神奈川県 GREEN×EXPO 2027 賓客等接遇業務委託
仕様書

1. 業務名

神奈川県 GREEN×EXPO 2027 賓客等接遇業務

2. 業務目的

令和9年に開催される GREEN×EXPO 2027（以下「博覧会」という。）においては、国内外から多数の賓客等が来場することが想定されている。

神奈川県（以下「県」という。）の賓客等が安全かつ快適に過ごせるよう、適切な接遇を実施することを本業務の目的とする。

3. 契約期間

契約締結日から令和 10 年3月 31 日まで

4. 委託業務内容（業務内容の詳細は別途提供予定の「仕様書（業務内容詳細）」を参照）

〇総合調整

本業務全般に係る進行管理及び調整

〇接遇に係る関係機関との調整

ア 関係機関との調整

イ 賓客等が訪問を希望する各出展エリアとの調整

〇車両及び運転手の手配

ア 発注者の求めに応じて車両及び運転手を手配できる体制の構築

イ 車両運行計画の作成

ウ 運転手への必要事項の伝達・指示及び手配当日の行動管理

〇記念品及び接遇に必要な物品の手配

ア 賓客等にお渡しする記念品案の提案及び記念品の手配

イ 賓客等の来訪に伴い必要となる物品の手配

ウ 上記のほか、発注者が必要に応じて求める物品の手配

〇現場対応

会期中の博覧会会場内における賓客等関係者等への対応

〇日程の細目冊子及び報道のしおり（以下「細目冊子等」という。）の作成及び配付

細目冊子等のデータ作成・編集及び印刷・製本並びに関係各所への配付（発送作業含む）

〇記録写真の撮影並びに記録誌及び記録アルバム（以下「記録誌等」という。）の作成及び配付

ア 撮影計画の作成

イ 記録写真の撮影

ウ 記録誌等の作成・編集及び印刷・製本並びに関係各所への配付（発送作業含む）

〇接遇業務に係るマニュアル等の作成

県としての接遇業務の流れや方法を網羅した接遇マニュアル等の作成

〇通訳者の手配

ア 発注者の求めに応じて通訳者を手配できる体制の構築

イ 通訳者のシフト計画の作成

ウ 通訳者への必要事項の伝達・指示及び手配当日の行動管理

〇案件管理用システムの作成及び運用

関係者間で接遇案件に関する情報の管理・共有が可能なシステムの作成及び運用・保守

〇ナショナルデー等の参加国・国際機関に係る資料の作成

参加国基本情報シートの作成（様式の作成含む）

〇接遇案件の日報及び月報の作成

接遇案件の日時、場所、対応者、接遇内容等の情報を網羅した日報及び月報の作成（様式の作成含む）

5. 実施方針、実施計画書及び業務体制図の提出

受注者は、契約締結後速やかに、本業務の実施における実施方針、実施計画書及び業務体制図（実施体制及び連絡体制）を提出すること。

また、変更が生じた場合は、その都度速やかに、最新のものを提出すること。

さらに、発注者が業務の進捗状況等に応じて実施計画の見直しを求めた場合は対応すること。

6. 事業報告書の提出

受注者は、業務の実施状況を記載した中間業務報告書（令和9年3月31日まで）及び業務完了報告書（令和10年3月31日まで）をそれぞれ、紙媒体及び電磁的記録媒体（電子メール、DVD 等）により発注者に提出すること。

なお、各報告書には、業務実績に応じた費用の明細を記載すること。

また、契約金については、中間業務報告書及び業務完了報告書を提出後、発注者による検査を経て支払うものとする。

※ 電磁的記録媒体の提出にあたっては、必ずウイルスチェックを行うこと。

なお、電磁的記録媒体の購入費用は委託料に含めること。

7. 再委託、セキュリティ要件及び著作物の譲渡等に関する条件

（1）再委託について

業務の主要な部分や契約金額の相当部分を他の法人等に再委託することは認められないが、専門性等

の理由から、一部を受注者において実施することが困難な場合や、自ら実施するより再委託した方が高い効果が期待されるときは、再委託することを認める。

なお、再委託契約の締結にあたっては、事前に発注者と協議し、書面により承認を得ること。

ただし、簡易な業務として発注者が認めるものについては、この限りでない。

また、受注者は、再委託先に対して、本業務委託に係る受注者の義務と同等以上の義務を負わせるものとし、再委託先の行為について、自らの行為と同一の責任を負うものとする。

(2)セキュリティ要件について

ア 基本的な考え方

受注者は、業務遂行上知り得た情報を、契約期間中はもとより契約期間後においても第三者に漏らしてはならない。また、業務において、「個人情報の保護に関する法律」や「神奈川県情報セキュリティポリシー」及び契約書の特記事項等を遵守し、情報セキュリティ対策を講じること。なお、神奈川県情報セキュリティポリシーは、第1章 情報セキュリティ基本方針のみをホームページで公開しているが、発注の際には全内容を受注者に対して提示する。

https://www.pref.kanagawa.jp/docs/fz7/security/securitypolicy.html

イ クラウドサービス等の外部サービスのセキュリティ要件

業務においてクラウドサービス等の外部サービスを利用し、個人情報又は特に機密性が求められる情報を扱う場合(以下、「重要情報」)という)は、「セキュリティチェックリスト」(別添)のセキュリティ要件、外部サービス提供者回答欄や受注者回答欄に記載のセキュリティ対策も満たすクラウドサービスの選定、開発(導入・構築)、運用、保守、更改・廃棄を行うこと。

契約後、「セキュリティチェックリスト」の外部サービス提供者回答欄や受注者回答欄を記入し、発注者に根拠資料と共に提出すること。その後は、「セキュリティチェックリスト」のセキュリティ要件に従い、時点更新を行い、定期的に発注者へ提出すること。システムの特性等に応じて不適合又は対策不要等を判断した場合には、根拠を示す説明資料を併せて提出し、発注者の承認を得ること。なお、クラウドサービス等の外部サービスを利用せず、自社のデータセンター等にサービス提供基盤を構築する場合は、クラウドサービスを利用する場合に準じたセキュリティ対策が実施できること。

ウ メールのセキュリティ対応

受注者は、メールのセキュリティについて次の措置を行うものとする。

(ア) 問合せ者とのメール、システムの自動送信メール等において、個人情報及び重要情報(あて先の情報及び発信者に係る情報を除く。)をメール本文に記載しないこと。

(イ) メールデータについて、発注者以外の事業とは独立した領域(発注者の事業専用環境)にデータは保管され、発注者のデータは契約終了後に消去可能で、関係者以外はアクセスできないこと。

(ウ) メールに係るセキュリティ対策(※)等を適切に実施すること。

※メールに係るセキュリティ対策とは、マルウェア感染、不正アクセス、メール不正中継等に対する

基本的なセキュリティ対策、SPF・DKIM 認証等のメールの設定などを指す。

（エ） メールは原則、県のドメインを利用すること。やむを得ず、独自ドメインを使用する場合は、受注者の公式サイトのドメイン等（県の業務委託終了後も利用し続ける前提のドメイン）を除き、悪用防止のため、永続的に保持する必要があるため、事業終了後は県に引継ぐこと。 受注者の公式サイト等で管理しているドメインを使用する場合は、ドメインが不正利用されないよう適切な対策及び管理を委託業務終了後も行うこと。

エ 業務委託における作業環境等のセキュリティ対策

（ア） 受注者は、サーバや端末等で用いるOS・ソフトウェア等について、保守等の十分なサポートがなく脆弱性対策が実施されないなど、情報セキュリティ上問題となる恐れのあるOS・ソフトウェア等を利用しないこと。導入するOS・ソフトウェア等についてはライセンス違反のないよう管理すること。

（イ） 受注者は、サーバや端末等で用いるOS・ソフトウェア等の脆弱性情報を常に収集し、OS・ソフトウェア等の脆弱性に対する攻撃を防止するため、セキュリティパッチの適用、アップデート等の適切な措置を行うこと。

（ウ） 受注者は、サーバや端末等におけるプログラムの実行、コマンドの操作、ファイルへのアクセス等のアクセス権限・管理者権限等のアクセス制御は、必要最小限のものとすること。

（エ） 作業場所は、本委託業務に関係のない者が簡単に入れない適切な場所（入退室管理、施錠等）とすること。

（オ） 受注者が管理するサーバや端末等以外は使用しないこととし、必要最小限のものに限定した上で、台帳等で適切に管理すること。サーバや端末等は、セキュリティワイヤーでロックする等の盗難防止策を講じた上で、施錠若しくは入退室管理の可能な部屋に保管すること。また、サーバや端末等の外部への持ち出しを原則、禁止する。持ち出す場合には、発注者と協議を行い、承認を得ること。

（カ） サーバや端末等で個人情報及び重要情報を保存する場合は、パスワード等による暗号化を行うこと。

（キ） 受注者は、個人情報及び重要情報をCD-R、USBメモリ等の外部記録媒体へ保存すること及び外部への持ち出しを原則、禁止する。受注者は外部記録媒体を、やむを得ず利用する場合は、事前に発注者の承認を得た上で、保存する情報のパスワード等による暗号化や外部記録媒体の管理簿（委託業務で利用する外部記録媒体の一覧と利用及び持ち出しの記録）を作成するなどの適切な管理を行うこと。

（ク） 受注者は、作業環境等のネットワークについて、ファイアウォール等の機能により必要最小限の通信となるようにアクセス制御を行い、不審な通信の監視、検知・遮断を行う対策を講じること。また、ファイアウォール等のネットワーク機能の設定については、定期的に棚卸しを行うこと。

（ケ） 不正プログラムによる感染を防止するため、受注者は、不正プログラム対策ソフトウェアを導入する等の必要な対策を講じること。また、不正プログラム対策ソフトウェアのパターンファイル等の最新化が適切に行われること。

（コ） 受注者は、サーバや端末等で不要なプログラムを稼動させないこと。また、ネットワークポートについても必要なポート以外は閉塞すること。

（サ） 業務委託で扱うデータについて、データが国内の作業場所やデータセンター等のみに保存され、バックアップを含め海外にはデータ転送されないこと。併せて、個人情報保護法等の国内法が適用されること。

（シ） 受注者は、契約終了時、データを消去する前に発注者にデータの返還を行うこと。対象データ、受渡し方法等については発注者と協議すること。受注者は、契約終了後速やかに、本委託業務で使用したサーバや端末、外部記録媒体等に存在する、本委託業務に係るすべてのデータ（バックアップデータを含む）を復元不可能な方法で確実に廃棄・消去し、データ消去証明書を提出すること。

（ス） 受注者は、不正アクセスやシステムの障害等の情報セキュリティインシデントに対応する体制を整備し、発注者を含めた連絡フローや手順を整備すること。さらに、情報セキュリティインシデント（可能性を含む）を検知した場合は、速やかに発注者に報告すること。また、原因究明及び対処を行い、随時発注者に報告を行うこと。情報セキュリティインシデントの対応完了時には、再発防止対策の策定を行った上で、書面等により発注者に報告、承認を得ること。

（セ） 受注者は、サーバや端末等の正確な時刻設定及び時刻同期がなされるように適切に管理すること。

（ソ） 受注者は、ネットワーク機器の脆弱性を利用した不正アクセス、ランサムウェア、標的型攻撃等の最新のサイバーセキュリティ動向に留意し、必要な対策を継続的に行い、委託業務にあたること。

（タ） 情報セキュリティ対策を確認するため、発注者が必要に応じ情報セキュリティ監査を行うので、受注者はこれに応じること。

（3）著作物の譲渡等について

・成果物及び成果物に使用するため作成した全てのもの（原稿及び写真、データ等）の著作権（著作権法第21条から第28条に定める権利を含む）は、発注者に帰属するものとする。

・受注者は、業務の実施に当たり第三者が権利を有する著作物（映像・写真・音楽等）を使用する場合、著作権、肖像権等に厳重な注意を払い、当該著作物の使用に関して費用の負担を含む一切の手続きを行うものとする。

・受注者は著作者人格権を行使しないものとする。

・著作権、肖像権などの権利関係の処理・調整については受注者が行い、成果物に使用される全てのものは、必ず著作権等の了承を得て使用すること。

・受注者は、本業務に関し、第三者との間で著作権に係る権利侵害の紛争等が生じた場合には、当該紛争等の原因が専ら発注者の責に帰す場合を除き、自らの責任と負担において一切の処理を行うものとする。

8. その他の条件

（1）本仕様書の内容等について疑義が生じた場合は、その都度、発注者と協議の上、その指示に従い事業を進

めるとともに、発注者は委託期間中いつでもその進捗状況の報告を求めることができるものとする。

（2）その他、業務の遂行上必要と認められるもので本仕様書に定めのない事項が生じた場合及び本業務の実施にあたり疑義が生じた場合は、発注者と協議し、その指示に従うこと。

（3）本業務の企画立案、実施及びそれに付随する業務に係る一切の費用については、仕様書に特段の記述がなければ、原則、受注者が負担することとする。

（4）新興感染症の拡大や天災、事業の変更等のやむを得ない理由により、仕様書通りの事業の実施が困難な場合などの不測の事態への対応は、発注者と協議の上、方針を決定し、必要に応じて変更契約等を行うこと。また、その際、受注者は発注者に違約金を請求できないこととし、発注者はキャンセル料等の実費については支払うものとする。

（5）本業務の実施に際しては、安全を期し、事故等の損害賠償責任は受注者が負うこと。

（6）本業務に係る全ての証拠書類は、業務終了後、5年間保存すること。