科学技術革新省工業総局 (General Department of Industry, Ministry of Industry, Science, Technology and Innovation) (M I S T I)
 - ・ラオス人民民主共和国政府機関 (カウンターパート)
商工業省工業局 (Department of Industry, Ministry of Industry and Commerce) (M O I C)

(2) 業務報告書の作成

上記(1)の各工程において実施した内容等を踏まえて、業務報告書及びその概要版(PPT数枚)を作成する。

5. 納入物

(1) 業務報告書 (概要版含む)

報告書は電子媒体（PDF形式及び機械判読可能な形式）で3.までにメール等で提出すること。

(2) 納入場所

経済産業省 イノベーション・環境局 環境管理推進室（別館5階508号室）

(3) 納入期限

令和9年3月25日（木）

6. その他

- ・本業務において得られた情報は、厳重に管理し、紛失防止等を講じるとともに、本事業実施者は業務終了後、情報等を破棄すること。
- ・本仕様書及び契約条項に定めていない事項については、担当職員の指示に従うものとする。契約条項は以下を参照すること。
https://www.meti.go.jp/information_2/publicoffer/keiyaku_format.html
- ・会議（検討会、研究会及び委員会を含む。）を運営する場合は、別記2「会議運営について」に基づき、会議運営実績報告書を納入物とともに提出すること。

7. 情報セキュリティに関する事項

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すること。

8. 情報管理体制

- (1) 請負人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、注文者に対し「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）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、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。

9. 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。

10. 情報セキュリティに関する事項

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すること。

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。

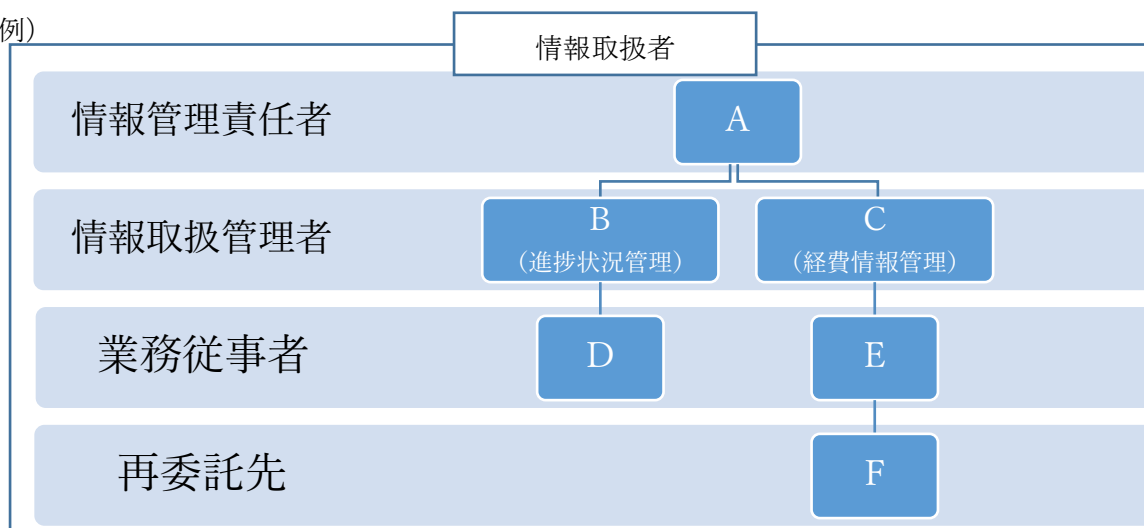
(※3) 本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

(※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。

会議運営について

会議（検討会、研究会及び委員会を含む。）を運営する場合は、国等による環境物品等の調達に関する法律（平成12年法律第100号）第6条第1項の規定に基づき定められた環境物品等の調達の推進に関する基本方針による以下会議運営の基準を満たすこととし、様式により作成した会議運営実績報告書を納入物とともに提出すること。

22-13 会議運営

(1) 品目及び判断の基準等

会議運営	<p>【判断の基準】</p> <p>○会議の運営を含む業務の実施に当たって、次の項目に該当する場合は、該当する項目に掲げられた要件を満たすこと。</p> <p>①紙の資料を配布する場合は、適正部数の印刷、両面印刷等により、紙の使用量の削減が図られていること。また、紙の資料として配布される用紙が特定調達品目に該当する場合は、当該品目に係る判断の基準を満たすこと。</p> <p>②ポスター、チラシ、パンフレット等の印刷物を印刷する場合は、印刷に係る判断の基準を満たすこと。</p> <p>③紙の資料及び印刷物等の残部のうち、不要なものについてはリサイクルを行うこと。</p> <p>④会議参加者に対し、会議への参加に当たり、環境負荷低減に資する次の取組の奨励を行うこと。</p> <p>ア. 公共交通機関の利用 イ. クールビズ及びウォームビズ ウ. 筆記具等の持参</p> <p>⑤飲料を提供する場合は、次の要件を満たすこと。</p> <p>ア. ワンウェイのプラスチック製の製品及び容器包装を使用しないこと。 イ. 繰り返し利用可能な容器等を使用すること又は容器包装の返却・回収が行われること。</p> <p>【配慮事項】</p> <p>①会議に供する物品については、可能な限り既存の物品を使用すること。また、新規に購入する物品が特定調達品目に該当する場合は、当該品目に係る判断の基準を満たすこと。</p> <p>②ノートパソコン、タブレット等の端末を使用することにより紙資源の削減を行っていること。</p> <p>③自動車により資機材の搬送、参加者の送迎等を行う場合は、可能な限り、電動車等又は低燃費・低公害車が使用されていること。また、エコドライブに努めていること。</p> <p>④食事を提供する場合は、ワンウェイのプラスチック製の製品及び容器包装を使用しないこと。</p> <p>⑤資機材の搬送に使用する梱包用資材については、可能な限り簡易であって、再生利用の容易さ及び廃棄時の負荷低減に配慮されていること。</p>
------	--

備考 1 「電動車等又は低燃費・低公害車」とは、環境物品等の調達の推進に関する基本方針に示した「13-1 自動車」を対象とする。

2 「エコドライブ」とは、エコドライブ普及連絡会作成「エコドライブ10のすすめ」（令和2年1月）に基づく運転をいう。

（参考）①自分の燃費を把握しよう②ふんわりアクセル『eスタート』③車間距離にゆとりをもって、加速・減速の少ない運転④減速時は早めにアクセルを離そう⑤エアコンの使用は適切に⑥ムダなアイドリングはやめよう⑦渋滞を避け、余裕をもって出発しよう⑧タイヤの空気圧から始める点検・整備⑨不要な荷物はおろそう⑩走行の妨げとなる駐車はやめよう

支出負担行為担当官

経済産業省大臣官房会計課長 殿

住 所

名 称

担当者氏名

会議運営実績報告書

契約件名：令和〇〇年度〇〇〇

会議（検討会、研究会及び委員会を含む。）の運営を営む業務の実施に当たって、次の項目に該当する場合は、該当する項目に掲げられた要件の実績を記載すること。

基 準	実 績	基準を満たせなかった理由
<ul style="list-style-type: none"> ・紙の資料を配布する場合は、適正部数の印刷、両面印刷等により、紙の使用量の削減が図られていること。また、紙の資料として配布される用紙が特定調達品目に該当する場合は、当該品目に係る判断の基準を満たすこと。 ・ポスター、チラシ、パンフレット等の印刷物を印刷する場合は、印刷に係る判断基準を満たすこと。 ・紙の資料及び印刷物等の残部のうち、不要なものについてはリサイクルを行うこと。 		
<ul style="list-style-type: none"> ・会議参加者に対し、会議への参加に当たり、環境負荷低減に資する次の取組の奨励を行うこと。 <ul style="list-style-type: none"> ア．公共交通機関の利用 イ．クールビズ及びウォームビズ ウ．筆記具等の持参 		
<ul style="list-style-type: none"> ・飲料を提供する場合は、次の要件を満たすこと。 <ul style="list-style-type: none"> ア．ワンウェイのプラスチック製の製品及び容器包装※を使用しないこと。 イ．繰り返し利用可能な容器等を使用すること又は容器包装の返却・回収が行われること。 		

記載要領

1. 契約において複数回会議を運営した場合、全会議を総合して判断すること。
 2. 実績については、すべての基準が満たせた場合は、「○」を記載し、基準を満たせなかった項目があった場合は、「×」を記載し基準を満たせなかった理由を記載すること。該当しない項目基準については「-」を記載すること。
- ※ワンウェイのプラスチック製の製品及び容器包装とは、一般的に一度だけ使用した後に廃棄することが想定されるプラスチック製のもので、具体的には、飲料用のペットボトル、カップ、カップの蓋、ストロー、マドラー、シロップやミルクの容器等を指す。

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、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った場合は、それに従うこと。

令和 年 月 日

経済産業省〇〇〇課長 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	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	

10)	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)	<p>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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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> <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。 <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> <ol style="list-style-type: none"> 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と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と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>(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、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。</p>	

<p>情報セキュリティに関する事項 17)</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。 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。</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））。