（別紙５）

令和元年度　企業間専門人材
派遣支援モデル事業

調達仕様書
（別紙）

復興庁

情報セキュリティ

（1）受注者は、情報システムが提供する業務及び取り扱う情報、利用環境を考慮した上で、脅威に対抗するために必要となる適切なセキュリティ対策を行うこと。なお、具体的な対策内容については「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」等を参照し、セキュリティ要件に応じた必要な対策を取り込むこと。

（2）受注者は、既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。また、セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合には速やかに修正すること。

（3）受注者は、導入するソフトウェアのサポート期間又はサポート打ち切り計画に関する情報を当庁に情報提供すること。

（4）受注者は、情報システムに実装されたセキュリティ機能を適切に運用するために、情報システムの運用環境に課せられるべき条件、セキュリティ監視を行う場合の監視手順や連絡方法、保守における情報セキュリティ対策の内容、運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策の要件に従い、適切に実施すること。

（5） 情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、契約期間保管するとともに、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能等）を備えること。また、ログの不正な改ざんや削除を防止するため、ログに関するアクセス制御機能を備えること。

（6）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。

（アプリケーション・コンテンツの作成等を行う場合）

（1）作成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。

（2）作成するアプリケーション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限り、実行プログラムの形式でコンテンツを提供しないこと。

（4）電子証明書を利用するなど、作成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。

（5）作成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 や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、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）サービス利用に当たって必須ではない、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。

（7）利用者が検索サイト等を経由して当庁のウェブサイトになりすました不正なウェブサイトへ誘導されないようサーバの正当性を確認できる機能を備えるとともに、許可されていない端末、サーバ装置、通信回線装置等の接続を防止する機能を備えること。

（庁外向けにウェブサイト等を提供する場合）

（１）.go.jp で終わる政府ドメイン名を使用すること。

（２）GPKI（Government Public Key Infrastructure）に対応した電子証明書を使用すること。

（３）インターネットを介して転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策を講じること。

（クラウドサービスを利用する場合）

（１）ISO/IEC27001 又はそれに基づく認証を取得しているクラウドサービスを採用すること。また、当該認証の証明書等の写しを提出すること。

（２）クラウドサービスの情報セキュリティ水準を証明する以下のいずれかの証明書等の写しを提出すること。

① ISO/IEC27017 又は ISMS クラウドセキュリティ認証制度に基づく認証

② セキュリティに係る内部統制の保証報告書（SOC 報告書（Service Organization Control Report））

③ 情報セキュリティ監査により対策の有効性が適切であることを証明する報告書（クラウド情報セキュリティ監査制度に基づく CS マークが付された CS 言明書等）

（３）クラウドサービスにおいて個人情報又は当庁における要機密情報が取り扱われる場合には、当該クラウドサービスのデータセンター（バックアップセンターを含む。）は国内に限ること。

（４）クラウドサービスの廃止、サービス内容の変更等に伴い契約を終了する場合は、他のクラウドサービス等に円滑に移行できるよう、十分な期間をもって事前（サービス廃止等の１年以上前が望ましい。）に担当部署へ通知すること。また、要安定情報を取り扱う場合には、サービス中断時の復旧目標時間を担当部署へ通知すること。

（５）クラウドサービスの契約を終了する場合、クラウドサービス上に保存された当庁のデータについて、汎用性のあるデータ形式に変換して提供するとともに、クラウドサービス上において復元できないよう抹消し、その結果を担当部署に書面で報告すること。

（６）クラウドサービスに係るアクセスログ等の証跡を保存し、担当部署からの要求があった場合は提供すること。なお、証跡は１年間以上保存することが望ましい。

（７）インターネット回線とクラウド基盤との接続点の通信を監視すること。

（８）クラウドサービスに係る業務の一部がクラウドサービス事業者以外の事業者に外部委託されている場合は、当該クラウドサービス事業者以外の事業者に「再受託に関する事項（下記参照）」の措置を講ずること。

（９）クラウドサービスにおける脆弱性対策の実施内容を担当部署が確認できること。

（10）クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切替等の対策が講じられていること。また、クラウドサービスに障害が発生した場合の復旧時点目標（RPO）等の指標を提示すること。なお、当庁の要安定情報を取り扱う場合は、データセンターを地理的に離れた複数の地域に設置するなどの災害対策が講じられていること。

（11）クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。

（12） クラウドサービスの利用者が、自らの意思によりクラウドサービス上で取り扱う情報を確実に抹

消できること。

(13)　本業務において、クラウドサービスに係る情報について、業務開始時に開示項目や範囲を明記した資料を提出すること。

(14)　当庁に対して、クラウドサービスに係る機密性の高い情報を開示する場合は、当庁において、当該情報を審査又は本業務以外の目的で利用しないよう適切に取り扱うため、必要に応じて当該情報に取扱制限を明記するなどの措置を講じること。

（データベースを導入・運用する場合）

（１）データベースに対する管理者アカウントの適正な権限管理を行うこと。また、権限の不適切な付与を検知できるよう、措置を講ずること。

（２）データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。

（３）データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知するための対策として、一定数以上のデータの取得に関するログを記録し警告を発する措置やデータを取得した時刻が不自然である操作に関するログを記録し警告を発する措置等を講ずること。

（４）データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。また、データベースにアクセスする機器上で動作するプログラムに対してはSQLインジェクションの脆弱性を排除すること。プログラムの対策のみでは不十分な場合には、ウェブアプリケーションファイアウォールやデータベースファイアウォール等の導入を行うこと。

（５）データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合には、適切に暗号化すること。データベースに格納されているデータに対して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施すること。

再受託に関する事項

再受託の制限及び再受託を認める場合の条件

（１）本業務の受注者は、業務を一括して又は主たる部分を再受託してはならない。
（２）受注者における遂行責任者を再受託先事業者の社員や契約社員とすることはできない。
（３）受注者は再受託先の行為について一切の責任を負うものとする。
（４）再受託を行う場合、再受託先が「概算金額、入札制限」に示す要件を満たすこと。
（５）再受託先における情報セキュリティの確保については受注者の責任とする。

承認手続

（１）本業務の実施の一部を合理的な理由及び必要性により再受託する場合には、あらかじめ再受託の相手方の商号又は名称及び住所並びに再受託を行う業務の範囲、再受託の必要性及び契約金額等について記載した再受託承認申請書を当庁に提出し、あらかじめ承認を受けること。

（２）前項による再受託の相手方の変更等を行う必要が生じた場合も、前項と同様に再受託に関する書面を当庁に提出し、承認を受けること。
（３）再受託の相手方が更に受託を行うなど複数の段階で再受託が行われる場合（以下「再々受託」という。）には、当該再々受託の相手方の商号又は名称及び住所並びに再々受託を行う業務の範囲を書面で報告すること。

再受託先の契約違反等

再受託先において、義務違反又は義務を怠った場合には、受注者が一切の責任を負うとともに、当庁は、当該再受託先への再受託の中止を請求することができる。

作業の実施に当たっての遵守事項

機密保持、資料の取扱い

（１）当庁から復興庁セキュリティポリシー（以下「ポリシー」という。）等の説明を受けるとともに、本業務に係る情報セキュリティ要件を遵守すること。また、ポリシーに定める情報セキュリティ管理体制を整備するとともに、本業務の従事者に対して、ポリシーと同等の情報セキュリティ対策の教育を実施すること。

（２）本業務の遂行に当たり、以下の内容を含む情報セキュリティ対策について定めた書類を入札に先立ち提出すること。

① 受注者に提供される情報の目的外利用の禁止

② 情報セキュリティ対策の実施内容及び管理体制及び管理責任者

③ 業務の実施に当たり、受注者又はその従業員、再委託先、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 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・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

（３）当庁が必要と認めた場合は、情報セキュリティ監査の受入を行うとともに、業務内容、品質等のサービス水準（サービスレベル）について保証すること。

（４）受注者が、その役務内容を一部再委託する場合は、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、上記の措置の実施を委託先に担保させること。

（５）当庁から情報セキュリティ対策の履行状況の確認を求められた場合には、速やかにその結果を報告すること。

（６）本業務に係る情報セキュリティインシデントの発生若しくは情報の目的外利用等の認知に際し、当庁の指示に従い、必要な措置を講じること。

（７）本業務の終了時には、受注者において取り扱われた情報を確実に返却、又は抹消し、その結果を書面にて報告すること。

法令等の遵守

（１）個人情報（生存する個人に関する情報であって、当該契約に含まれる氏名、生年月日、その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む。）をいう。以下同じ。）の取扱いに係る事項について当庁と協議を行い、個人情報保護取扱責任者を定めた上、以下の項目を含む事項を書面で提出すること。なお、個人情報保護取扱責任者が、「・機密保持、資料の取扱い」（２）②の管理責任者と同一の場合には、その旨を記載すること。

① 個人情報保護取扱責任者の所属、氏名等を記載した管理体制

② 個人情報の管理状況の検査に関する事項（検査時期、検査項目、検査結果において問題があった場合の対応等）

（２）本業務の作業を派遣労働者に行わせる場合には、労働者派遣契約書に秘密保持義務等、個人情報の適正な取扱いに関する事項を明記し、認識を徹底させること。
（３）個人情報を複製する場合には、事前に当庁の許可を得ること。なお、複製は必要最小限とし、複製物が不要となり次第、その内容が絶対に復元できないように破棄・消去すること。
（４）個人情報の漏えい等安全確保の上で問題となる事案を把握した場合には、直ちに被害の拡大防止等のため必要な措置を講じるとともに、当庁に事案の発生、被害状況、復旧等の措置及び本人への対応等を直ちに報告すること。
（５）個人情報の適正な取扱いがなされなかった場合は、契約を解除することとする。

知的財産等

（１）本件調達に関して作成、変更、更新されるドキュメント類及びウェブサイトプログラムの著作権（著作権法（昭和 45 年法律第 48 号）第 21 条から第 28 条に定めるすべての権利を含む。）は、受託者が本件調達の受託前より権利を保有していた等の明確な理由により、あらかじめ書面にて権利譲渡不可能と示されたもの以外の権利については、すべて当庁に帰属するものとする。
（２）本件調達に関して発生した権利については、受託者は著作者人格権（著作権法第 18 条から第 20 条までに規定する権利をいう。）を行使しないものとする。
（３）本件調達に関して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、受託者は原著作物の著作権者としての権利を行使しないものとする。
（４）本件調達に関して作成、変更、修正されるドキュメント類及びウェブサイト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、受託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を行うこと。この場合は事前に当庁に報告し、承認を得ること。
（５）本調達に関して第三者との間に著作権に係る権利侵害の紛争が生じた場合には、当該紛争の原因が専ら当庁の責めに帰すべき場合を除き、受託者の責任、負担において一切を処理すること。この場合、当庁は係る紛争の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者に委ねる等の協力措置を講ずるものとする。
（６）受託者の著作又は一般に公開されている著作について、引用する場合は出典を明示するとともに、受託者の責任において著作権者等の承認を得るものとし、当庁に提出する際は、その旨併せて報告するものとする。
（７）受託者は本件調達の実施状況を公表しようとするときは、あらかじめ当庁の承認を受けなければならない。

秘密の保持

（１）受託者は、契約の履行に当たり業務上知り得た情報については、他人に漏らす、又は、他に利用するための情報として提供してはならない。なお、予め第三者に提供することを明らかにした上で収集した情報については、この限りではない。
（２）受託者は、業務を行うために個人情報を取り扱う場合には、個人情報の保護に関する法律（平成 15 年法律第 57 号）の規定を遵守し、個人情報に係る苦情及び条例違反と認められる事例が発生した場合又は発生するおそれがあることを知った場合には、速やかに当庁に報告するとともに、その指示に基づき、被害の拡大の防止、復旧等のために必要な措置を講ずること。

運用作業

定常時対応

（1）受注者は、定常時運用業務（システム操作、運転管理・監視、稼動状況監視、サービスデスク提供等）を行うこと。具体的な実施内容・手順は当庁が定める運用計画に基づいて行うこと。

（2）受注者は、運用計画及び運用実施要領に基づき、運用業務の内容や工数などの作業実績状況、サービスレベルの達成状況、情報システムの構成と運転状況（情報セキュリティ監視状況を含む。）、情報システムの定期点検状況、情報システムの利用者サポート、教育・訓練状況、リスク・課題の把握・対応状況について月次で運用作業報告書を取りまとめること。

（3）受注者は、月間の運用実績を評価し、達成状況が目標に満たない場合はその要因の分析を行うとともに、達成状況の改善に向けた対応策を提案すること。

（4）受注者は、運用作業報告書の内容について、月例の定期運用会議に出席し、その内容を報告すること。

（5）受注者は、ソフトウェア製品の保守の実施において、ソフトウェア製品の構成に変更が生じる場合には、当庁にその旨を報告し、変更後の環境がライセンスの許諾条件に合致するか否かの確認を受けること。

（6）受注者は、情報システムのセキュリティ監視を行う場合は、監視するイベントの種類、監視体制、監視状況の報告手順、情報セキュリティインシデントの可能性を認知した場合の報告手順、監視運用における情報の取扱い（機密性の確保）を定め、適切に監視運用すること。

（7）受注者は、情報システムに実装されたセキュリティ機能が適切に運用されていることを確認すること。

（8）受注者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずること。

障害発生時対応

（1）受注者は、情報システムの障害発生時（又は発生が見込まれる時）には、速やかに当庁に報告するとともに、その緊急度及び影響度を判断の上、障害発生時運用業務（障害検知、障害発生箇所の切り分け、保守事業者への連絡、復旧確認、報告等）を行うこと。障害には、情報セキュリティインシデントを含めるものとする。具体的な実施内容・手順は当庁が定める運用計画及び運用実施要領に基づいて行うこと。

（2）受注者は、情報システムの障害に関して事象の分析（発生原因、影響度、過去の発生実績、再発可能性等）を行い、同様の事象が将来にわたって発生する可能性がある場合には、恒久的な対応策を提案すること。

（3）受注者は、大規模災害等の発災時には、当庁の指示を受けて、情報システム運用継続計画に基づく運用業務を実施すること。

（4）受注者は、情報セキュリティインシデント発生時又は 情報セキュリティインシデントの可能性を認知した際には、復興庁 CSIRT と連携を行い、適切に対処すること。