令和５年度
契約内容説明用タブレット端末の借入

調達仕様書

独立行政法人都市再生機構

目次

１．件名

令和５年度契約内容説明用タブレット端末の借入

２．調達概要

２．１　目的

独立行政法人都市再生機構（以下「機構」という。）の募集窓口ではタブレット端末を用いて、TV 会議システムによる契約内容説明などを実施している。

本調達の目的は、令和５年８月以降に利用するタブレット端末を導入することである。

２．２　調達範囲

本仕様書における調達の範囲は、以下の項目とする。

（１）　タブレット端末　一式

（２）　モバイル端末管理（MDM）サービス　一式

（クラウドサービスに該当する場合は、競争参加資格確認時点で ISMAP クラウドサービスリストに掲載されているサービスとする。）

（３）　（１）に導入したソフトウェアに関する保守・サポート業務　一式

（４）　（１）の調整及び保守業務　一式

（５）　本調達対象機器等に関する稼動維持作業　一式

（６）　本調達対象機器等の導入並びに賃貸借期間終了時のデータ消去及び撤去　一式

２．３　調達物品の内訳及び数量

「４．端末等要件」を参照し、これと同等以上の機器等を納品すること。また、特に記載がなくても要件を満たすために必要な機器等についても、本調達に含めるものとする。

（１）　納品完了期限

令和５年７月上旬を目途に設定を完了し、機構が指定する箇所（https://www.ur-net.go.jp/chintai/counter/のうちの一部）への納品を７月下旬までに完了させること。

なお、令和５年６月中を目途に、機構が別途調達する「令和５年度契約内容説明用 WiFi ルータの調達」の受注者から WiFi ルータの納入を受け、タブレット端末一式と併せて納品すること。

（２）　賃貸借期間

本調達機器等の賃貸借期間は令和５年８月１日から令和７年 10 月 31 日とする。

（３）　調達物品の要求仕様

本調達機器等の要求仕様については「４．端末等要件」を参照のこと。

ただし、国等による環境物品等の調達の推進等に関する法律（平成 12 年法律第 100 号）における対象製品については、定められた判断の基準を満たしていること。

２．４　機器の基本要件

本調達で導入する機器の基本要件は下記のとおりである。

（１）　ＯＳ等のセキュリティホール対策

ＯＳ等のソフトウェアは、既知のセキュリティホールに対する対策が施されていること。また、導入完了期限までに指摘されているセキュリティホール等に対して、修正モジュールのインストール等、適切な処理を施すこと。

（２）　安全性・信頼性要件

①　ハードウェア及びソフトウェアについては、製品の動作等十分に保証及び確認されていること。

②　本調達機器等のネットワークへの接続によって、ネットワークのセキュリティ水準が低下することのないよう十分な対策が講じられていること。

③　本調達機器等は機械的及び電気的に人体等に危険のない構造であること。

④　通常の使用環境において、放電や雑音電圧が混入した場合でも、装置が容易に誤作動しないこと。

⑤　ハードウェア内のデータは可能な限り、暗号化とデータ保護の措置が講じられること。

２．５　情報システムのライフサイクルの各段階における対策

受注者は、以下の情報システムのライフサイクルの各段階における対策を整備・規定し、かつ、実効性を担保すること。

（１）　実施体制の確保

受注者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制を確保すること。

（２）　情報システム導入時の対策

① 受注者は、導入する情報システムに関連する以下の脆弱性への対策を実施すること。

（イ） 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。

（ロ） ソフトウェアのサポート期間又はサポート打切り計画に関する機構への情報提供

②　受注者は、情報セキュリティの観点に基づく試験の実施について、次の各号を含む事項を実施すること。

（イ） MDM の機能有効に働いているか、リモートワイプ機能が有効に働いているか等の情報セキュリティの観点から試験を実施すること。

（ロ）情報セキュリティの観点から実施した試験の実施記録を保存すること。

③　受注者は、導入した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から次の各号を含む必要な情報セキュリティ対策を講じること。

（イ）情報セキュリティに関わる運用保守体制の整備

（ロ）運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施

（ハ）情報セキュリティインシデントを認知した際の対処方法の確立

（３）導入する情報システムの OS のサポートが終了又はバージョンアップが不可となった

場合、機構と事業者の協議の上、利用期間中の解約を可能とすること。

２．６　情報セキュリティ対策に関する要件

情報セキュリティ対策においては、民法（明治 29 年法律第 89 号)、刑法（明治 40 年法律第 45 号)、著作権法（昭和 45 年法律第 48 号)、個人情報の保護に関する法律（平成 15 年法律第 57 号)、不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）等の関連法規を遵守することはもとより、政府機関統一基準等関連ガイドラインを理解した上で、都市機構情報セキュリティ関連規程(以下、「セキュリティ関連規程」という。）を遵守すること。また、システムの構成や特性に応じ情報の機密性、完全性及び可用性を各々適切に確保し取組を行うと同時に、万全な体制を整えそれを維持していくこと。

セキュリティ関連規程の詳細については、受注者へ開示する。

受注者は、以下のセキュリティ対策を整備・規定し、かつ、実効性を担保すること。

（１）　調達時に実現可能な技術を用いたセキュリティ対策について、システム構成等を考慮した上で実施すること。

（２）　既知のセキュリティ対策においては、全般的に網羅されている上で、情報セキュリティを取り巻く状況の変化に迅速かつ柔軟に対応すること。

（３）　タブレット端末の USB 接続に関し、監視範囲の制御を行うこと。なお、制御設定については、機構と協議の上決定するものとする。

（４）　作業の実施にあたっての遵守事項

①　情報セキュリティの確保

（イ）受注者は、自らが担当している業務の遂行のために必要な範囲に限って、情報を利用すること。

（ロ）受注者は、次の各号の内容を含む情報セキュリティ対策の遵守方法及び情報セキュリティ管理体制等に関する確認書等を提出すること。また、変更があった場合は、速やかに再提出すること。

一　当該委託業務に携わる者の特定

二　当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容

（ハ）受注者は、本調達に係る業務の遂行において、機構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を、一貫した品質保証体制の下で行うこと。

（ニ）受注者の資本関係・役員等の情報、本業務の実施場所、本業務従事者の所属・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を行うこと。

（ホ）受注者は、本調達に係る業務の遂行において、定期的に情報セキュリティ対策の履行状況を報告するとともに情報セキュリティが侵害され又はその恐れがある場合には、直ちに機構に報告すること。これに該当する場合には、以下の事象を含む。

一　受注者に提供し、又は受注者によるアクセスを認める機構の情報の外部への漏えい及び目的外利用

二　受注者による本業務の範囲を超えた、機構が認めない情報への不正なアクセ

ス

（ヘ）受注者は、被害の程度を把握するため、受注者は必要な記録類を契約終了時まで保存し、機構の求めに応じて成果物とともに機構に引き渡すこと。

一　情報セキュリティ侵害の内容及び影響範囲を調査の上、当該情報セキュリティ侵害への対応策を立案し、機構の承認を得た上で実施すること。

二　発生した事態の具体的内容、原因及び実施した対応策等について報告書を作成し、機構へ納入して承認を得ること。

三　再発防止対策を立案し、機構の承認を得た上で実施すること。

四　上記のほか、発生した情報セキュリティ侵害について、機構の指示に基づく措置を実施すること。

（ト）受注者は、本業務の実施に当たり、履行状況の報告を適切に行い、機構が必要と認めた場合は、機構の情報セキュリティ監査を受け入れること。

（チ）受注者は、情報セキュリティ対策の履行が不十分な場合には、改善策を提示し、機構の承諾を得た上で、その対策を速やかに実施すること。

（５）　受注者は、情報システムや情報へのアクセス主体を特定し、それが正当な主体であることを検証するため、主体の識別及び主体認証を行う機能を設けること。

また、主体認証情報としてパスワードを使用し、利用者自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、強固なパスワードに必要な桁数や複雑さを利用者に守らせる機能を設けること。

（６）　受注者は、主体認証を行う情報システムにおいて、次の各号を含む主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講じること。

① 利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能を設けること。また、その他に例として、利用者が定期的に変更しているか否かを確認する機能、利用者が定期的に変更しなければ情報システムの利用を継続させない機能、利用者が主体認証情報を変更する際に以前に設定した主体認証情報の再設定を防止する機能のような機能を設けること。

② 主体認証情報を送信又は保存する場合には、その内容を暗号化すること。

③ 主体認証情報に対するアクセス制限を設けること。

また、主体認証情報を他の主体に不正に利用され、又は利用されるおそれを認識した場合の対策として、以下を例とする機能を設けること。

① 当該主体認証情報及び対応する識別コードの利用を停止する機能

② 主体認証情報の再設定を利用者に要求する機能

（７）　受注者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与（発行、更新及び変更を含む。以下本項において同じ。）し、次の各号を含む管理するための措置を講じること。

① 主体以外の者が識別コード又は主体認証情報を設定する場合に、主体へ安全な方法で主体認証情報を配布するよう、措置を講ずること。

② 識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認

証情報（必要に応じて、初期設定の識別コードも含む）を速やかに変更するよう、促すこと。

③ 知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう主体に注意を促すこと。

また、識別コードの付与に当たっては、以下を例とする措置を講ずること。

① 単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止

② 主体への識別コードの付与に関する記録を消去する場合の機構からの事前の許可

（８） 受注者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するため、次の各号を例とする措置を速やかに講じること。

① 当該主体の識別コードを無効にすること。

② 無効化した識別コードを他の主体に新たに発行することを禁止すること。

（９） 受注者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じること。

(10) 受注者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得すること。また、情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること。

(11) 受注者は、情報システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、不正な消去や改ざん及びアクセスを防止するための適切なアクセス制御を含むログ情報の保全方法、ログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。なお、管理するログは MDM（モバイルデバイス管理）サービス及びブラウザのログを想定している

また、受注者は、ログとして取得する以下の情報項目を定め、管理すること。

① 事象の主体（人物又は機器等）を示す識別コード

② 識別コードの発行等の管理記録

③ 情報システムの操作記録

④ 事象の種類

⑤ 事象の対象

⑥ 正確な日付及び時刻

⑦ 試みられたアクセスに関わる情報

⑧ 通信パケットの内容

⑨ 操作する者、監視する者、保守する者等への通知の内容

(12) 受注者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、次の各号

の措置を講じること。

① 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。

２．７ 機密保持に関する要件

（１） 機密保持、資料の取扱い

① 受注者は、機密情報の保持について以下の内容を遵守すること。

（イ）本仕様書における各作業の実施中はもとより、作業の実施後も、本仕様書上のシステム構造、機器及びその他本契約を履行する上で知り得た全ての情報を第三者に開示及び漏洩することのないこと。また、そのために必要な措置を講ずること。

（ロ）機構が提供する資料については、原則として貸出しとし、導入完了期限までに返却、又は機構と協議の上、適切な方法で廃棄すること。また、当該資料の複写及び第三者への提供はしないこと。

（ハ）機構が提供した情報を第三者に開示する必要がある場合は、事前に機構と協議を行った上で承認を得ること。

② 受注者は、情報の提供等を受ける際、次の各号に掲げる事項を遵守すること。

（イ）要保護情報の提供を受ける場合は、提供される情報を必要最小限とし、あらかじめ定められた安全な方法で受渡しすること。

（ロ）提供された要保護情報が不要になった場合は、これを確実に返却又は抹消すること。

③ 受注者は、機構との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について機構と合意し、定められた手順により情報を取り扱うこと。

④ 受注者は、受託した業務の終了時に、取り扱った情報を確実に返却、又は抹消したことを確認すること。

⑤ 受注者は、受注業務の実施において、民法、刑法、著作権法、個人情報の保護に関する法律、不正アクセス行為の禁止等に関する法律等の関連する法令等を遵守すること。

⑥ 受注者は、情報セキュリティ監査について、以下の内容を遵守すること。

（イ）本業務の実施に当たり、機構が必要と認めた場合は、機構の情報セキュリティ監査を受け入れること。

（ロ） 情報セキュリティ監査の結果、機構が改善を求めた場合には、機構と協議の上、必要な改善策を立案して速やかに実施すること。

（ハ）機構が外部からの監査を受けるに当たり、機構から指示があった場合には、受注者は、監査の対応に関して協力をすること。

２．８ 工程表の提出

受注者は、契約締結後７日以内に、本タブレット端末の導入における工程表を提出すること。

２．９　納品物

（１）　共通事項

①　受注者は、本調達機器及びシステムを納入する際に指定のドキュメントを紙、CD-ROM等の媒体により日本語で提供すること。また、提出予定のドキュメントを一覧にまとめ提出すること。

②　紙のサイズについては、Ａ４サイズとし必要に応じてＡ３サイズを使用すること。また、容易に差し替えができるようバインダー形式とする。

③　CD-ROM 等の媒体に保存する形式は、Microsoft Office 形式又は PDF 形式とする。ただし、機構が別形式による提出を求めた場合はこの限りではない。

（２）　提出内容の修正

提出したドキュメント等の修正が発生する場合においては、修正後再編した媒体を速やかに提出すること。

（３）　機器構成に関する納品物(各２部)

①　機器構成に関する資料

（４）　マニュアルに関する納品物(各２部)

①　システム運用マニュアル

②　機器利用マニュアル

③　４．２記載のキッティング手順書

（５）　その他の納品物(必要部数)

①　２．８記載の工程表

②　ライセンス契約書

③　その他関連ドキュメント

２．１０　媒体及びマニュアルの提供

ハードウェア及び搭載ソフトウェアの使用に必要な媒体、マニュアル、「４．３　キッティング要件」記載の手順書は電子納品とする。現在、機構が賃借している既存機器等のマニュアルによる納品も可能とするが、変更があった場合は変更内容を反映したマニュアルを納品すること。

２．１１　検査及び引渡し

受注者立会いの上で、機構の指定する職員が総合動作状態、書類等の検査を実施する。受注者は、情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを証明すること。検査の結果、本調達機器等の全部又は一部に不合格品を生じた場合には、受注者は直ちに当該機器を引き取り、機構の指定する職員が定めた日時までにその代替品を納入するものとする。

検査の結果、合格となった場合は、配備に関する目録を一式を用意し、速やかに引き渡すこと。

２．１２　データ消去及び撤去作業

賃貸借期間の終了時又は履行期間中の故障による交換時には、本調達機器等内に保存されているデータが漏洩することのないよう対策を講じ、本調達機器、指定のマニュアル、媒体等を撤去すること。

また、撤去関連作業の詳細については、機構が指定する職員と打合せを実施するとともに、以下の業務を実施すること。

なお、本調達機器等の回収作業開始時から、データ消去を依頼した本調達機器等から情報漏洩があったと証明された場合、損害賠償請求をすることもありうる。

（１）　撤去関連作業工程表の作成

撤去関連作業について、機構が指定する職員の指示に従いデータ消去、撤去等に係る作業工程表を作成し提出すること。

（２）　本調達機器等の回収及び撤去

本調達機器、媒体、マニュアル等を回収すること。また、当該機器の搬送に対しては、破損の恐れのないように実施すること。

（３）　データ消去作業及び証明書の発行

いかなる方法をもってしてもデータの回復ができない方法により、本調達機器等よりデータを消去すること。

データ消去作業を実施した証明として、型番及び製造番号が記載された作業報告書兼データ消去証明書を発行すること。

２．１３　連絡指示事項

本仕様書の各項目に不明な点がある場合は、機構が指定する職員と随時打ち合わせを実施し、その指示に従うものとする。

２．１４　保守

（１）　保守業務の種類

保守業務の内容は、次のとおりとする。

①　事後保守

機構は、本調達機器等に異常が発生したときは、速やかに受注者に通知するものとし、受注者は、その通知を受けたときは、直ちに当該異常解消のための措置を講ずること。

②　受注者の報告義務

実施した保守業務があれば、詳細を月毎に書面により機構へ報告すること。

（２）　消耗品の提示

４．１（１）のほかに、本調達機器で利用する消耗品がある場合には、指定品を契約締結後速やかに提示すること。

（３）　保守部品

本調達機器に関して必要となる保守部品については、本調達に含めること。

（４）　機構の指示権

機構は、必要と認めるときは、受注者に対し、保守業務の実施方法又は実施内容の改善を指示することができるものとし、受注者はその指示を受けたときは、遅滞なく所要の措置を講じなければならない。

２．１５　その他

（１）　ハードウェア及びソフトウェアのライセンス登録が必要な場合は、受注者が代行し登録を行い、かつ登録の証明を示すライセンス書等を一式にし、機構へ納めること。また、ライセンス登録情報の変更、ライセンス登録の継続等についても、機構の指定する職員の指示に従い作業を行うこと。

（２）　本仕様書に記載のない事項であって、本調達に際し必要と認められる事項が発生した場合は、機構の指定する職員と協議し、その指示に従うこと。

３．タブレット端末の用途

導入するタブレット端末は全国の住宅相談窓口に設置し、主に以下の目的で利用する。

- 賃貸住宅の契約の際に、お客様が希望される場合は来店によらず本タブレット端末上で TV 会議システムを利用し、オンラインで契約内容説明を行う。
- ブラウザを利用し、賃貸住宅をお探しのお客様に UR 賃貸住宅 WEB サイトを閲覧いただく。
- お客様に賃貸借契約時説明内容の動画をご視聴いただく。

４．端末等要件

４．１　タブレット端末要件

（１）　ハードウェア要件

機　器			数　量
iPad Wi-Fi モデル			150
1	OS	iOS	
2	画面サイズ	10.2 インチ以上	
3	画面解像度	2,160×1,620px 以上	
4	CPU	A12 Bionic 以上	
5	ストレージ	32GB 以上	
6	Wi-Fi 規格	Wi-Fi （802.11ac） 以上	
保護シート			150
1	タブレット端末の前面を覆うフィルムタイプのものであること。		
2	覗き見防止機能のあるシートであること。		
3	指紋等の汚れが残りにくいものであること。		
4	貼付け時に気泡ができないよう工夫されていること。		
保護ケース			150

1	当該ケースを装着した状態で、タブレット端末の全てのインタフェースが使用できること。	
2	本体部分は耐衝撃性の高い素材（TPU 製等）であること。	
USB 電源ケーブル		150
USB 電源アダプタ		150

（２） 利用サービス要件

以下の機能を備えた MDM（モバイルデバイス管理）サービスであること。

なお、MDM サービスがクラウドサービスに該当する場合は、競争参加資格確認時点で ISMAP クラウドサービスリストに登録されているサービスであること。

① 端末管理

- ADE（Automated Device Enrollment）対応であること。
- Wi-Fi 利用制限
- ホワイトリストによる接続先サイトの制限
- アプリケーション利用制限
- アプリケーションのインストール/アンインストール制限
- リモートワイプ機能
- リモートロック機能
- パスワードリセット
- 一定時間無操作時の画面ロック
- メール機能の利用不可設定

② 設定登録

- 設定値の一括登録
- パスワードポリシー設定
- アプリケーション配布

③ 状況確認

- デバイス情報管理
- 設定情報管理

４．２ キッティング要件

- タブレット端末に対し、OS のログインパスワードを端末ごとに設定すること。なお、ログインパスワードについては８桁以上とし、英数字及び記号を用いた複雑性を持たせたものとすること。
- Wi-Fi 利用制限を行うこと。
- 機構が別途調達する「令和５年度契約内容説明用 WiFi ルータの調達」の受注者から納品を受けた WiFi ルータとの接続の設定を行うこと。
- ホワイトリストによる接続先サイトの制限を行うこと。
- スクリーンショット機能、電話機能、アドレス帳機能、メール機能、SMS 機能、FaceTime 機能、スケジュール機能等を使用不可とすること(MDM サービスによる制限を行うこと。)。

なお、使用不可の設定ができない場合は、端末上に「利用不可」のフォルダを作成し、そのフォルダに入れる等の対策を行い、容易に利用できないようにすること。

・　アプリケーションのインストール/アンインストール制限を行うこと。
・　リモートワイプ機能を有効にすること。
・　リモートロック機能を有効にすること。
・　液晶保護フィルム貼付、タブレット端末へのSIMカードの格納、動作確認を行うこと。
・　テザリング機能を無効にすること。
・　USBによる他との端末との接続を不可とすること。
・　機構が指定する仕様及び条件に基づき識別シールを作成し、導入する機器に貼付すること。識別シールの詳細な仕様等については、受注者へ開示する。
・　上記キッティング作業の手順書を作成すること。

５．支払

５．１　支払

毎月払いとする。

６．保守要件

６．１　保守対応時間

保守対応時間は9：30～18：00とする。対応日は年末年始を除く毎日。１時間以内に保守対応を開始すること。

６．２　稼動維持作業

（１）　保守サービス

本調達で導入した機器（予備電池等のオプション品含む）、ソフトウェア等において、機器の故障等（電池については充電耐用回数を超え通常使用に支障をきたす場合を含む。）の障害が発生した場合、無償修理・交換が可能な保守サービスを提供すること。ただし、保護シート、保護ケース、USB電源ケーブル及びUSB電源アダプタは消耗品とし、消耗品は保守サービスの対象外とする。

なお、構築期間中の保守サービスについては、受注者負担とする。

（２）　問合せ窓口の設置について

本調達で導入したハードウェア・ソフトウェアにおいて、タブレット端末配布先における機構担当者からの問合せ窓口を設置すること。

６．３　保守作業

・　機器の障害等によるOS環境及び導入ソフトウェアの再セットアップが必要な場合は、受注者の負担と責任において再セットアップを行った上、適切な動作確認を行うこと。

７．運用要件

７．１　タブレット端末等紛失時における対応について

タブレット端末等の紛失が生じた場合、機構及び機構が別途発注した業務の受注者等からの依頼に基づき、以下のとおり業務を行うこと。

（１）　対応時間

オペレータが 365 日 24 時間受付けるものとし、即時に対応を開始すること。

（２）　業務内容

MDM サービスによる４．１（２）①に掲げる操作

８．再委託

８．１　再委託に関すること

（１）　受注者は、作業の全部を第三者に委託又は請け負わせてはならない。作業の一部を第三者へ委託する場合、機構の承認を得ること。

（２）　受注者が作業の一部を第三者に委託する場合、受注者は知的財産権、情報セキュリティ（機密保持及び遵守事項）、ガバナンス等に関して本仕様書が定める受注者の債務一切を再委託先事業者も負うよう、必要な処置を実施し、機構に報告し、承認を得ること。

なお、第三者に委託する場合も、当該事業者において同様の措置を定め、その最終的な責任を受注者が負うこと。

９．情報セキュリティが侵害された場合の対処

（１）　本調達に係る業務の遂行において、定期的に情報セキュリティ対策の履行状況を報告するとともに情報セキュリティが侵害され又はその恐れがある場合には、直ちに機構に報告すること。これに該当する場合には、以下の事象を含む。

（イ）受注者に提供し、又は受注者によるアクセスを認める機構の情報の外部への漏えい及び目的外利用

（ロ）受注者による本業務の範囲を超えた、機構が認めない情報への不正なアクセス

（２）　また、被害の程度を把握するため、受注者は必要な記録類を契約終了時まで保存し、機構の求めに応じて成果物とともに機構に引き渡すこと。

（イ）情報セキュリティ侵害の内容及び影響範囲を調査の上、当該情報セキュリティ侵害への対応策を立案し、機構の承認を得た上で実施すること。

（ロ）発生した事態の具体的内容、原因及び実施した対応策等について報告書を作成し、機構へ納入して承認を得ること。

（ハ）再発防止対策を立案し、機構の承認を得た上で実施すること。

（ニ）上記のほか、発生した情報セキュリティ侵害について、機構の指示に基づく措置を実施すること。

10. 情報セキュリティ対策に関する事項

政府機関統一基準等関連ガイドラインを理解した上で、次の機構の定めるセキュリティ関連規程及び個人情報保護規程を遵守し、システムの構成や特性に応じ情報の機密性・完全性・可

用性を各々適切に確保し取組を行うものとすること。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。

【機構の定めるセキュリティ関連規程及び個人情報保護規程】

イ　独立行政法人都市再生機構情報化等管理規程（平成 20 年規程第 21 号）

ロ　独立行政法人都市再生機構情報化等管理に関する達（平成 20 年達 21 号）

ハ　独立行政法人都市再生機構情報セキュリティ管理に関する規程（平成 20 年規程第 22 号）

ニ　独立行政法人都市再生機構情報セキュリティ管理に関する達（令和３年達第 29 号）

ホ　独立行政法人都市再生機構個人情報保護規程（平成 17 年規程第１号）

【政府機関統一基準等関連ガイドライン】

イ　政府情報システムの整備及び管理に関する標準ガイドライン（平成 26 年 12 月３日各府省情報化統括責任者(CIO)連絡会議決定）

ロ　政府機関等の情報セキュリティ対策のための統一基準群（令和３年度版７月７日内閣サイバーセキュリティセンター）

（イ）政府機関等の情報セキュリティ対策のための統一規範

（ロ）政府機関等の情報セキュリティ対策の運用等に関する指針

（ハ）政府機関等の情報セキュリティ対策のための統一基準（令和３年度版）

（ニ）政府機関等の対策基準策定のためのガイドライン（令和３年度版）

ハ　「高度サイバー攻撃対処のためのリスク評価等のガイドライン」(内閣サイバーセキュリティセンター)

(イ)『高度標的型攻撃』対策に向けたシステム設計ガイド(独立行政法人情報処理推進機構)

（ロ）『新しいタイプの攻撃』の対策に向けた設計・運用ガイド（独立行政法人情報処理推進機構）

（ハ）『標的型メール攻撃』対策に向けたシステム設計ガイド（独立行政法人情報処理推進機構）

ニ　「クラウドセキュリティガイドライン活用ガイドブック（2013 年度版)」(経済産業省)

ホ　「クラウドサービスの安全・信頼性に係る情報開示指針（総務省)」

（イ)「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）2021 年９月」

（ロ)「ASP・SaaS 事業者連携ガイド（平成 24 年７月策定)」

（ハ)「データセンターの安全・信頼性に係る情報開示指針（平成 23 年 12 月改定)」

（ニ)「IaaS・PaaS の安全・信頼性に係る情報開示指針（平成 23 年 12 月策定)」

（ホ)「ASP・SaaS の安全・信頼性に係る情報開示指針（平成 19 年 11 月策定)」

ヘ　「安全なウェブサイトの作り方　改訂第７版　2021 年３月」(独立行政法人情報処理推進機構)

（イ）付属 :「セキュリティ実装 チェックリスト」

（ロ）別冊 :「安全な SQL の呼び出し方（2010 年３月 18 日公開)」

（ハ）別冊 :「ウェブ健康診断仕様（2012 年 12 月 26 日公開)」

ト　「ISO／IEC 15408(CC) IT セキュリティ評価及び認証制度(JISEC) 」(独立行政法人情報処

理推進機構）

チ　「サイバーセキュリティ経済基盤構築事業クラウドセキュリティ監査制度の見直し（平成27年２月）」（経済産業省）

リ　「政府情報システムのためのセキュリティ評価制度（ISMAP）」（令和２年１月30日サイバーセキュリティ戦略本部決定）

ヌ　「スマートフォン&タブレットの業務利用に関するセキュリティガイドライン」（2014年３月25日）