令和７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８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、発注者に書面で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を、クラウドサービス（データ通信含む）を調達して整備すること。また、ネットワークカメラシステムが使用可能な状況を維持するための保守管理を行い、業務完了時には当該システム運用状況を検証すること。

(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　6回線、15か月間
　② データ通信　　固定カメラ　6回線、15か月間

(2)　固定カメラ３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。移動先については東京都内を想定。具体の地区については別途指示する。

(3)　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。

(4)　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。

(5)　運用状況については、各工事現場担当者へのヒアリング等を行い、当該システムの利用状況や成果及び課題点を検証し、業務完了時に書面で報告すること。

(6)　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。

(7)　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。

(8)　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以下①～④の通り。

① 固定カメラ　　ELMO　QBiC CP-2LTE　　6 台
② ウェアラブルカメラ　ELMO　Wearable Camera EW-1　　4 台
③ モバイルルーター　　FUJISOFT　FS030W　　4 台
④ ソーラーシステム　　太陽電池：Next Energy　RS-160-12　　9 台
充電コントローラー：Next Energy　MPPT100/30　　3 台
インバーター：Yinleader　正弦波 12V500W　　3 台
バッテリー：ACDelco　M31MF　　15 台
バッテリー充電器：ACDelco　AD-2002　3 台

機器の設置場所と個数については以下の通り。() 内は未稼働。

		東京都大田区	東京都港区	東京都中野区	東京都新宿区
固定カメラ		1(1)	2	2	0
ウェアラブルカメラ		(1)	(1)	(1)	(1)
モバイルルーター		(1)	(1)	(1)	(1)
ソーラーシステム	太陽電池	3(3)	(3)	0※	0
	充電コントローラー	1(1)	(1)		
	インバーター	1(1)	(1)		
	バッテリー	5(5)	(5)		
	バッテリー充電器	1(1)	(1)		

※商用電源を使用のため、ソーラーシステムは未設置。

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、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。

7　セキュリティ要件

業務にあたっては、以下のセキュリティ要件を遵守すること。

I.　作業の実施にあたっての遵守事項

1.　要保護情報を取り扱う作業実施前の対策

(1) 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　作業の遂行にあたり、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あたり、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

イ　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

(1) 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

(1) 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

（1）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、以下の情報セキュリティ対策を実施すること。
一　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の確保

（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)

(1) 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。

一 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、以下の措置を講ずること。

一 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。

(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。

一　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。

二　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。

(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し、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

(1) 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