20240809財東北第1号

経済産業省 関東東北産業保安監督部 東北支部ウェブサイトのウェブアクセシビリティ試験評価業務に係る請負先の公募について

下記について請負先を募集しますので、受注を希望される場合は見積書等を提出して下さい。

令和6年8月23日

支出負担行為担当官
東北経済産業局総務企画部長　千嶌　浩

1.契約概要

(1)請負業務の名称等

経済産業省 関東東北産業保安監督部 東北支部ウェブサイトのウェブアクセシビリティ試験評価業務

(2)業務内容及び実施場所

別紙仕様書のとおり

2.参加資格

オープンカウンターに参加することができる者は、見積書提出期日において、次の各号に定めるすべての事項を満たす者とする。

(1)経済産業省所管の契約に係る競争参加者資格審査事務取扱要領(昭和38年6月26日付け38会第391号)に基づいた、令和04･05･06年度経済産業省競争参加資格(全省庁統一規格)において「役務の提供等」の「B」、「C」又は「D」の等級に格付けされ、競争参加地域を「東北」としている者。

(2)予算決算及び会計令(以下、「予決令」という。)第70条の規定に該当しない者。

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。

(3)予決令第71条の規定に該当しない者。

(4)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。

(5)暴力団員による不当な行為の防止等に関する法律第2条第2号に規定する暴力団及び警察当局から排除要請がある者に該当しない者。

(6)情報管理体制として、過去3年以内に情報管理の不備を理由に経済産業省から契約を解除されている者ではないこと。

3.質問方法及び問い合わせ先

(1)質問方法

電話またはFAXの受付とし、受付時間は次のとおりとする。
9時30分から12時まで、13時30分から16時30分まで
(但し、土曜日、日曜日等閉庁日を除く。)

(2)業務内容に関する問い合わせ先

関東東北産業保安監督部東北支部　管理課
電　話　022-221-4943
FAX　　022-261-1376

(3)見積書提出に関する問い合わせ先
東北経済産業局総務企画部会計課調度係
電　話　022-221-4869
FAX　　022-261-7390

4.見積書等の提出期限等
(1)提出期限
令和6年8月30日（金曜日）12時00分まで

(2)提出方法
1)電子調達システムを利用した提出
調達ポータル　https://www.p-portal.go.jp/pps-web-biz/UZA01/OZA0101/

2)紙による提出
提出先
〒980-8403 仙台市青葉区本町三丁目3番1号　仙台合同庁舎B棟4階
東北経済産業局総務企画部会計課調度係
電　話　022-221-4869
※郵送により見積書等を提出する場合は、予め電話により調度係に連絡すること。

3)提出する書類
ア　見積書
イ　2.(1)に係る競争参加資格証明書の写し。ただし、同一年度内におけるオープンカウンター案件への2回目以降の見積書提出時は不要とする。
ウ 別添「情報セキュリティの確保・個人情報の取扱い等に関する同意書」

4)見積書に関する注意事項
ア　紙での見積書提出に際しては見積書の様式は任意とするが、
Ⅰ）見積書の宛名は「支出負担行為担当官　東北経済産業局総務企画部長」とし、日付は提出日とすること。
Ⅱ）法人の場合は、会社名、住所、連絡先、代表者の役職及び氏名を記載すること。代表者印及び社印の押印は不要。
Ⅲ）税抜き価格と税込み価格の双方を記載すること。
イ　電子調達システムでの見積書提出に際しては、システムにて税抜き価格を設定し提出すること。ただし見積内訳書（様式は任意）を添付すること。

5.電子調達システムの利用
・本件は、電子調達システムを利用した手続により、実施するものとする。
・ただし、紙による提出も可とする。

6.その他
・本件は、請書の提出を要する。
・請負先の決定方法は、期限内に見積書を提出した者のうち、予定価格の範囲内で最低の価格をもって有効な見積書を提出した者とする。
・結果は落札者に通知するほか、局ホームページにて公表する。
・受注した場合の支払いは、後日銀行振り込みとし、当局が請求書を受理してから30日以内とする。

（別添）

甲：東北経済産業局総務企画部会計課長 殿

作成年月日：　年　月　日

情報セキュリティの確保・個人情報の取扱い等に関する同意書

乙：〇〇〇〇株式会社

下記の事項に同意し、甲の指示があったときにその指示に従いますので、見積書を提出いたします。

記

1. 仕様書の内容及び東北経済産業局役務請負契約条項の情報セキュリティの確保（第16条）及び個人情報の取扱い（第17条）（※1）を遵守すること。

（参考）

ア. 東北経済産業局役務請負契約条項（印刷製造、その他物品製造含む）
https://www.tohoku.meti.go.jp/kaikei/format/downloadfiles/2024_ukeoi_r6-ek-1.pdf

東北経済産業局役務請負契約条項・コンテンツバイドール版
https://www.tohoku.meti.go.jp/kaikei/format/downloadfiles/2024_ukeoi_r6-ekcb-1.pdf

イ. 経済産業省情報セキュリティ管理規程
https://www.meti.go.jp/intro/data/pdf/kanri_kitei.pdf

ウ. 経済産業省情報セキュリティ対策基準
https://www.meti.go.jp/intro/data/pdf/taisaku_kijun.pdf

エ. 経済産業省個人情報保護管理規程
https://www.meti.go.jp/policy/kojinjyohohogo/kitei.pdf

（※1）東北経済産業局役務請負契約条項・コンテンツバイドール版の場合には契約条項第26条及び第27条を指す。

別紙

仕様書

1. 件名

経済産業省 関東東北産業保安監督部 東北支部ウェブサイトのウェブアクセシビリティ試験評価業務

2. 目的

経済産業省ウェブサイトは経済産業省の情報発信のためのツールとして非常に重要な役割を果たすものであることから、高齢者や障害者を含む誰もが利用することができるよう、ウェブコンテンツのアクセシビリティ規格である日本産業規格（JIS X 8341-3:2016 高齢者・障害者等配慮設計指針－情報通信における機器、ソフトウェア及びサービス－第3部：ウェブコンテンツ）に基づく経済産業省ウェブアクセシビリティ方針を定め、ウェブサイト一式の適合レベル AA 準拠を目標に継続的な修正を加えつつ運用している。

本件は、経済産業省 関東東北産業保安監督部 東北支部ウェブサイトについて令和6年度以降においても引き続きアクセシビリティ方針に定めた達成目標 JIS X 8341-3:2016 適合レベル AA 準拠の達成度の評価を目標とするため実施するもの。

3. 作業内容等

経済産業省関東東北産業保安監督部東北支部ウェブアクセシビリティ方針を踏まえ、JIS X 8341-3:2016 に基づき適合レベル A 及び AA に定める達成基準の合否判定試験（以下、「試験」という。）を行うこと。その際の評価用機器については、事業者が用意すること。

なお、試験にあたっては、JIS X 8341-3:2016 及びウェブアクセシビリティ基盤委員会の「JIS X 8341-3:2016 試験実施ガイドライン 2020 年 12 月版」を参照すること。

（1） 経済産業省 関東東北産業保安監督部 東北支部ウェブサイト（https://www.safety-tohoku.meti.go.jp/）のトップページからリンクでたどれる全 HTML ファイルに対し評価ツールを用いて一括評価する。（総ページ約160 件）

評価ツールには、総務省が提供している「みんなのアクセシビリティ評価ツール：miChecker_ Ver.3.1」又は同等のツールを使用すること。

評価は、パソコン表示の内容、スマートフォン表示の内容を対象とし、評価結果を報告すること。

（2） 経済産業省 関東東北産業保安監督部 東北支部ウェブサイト（https://www.safety-tohoku.meti.go.jp/）のトップページからリンクでたどるツールを使用して、リンク切れを調査する。（総ページ約160 件）

調査は、パソコン表示の内容、スマートフォン表示の内容を対象とし、調査結果を報告すること。

（3） 試験対象ページは、経済産業省 関東東北産業保安監督部 東北支部ウェブサイト（https://www.safety-tohoku.meti.go.jp/）の CMS 管理下ページを対象に「JIS X 8341-3:2016、附属書 JB（参考）試験方法 JB.1 適合試験の要件 JB.1.2 ウェブページ一式単位 D)ウェブページ一式を代表するウェブページとランダムに選択したウェブページとを併せて選択する場合」に定める要件を満たすページ 40 ページを選択の上、試験前に経済産業省関東東北産業保安監督部 東北支部 管理課（以下、「当課」という。）に了解を得ること。なお、その際にはウェブページ一式を代表するウェブページの各ページを選択した理由をそれぞれ記述すること。

なお、ページ数の内訳は以下の通りとする。

〇ウェブページ一式を代表するウェブページ：10 ページ

①ウェブページ一式における共通のウェブページ

トップページ： 1 ページ

https://www.safety-tohoku.meti.go.jp/index.html

②ウェブページ一式のアクセシビリティに関連するウェブページ

アクセシビリティに関する方針，及び解説のあるウェブページ： 1 ページ

https://www.safety-tohoku.meti.go.jp/info/accessibility.html

利用者からの問合せを受け付けるウェブページ： 1 ページ

https://www.safety-tohoku.meti.go.jp/contact/

上記 1)及び 2)以外でウェブページ一式を代表するウェブページ

ウェブページ一式の中で重要な情報を提供するウェブページ：7 ページ

https://www.safety-tohoku.meti.go.jp/electric/index.html

https://www.safety-tohoku.meti.go.jp/citygas//index.html

https://www.safety-tohoku.meti.go.jp/lpgas/index.html

https://www.safety-tohoku.meti.go.jp/hipregas/index.html

https://www.safety-tohoku.meti.go.jp/gunpowder/index.html

https://www.safety-tohoku.meti.go.jp/mine/index.html

https://www.safety-tohoku.meti.go.jp/info/index.html

〇ランダムに選択したウェブページ：30 ページ

（4） JIS X 8341-3:2016 の附属書 JB「（参考）試験方法 JB.2 試験の手順」に基づき、ページ単位で達成方法（実装方法）及びその検証方法を特定できる技術的根拠を示した上で、適合及び不適合箇所を明確にすること。その際、検査した全てのページについて個別に問題点の指摘及び改善方法について提案を行うこと。

（5） 試験結果を経済産業省 関東東北産業保安監督部 東北支部（以下、「当支部」という。）ウェブサイトに掲載するため、JIS X 8341-3:2016 の「JB.3 試験結果の表示」に基づく表示内容を作成し提出すること。

（6） ウェブアクセシビリティの方針改定支援として、本試験結果により変更する必要があると判断される箇所があれば、それを指摘し修正案を提供すること（例えば、対象範囲にある「対象外」と「例」にある記載内容が適切であるかを確認し、変更が必要な場合は変更案を提示する。また、試験結果へのリンクを追加するなど）。

（7） JIS X 8341-3:2016 の試験対象ページより、当支部と協議の上で5ページ選定し、WCAG2.1 及び 2.2 で追加された達成基準に基づく検証を実施する。検証により確認された問題点等について、JIS X 8341-3:2016 試験実施箇所及び不具合箇所報告書において併せて報告する。

4. 請負者の要件

請負者は、過去に国及び地方公共団体等の公的機関において、JIS X 8341-3:2016 に基づくウェブアクセシビリティ方針の策定及び JIS X 8341-3:2016 に基づく適合レベル AA 全項目の適合試験実績を有し、これらを証する書面を提出すること。

5. 履行期間

契約締結日から令和7年3月31日まで

6. 納入成果物

DVDにて正副2枚を納品（納品形式は、Microsoft 製 Office 形式とする）

（1） 全ページのアクセシビリティ検査結果

（ア） URL 別評価ツール評価結果一覧

（2） 全ページのリンク切れ調査結果

（ア） URL 別リンク切れ検査結果

（3） JIS X 8341-3:2016 適合レベル AA 適合性評価試験

（ア） 試験対象ページ選定書 一覧

（イ） 達成基準チェックリスト及び実装チェックリスト 一式

（ウ） JIS X 8341-3:2016 試験実施箇所及び不具合箇所報告書 一式

7. 納入場所

〒980-0014 宮城県仙台市青葉区本町3－2－23 仙台第2合同庁舎9階
経済産業省 関東東北産業保安監督部 東北支部 管理課
連絡先 022-221-4943

8. その他

（1） 本業務で作成したコンテンツを当支部ウェブサイト等に掲載するため、また担当者においてコンテンツを自由に改変するため、それを公表する等に必要な著作権等は当支部に帰属することとする。

（2） 本事業の実施中に事故が発生した場合は、請負業者の責任において対処すること。

（3） 本仕様書の定めのない事項については、担当職員の指示に従うこと。

（4） 本業務に係る請負作業において知り得た情報（公知の情報等は除く。）を、第三者に開示、漏洩又は他の目的に使用してはならない。また、そのために必要な措置を講ずること。当該情報等を第三者に開示する必要がある場合は、当課と事前に協議し、承諾を得ること。

９．秘密保全

（１）本作業に関して、当支部が開示した情報（公知の情報等を除く。以下同じ。）及び契約履行過程で生じた納品物等に関する情報を、実施体制に定めた者以外の者には秘密とし、当該作業の遂行以外の目的に使用しないこと。また、そのために必要な措置を講ずること。なお、当該情報を本契約以外の目的に使用又は第三者に開示する必要がある場合は、事前に当支部 管理課の承認を得ること。

（２）本作業に関して、当支部から提供された情報を、当該作業の終了時に管理課に返却するか、消去又は破棄してその旨を書面で報告すること。

（３）本作業に関して、当支部から提供、貸与等された情報その他知り得た情報を、当該作業の終了後においても他者に漏えいしないこと。

（４）情報セキュリティが侵害された又はそのおそれがあると判断した場合には、直ちに管理課に口頭にてその旨第一報を入れること。管理課への第一報は、情報セキュリティインシデントの発生を認知してから遅くとも１時間以内に行われるように留意して行うこと。

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。

11. 情報管理体制

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）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）」様式1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、当局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。

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。

（別記）

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」（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。

別紙

令和　　年　　月　　日

経済産業省○○○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））。）

（様式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						
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。

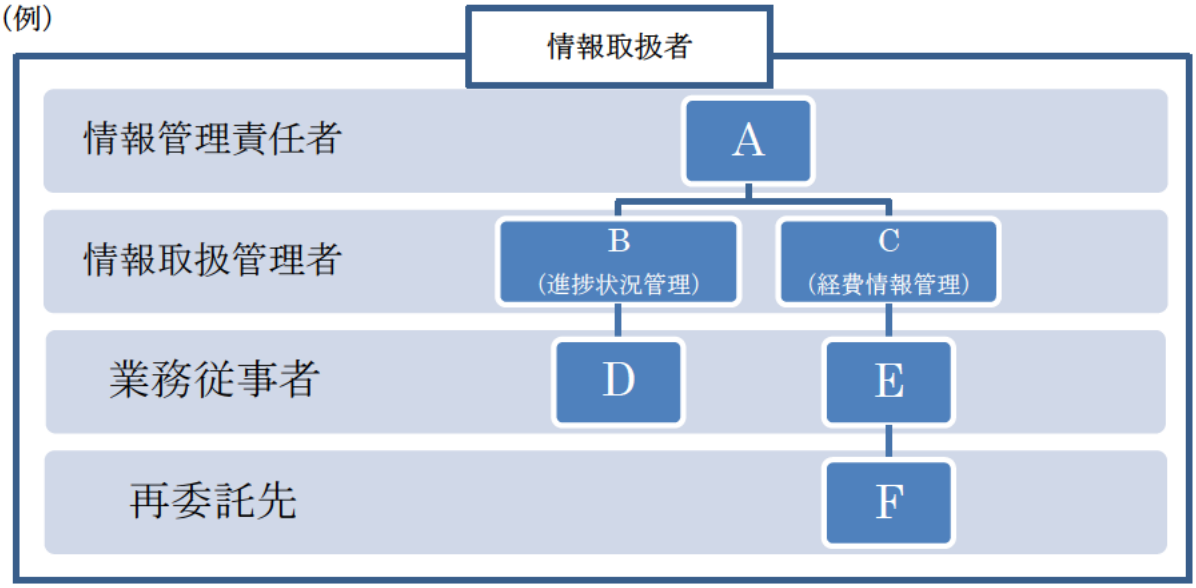
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※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。