オープンカウンター方式による見積合せの公示

次のとおり、オープンカウンター方式による見積合せを実施します。

令和８年９月 14 日

独立行政法人都市再生機構

東日本都市再生本部

本部長 松村　秀弦

1　調達内容

(1)　調達件名

令和８年度既存の機器材を活用したネットワークカメラシステムの整備及び保守管理業務

(2)　調達内容詳細

仕様書による。

(3)　履行期間

契約締結日の翌日 から 令和９年９月 30 日 まで

(4)　履行又は納入場所

仕様書による。

(5)　見積方法

見積金額は、総価を記載すること。

契約の相手方の決定に当たっては、見積書に記載された金額に当該金額の 100 分の 10 に相当する額を加算した金額（当該金額に１円未満の端数があるときは、その端数金額を切り捨てた金額とする。）をもって決定価格とするので、見積書を提出する者は、消費税及び地方消費税に係る課税事業者であるか免税事業者であるかを問わず、見積もった契約希望金額の 110 分の 100 に相当する金額を見積書に記載すること。

なお、見積書は本公示に記載の書式を使用すること。

2　参加資格

(1)　独立行政法人都市再生機構会計実施細則（平成 16 年独立行政法人都市再生機構達第 95 号）第 331 条及び第 332 条の規定に該当する者でないこと。

(2)　当機構東日本地区における令和７・８年度物品購入等の契約に係る競争参加資格審査において、「役務提供」に係る競争参加資格の認定を受けていること。

※「全省庁統一資格」は当機構の競争参加資格とは関係ないため注意すること。

(3)　公示日から見積合せ日までの期間に、当機構から本件の履行場所を含む区域を措置対象区域とする指名停止を受けていないこと。

(4)　暴力団又は暴力団員が実質的に経営を支配する者若しくはこれに準ずる者でないこと。

(5)　本公示、仕様書及びオープンカウンター方式による見積合せ説明書（当機構ホームページ→入札・契約情報→入札・契約の合理化のための取組み→オープンカウンター方式（https://www.ur-net.go.jp/order/aratanatorikumi.html）参照）等を承諾していること。

3　見積書の提出場所等

(1)　見積書の提出場所及び見積手続等に関する問合せ先

〒163-1315　東京都新宿区西新宿６丁目５番１号　新宿アイランドタワー15 階

独立行政法人都市再生機構東日本都市再生本部　総務部経理課

電話　03-5323-0705

(2)　見積書の提出期限及び提出方法

①　提出期限　令和８年９月 18 日（金）16 時 00 分

②　提出方法

②-1　持参又は郵送による提出方法　（押印した見積書）

持参又は同日同時刻必着の書留郵便による郵送とする。なお、郵送による場合は二重封筒とし、表封筒に「オープンカウンター見積書在中」と必ず朱書きすること。提出場所は上記（1）と同じ。

②-2　電子メールによる提出方法　（押印を省略した見積書）

本件は見積書を電子メールにより提出することができる。ただし、「押印を省略し責任者情報を記載のうえ、PDF 形式とした見積書」とし、提出期限までに下記専用電子メールアドレスに送信され、受信確認できたものに限る。

専用電子メールアドレス　tosai-keiri@ur-net.go.jp

※見積書送付時の電子メールの件名に【9/18 オープンカウンター見積書】と記載すること。

※見積書送付の電子メール本文中に、住所・会社名・担当者氏名・連絡先電話番号を記載すること。

(3)　見積合せの日時

見積書の提出期限後、遅滞なく実施する。なお、見積参加者の立会は求めない。

4　その他

(1)　契約保証金　免除

(2)　契約書作成の要否　不要

(3)　見積りの無効

本公示に示した競争参加資格のない者のした見積り及び見積りに関する条件に違反した見積りは無効とする。

(4)　契約の相手方の決定方法

独立行政法人都市再生機構会計規程第 52 条の規定に基づいて作成された予定価格の制限の範囲内で最低価格をもって有効な見積りを行った者を契約の相手方とする。

(5)　競争参加資格の認定を受けていない者の参加

上記 2(2)に掲げる競争参加資格の認定を受けていない者も、上記 3(2)により見積書を提出することができるが、競争に参加するためには、見積書の提出より前に当該資格審査に係る申請書を提出し、当該資格の認定を受け、かつ、競争参加資格の確認を受けなければならない。

(6)　仕様書の内容に係る質問等の受付先

独立行政法人都市再生機構東日本都市再生本部

技術監理部企画第１課　担当：猪狩　　電話：03-3347-4288

以　上

見　　積　　書

金　　円也（税抜：総額）

ただし、令和８年度既存の機器材を活用したネットワークカメラシステムの整備及び保守管理業務

オープンカウンター方式による見積合せ説明書を承諾の上、見積りします。

年　　月　　日

住　所

会社名

代表者　　印 ※１

独立行政法人都市再生機構

東日本都市再生本部

本部長　松村　秀弦　殿

※１ 本件責任者（会社名・部署名・氏名）：

担 当 者（会社名・部署名・氏名）：

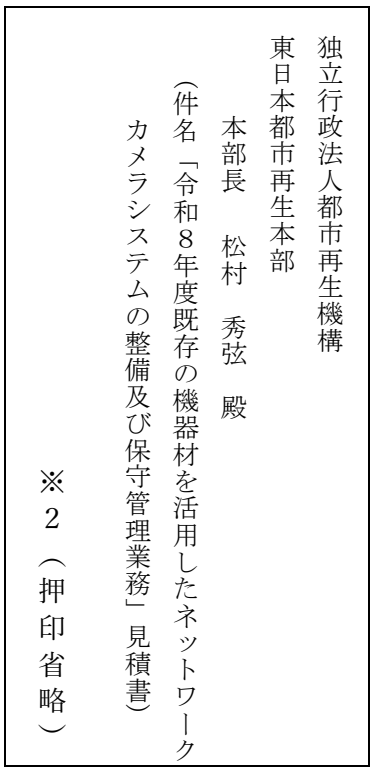
※２ 連絡先（電話番号）１　：

連絡先（電話番号）２　：

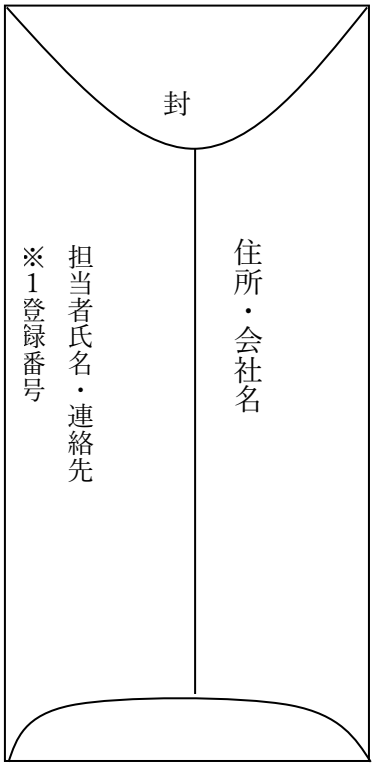
※１ 本件責任者及び担当者の記載がある場合は、押印は不要です。
押印する場合は、本件責任者及び担当者の記載は不要です。

※２ 連絡先は、事業所等の「代表番号」「代表番号+内線」「直通番号」等を記載。
個人事業主などで、複数回線の電話番号がない場合は、1 回線の記載も可。

表



裏



※１　当機構ホームページで公表されている「有資格者名簿（東日本地区）物品購入等」に記載されている登録番号を記載すること。なお、競争参加資格を申請中の者にあっては、「競争参加資格申請中」と記載すること。提出された見積書については、開封の前後を問わず、引換え、変更又は取消しをすることができないので注意すること。

※２　押印を省略する場合は、封筒に「（押印省略）」と記載すること。

令和８年度既存の機器材を活用したネットワークカメラシステムの整備及び保守管理業務
仕　様　書

1　業務の目的

当機構が過年度業務において工事現場に設置した既存のカメラ等機器材を活用して、工事進捗や災害発生時の状況、現場の課題等をリアルタイムに関係者間で共有できるネットワークカメラシステムを整備し、当該システムを保守管理することを目的とする。

2　業務の履行期間

契約締結日の翌日から令和９年９月30日まで

3　業務責任者等

受注者は、本契約に係る総括的な連絡、調整等を行う業務責任者を定め、発注者に書面（様式は任意）で契約後速やかに通知するものとする。

4　業務の内容

既存のカメラ等機器材を活用し、工事現場を撮影した映像をリアルタイムに閲覧、確認できるネットワークカメラシステム及び、クラウドサービス（データ通信含む）を調達して整備し、当該システムが使用可能な状態を維持するための保守管理を行う。また、今後当機構が新たにネットワークカメラシステムを調達するに当たり、調達方法・仕様・運用の検討に係る基礎資料及び方針案の作成を行う。

(1)　①、②を調達し、ネットワークカメラシステムを整備すること。
　① クラウドサービス　　ELMO　QBiC CLOUD　5回線、12か月間
　② データ通信　　固定カメラ　5回線、12か月間

(2)　固定カメラ２台について、設置場所を別の地区へ変更する。地区間の機材運搬及び移動先での動作確認を実施すること。移動については東京都内（品川区）→神奈川県内（藤沢市）、東京都内（品川区）→神奈川県内（鎌倉市）をそれぞれ想定。具体の地区については別途指示する。

(3)　固定カメラ１台について、東京都内（品川区→新宿区内の当機構事務所を想定）で機材運搬を行い、一定期間経過後に処分すること。なお、当該期間における保管は当機構が行う。詳細については別途指示する。

(4)　データ通信においては、映像を遅延や乱れなくリアルタイムに閲覧できるものを選定し、データ通信容量は無制限とすること。

(5)　保守管理においては、セキュリティの管理及びトラブル時の電話によるサポートを主とし、必要に応じて現地での保守対応を行うこと。また、工事の進捗により撮影箇所の変更が必要になった場合、カメラ設置位置の変更に伴う通信状況の点検や通信回線の切り替え等に対応すること。

(6)　当該システムに対する各工事現場担当者へのヒアリング、現状の課題の抽出、他機関等におけるシステムの事例調査を実施し、当機構から示す必要要件を踏まえ、新たにネットワークカメラシステムを調達するための調達方法・仕様・運用等の検討に係る基礎資料及び方針案を作成する。

なお、成果については業務完了時に書面で報告すること。

(7)　閲覧は、パソコン、タブレット、スマートフォンで対応できるようにすること。

・パソコンの場合は専用ソフト不要でブラウザへの URL 入力で閲覧できるようにする。

・タブレット、スマートフォンの場合はアプリ対応（Android、iOs）とする。

(8)　撮影したデータは 30 日で上書きするサイクルとすること。

(9)　詳細のセキュリティ要件については「7　セキュリティ要件」を確認すること。

＜参考＞

当機構が所有する既存の機器材については次のとおり。

固定カメラ　　ELMO　QBiC CP-2LTE　　6 台

機器の設置場所と個数については以下のとおり。

	東京都品川区	東京都港区	東京都中野区	東京都新宿区
固定カメラ	2	2	2	0

※電源は全て商用電源を使用している。

5　守秘義務

業務の履行上知り得た事項は、一切外部へ漏らしてはいけない。ただし、書面により発注者の承諾を得たときは、この限りではない。

6　留意事項

(1)　本仕様書に記載の無い事項等、疑義が生じたときは、その都度当機構担当者と協議すること。

(2)　関係各所との打合せに必要な資料は、随時、当機構担当者と協議の上作成すること。

(3)　法令及び条例等の関係法令を遵守すること。

(4)　暴力団員等による不当介入を受けた場合の措置について

① 業務の履行に際して、暴力団員等による不当要求又は業務妨害（以下「不当介入」という。）を受けた場合は、断固としてこれを拒否するとともに、不当介入があった時点で速やかに警察に通報を行うとともに、捜査上必要な協力を行うこと。

② 上記により警察に通報を行うとともに、捜査上必要な協力を行った場合には、速やかにその内容を記載した文書により発注者に報告すること。

③ 暴力団員等による不当介入を受けたことにより、工程に遅れが生じる等の被害が生じた場合は、発注者と協議を行うこと。

(5)　情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、受注者は、当該事項について速やかに当機構に報告すること。

7　セキュリティ要件

業務に当たっては、以下のセキュリティ要件を遵守すること。

I.　作業の実施に当たっての遵守事項

1.　要保護情報を取り扱う作業実施前の対策

受注者は、要保護情報を取り扱う作業の実施までに、以下の内容を全て含む情報セキュリティ対策を整備すること。

一　受注者における情報の適正な取扱いのための情報セキュリティ対策の実施内容及び管理体制

二　以下の内容を含む、受注者において発生した情報セキュリティインシデントへの対処方法

イ　当事者及び関係者の役割を含む体制

ロ　インシデント対処体制、責任者、作業担当者から当該体制への報告フロー等の概要

三　情報セキュリティ対策の履行状況の確認方法

四　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

五　当機構との情報の受渡し方法や作業終了時の情報の廃棄方法等を含む情報の取扱手順

2.　要保護情報を取り扱う作業実施期間中の対策

(1) 受注者は、作業の実施期間を通じて、以下を全て含む対策を遵守すること。

一　受注者に提供する情報の受注者における目的外利用の禁止

二　当機構と合意した情報の取扱手順による情報の取扱い

三　作業において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、作業の一時中断などの必要な措置を含む対処及び報告手順に従った遅滞のない当機構への報告

(2) 受注者は、情報セキュリティ監査について、以下を全て含む内容を実施すること。

一　作業の遂行に当たり、当機構から指示があった場合には当機構の情報セキュリティ監査を受入れること

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

三　当機構が外部からの監査を受けるに当たり、当機構から指示があった場合には、監査の対応に関して協力すること

(3) 受注者は、作業の実施期間を通じて、作業における情報の適正な取扱いを担保するため、以下の内容を全て含む情報セキュリティ対策を実施すること。

一　作業の実施期間中に情報セキュリティインシデントの検出有無等について定期的な報告を行うこと

二　作業に関して当機構が提供する要保護情報を格納する機器等（記録媒体、紙媒体を含む）の使用や保管に係る対策を実施するため、情報を取り扱う機器等の物理的保護に関する以下の対策を実施すること

イ　情報又は機器等へのアクセスを許可されている要員だけに認めること

ロ　機器等を廃棄又は再利用する際は、事前にデータを抹消又は破壊すること

三　作業に従事する受注者の従業員等及び当機構が提供する要保護情報を取り扱う受注者内の情報システムにアクセスを許可する受注者の従業員等に、遵守すべき情報セキュリティ対策に関する事項を確実に認識させるため、情報を取り扱う要員への周知と統制に関する以下の対策を実施すること

従業員等の異動・退職等の際にアクセス権の削除や秘密保持の徹底等を求めること

四　作業に関して当機構が提供する要保護情報を取り扱う受注者内の情報システムが接続するネットワークの外部境界及び主要な内部境界において、通信又は送受信データを監視し、制御し、保護するため、受注者内の情報システムの完全性の保護に関する以下の対策を実施すること

イ　業務に必要な通信だけを許可し、許可していない不正な通信の発生を防止すること

ロ　不正利用防止のための職務分掌を徹底すること

3.　作業終了時の対策

受注者は、契約に基づき、作業の終了に際して以下を全て含む対策を実施すること。

一　作業の実施期間を通じてセキュリティ対策が適切に実施されたことの報告

二　提供を受けた情報を含め、作業において取り扱った情報の返却、廃棄又は抹消

4.　情報セキュリティポリシーの遵守

受注者は、政府機関統一基準等関連ガイドラインを理解した上で、次の当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。

【当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】

一　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）

二　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 年達第 21 号）

三　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（令和 5 年規程第 27 号）

四　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 5 年達第 24 号）

五　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】

一　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）

二　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）（令和 5 年 7 月 4 日、サイバーセキュリティ戦略本部・内閣サイバーセキュリティセンター）

イ　政府機関等のサイバーセキュリティ対策のための統一規範

ロ　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）

ハ　政府機関等の対策基準策定のためのガイドライン（令和 5 年度版）

三　「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）

四　「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）

五　「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）（令和 3 年 9 月改定）」

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 29 年 3 月改定)」
ニ　「IaaS・PaaS の安全・信頼性に係る情報開示指針（第 2 版）（平成 29 年 3 月改定)」
ホ　「ASP・SaaS の安全・信頼性に係る情報開示指針（ASP・SaaS 編）第 3 版（令和 4 年 10 月改定)」
六　「安全なウェブサイトの作り方　改訂第 7 版（令和 3 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（平成 22 年 3 月 18 日公開)」
ハ　別冊：「ウェブ健康診断仕様（平成 24 年 12 月 26 日公開)」
七　「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）
八　「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）
九　「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）

5.　再委託に関する対策

受注者は、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、「1.要保護情報を取り扱う作業実施前の対策」及び「2.要保護情報を取り扱う作業実施期間中の対策」の措置を再委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を当機構に提供し、当機構の承認を受けること。

II.　情報セキュリティ要件

1.　業務委託

（情報システムに関する業務委託における共通的対策）

(1)　受注者は、受注者、再委託先又はその他の者によって、情報システムに当機構が意図しない変更が加えられないための管理体制を確保する情報セキュリティ対策を実施すること。

（情報システムの運用・保守を業務委託する場合の対策）

(2) 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（物理的、ネットワーク環境的及び人的側面）を整備し、当機構の承認を得ること。

(3) 受注者は、受注者が実施する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、当機構に速やかに報告すること。

2.　情報システムのライフサイクルの各段階における対策

（情報システムの運用・保守時の対策）

(1) 受注者は、情報システムの運用・保守において、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。

(2) 受注者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理し、運用・保守によって機器の構成や設定情報

等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、見直しが必要な場合には当機構に提案すること。

（情報システムについての対策の見直し）

(3) 受注者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を当機構に提案すること。

3. サーバ装置

（サーバ装置の運用時の対策）

受注者は、クラウドサービスに新たな機能が追加されていないか、アクセス権が適切に付与されているか等を定期的に確認し、不適切な状態にあると判断した場合には改善を図ること。なお、改善を図る場合は、作業日、作業を行ったクラウドサービス名、具体的な作業内容及び作業者、正常動作を確認した者などを含む変更事項等を記録し、管理すること。

4. 情報システムのセキュリティ機能

（主体認証機能の導入）

(1) 受注者は、主体の識別及び主体認証を行う機能を設けること。なお、主体認証機能を設けるに当たっては、以下の主体認証方式を導入すること。

知識（パスワード等、利用者本人のみが知り得る情報）による認証

(2) 受注者は、主体認証を行う情報システムにおいて、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として、以下の対策を講ずること。

一 主体認証情報の漏えい等による不正なアクセスを防止するため、以下を全て含む措置を講ずること。

イ 原則として、機器等において初期値として設定されている識別コードを使用しない。

ロ 不要な識別コードを無効にする。

二 主体認証情報が第三者に対して明らかにならないよう、主体認証情報を送信又は保存する場合には、その内容を暗号化し、適切に管理すること。

（識別コード及び主体認証情報の管理）

(3) 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。）し、管理するため、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与すること措置を講ずること。

(4) 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、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、以下の措置を講ずること。

一 当該主体の識別コードを無効にする。

二 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。

（アクセス制御機能の導入）

(5) 受注者は、情報システムの特性、情報システムが取り扱う情報の格付及び取扱制限等に従い、権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。

(6) 受注者は、主体の属性、アクセス対象の属性に基づき、以下のアクセス制御を実施すること。

権限を有する者のみがアクセス制御の設定等を行うことができる機能を設けること。

(7) 受注者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス

制御機能を適切に運用すること。また、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を適時確認により、見直すこと。

（権限の管理）

(8) 受注者は、主体から対象に対するアクセスの権限を必要最低限の範囲で適切に設定するよう、措置を講ずること。

(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として、以下の対策を講ずること。

一　業務上必要な場合に限定する

二　管理者権限を有する識別コードの利用は権限を必要とする業務に限定し、一般の業務として使用させないこと。

(10) 受注者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認すること。

III. 機器等の管理に関して

工事現場におけるカメラ等機器材の盗難防止のため、ワイヤーによる固定や施錠等の物理的な措置を講じること。

以　上