別 添

令和7～11 年度
第4次原子力規制委員会ネットワークシステムの
構築及び運用・保守業務
調達仕様書案

令和6年 10 月

原子力規制委員会原子力規制庁

長官官房総務課情報システム室

目次

1　調達案件の概要

(1) 調達件名

令和7～11 年度第4次原子力規制委員会ネットワークシステムの構築及び運用・保守業務

(2) 調達の背景

原子力規制委員会（以下「当委員会」という。）は、国民の生命、健康及び財産の保護、環境の保全並びに我が国の安全保障に資するため、原子力利用における安全の確保を図ること（原子力に係る製錬、加工、貯蔵、再処理及び廃棄の事業並びに原子炉に関する規制に関することを含む。）を任務とする組織である。

現行の原子力規制委員会ネットワークシステム（以下「行政 LAN」という。）は、当委員会の IT 基盤として、令和3年度（令和4年1月）に運用を開始している第3次行政 LAN であり、令和 8 年度に第4次行政 LAN への更改を予定している。一方で、各省庁においては、デジタル庁が整備するガバメントソリューションサービス（GSS）への移行が推進されており、当委員会においても GSS に移行する。GSS への移行にあたっては、第3次行政 LAN の機能のうち、GSS にて具備されない機能や第3次行政 LAN 上で稼働している情報システムの移行を併せて検討する。

そのほか、当委員会は令和9年度以降に本庁舎の移転を予定しており、第4次行政 LAN の稼働期間中に新庁舎へ移転することを想定している。

(3) 調達目的及び調達の期待する効果

前述の背景を踏まえ、第 4 次行政 LAN の整備と GSS への円滑な移行とともに、運用業務の効率化、セキュリティの維持向上及びデジタル化対応を目的とする。加えて、当委員会が別途構築・運用している安全研究用解析ネットワークシステム及び高機密性情報ネットワークシステムについて、第4次行政 LAN の構築に併せて運用の統合を推進する。また、将来的に統合原子力防災ネットワークシステム及び内閣府防災システムと連携できるよう、ネットワークの拡張性を備える。

（4） 業務・情報システムの概要

行政 LAN の概要は次の図のとおりである。

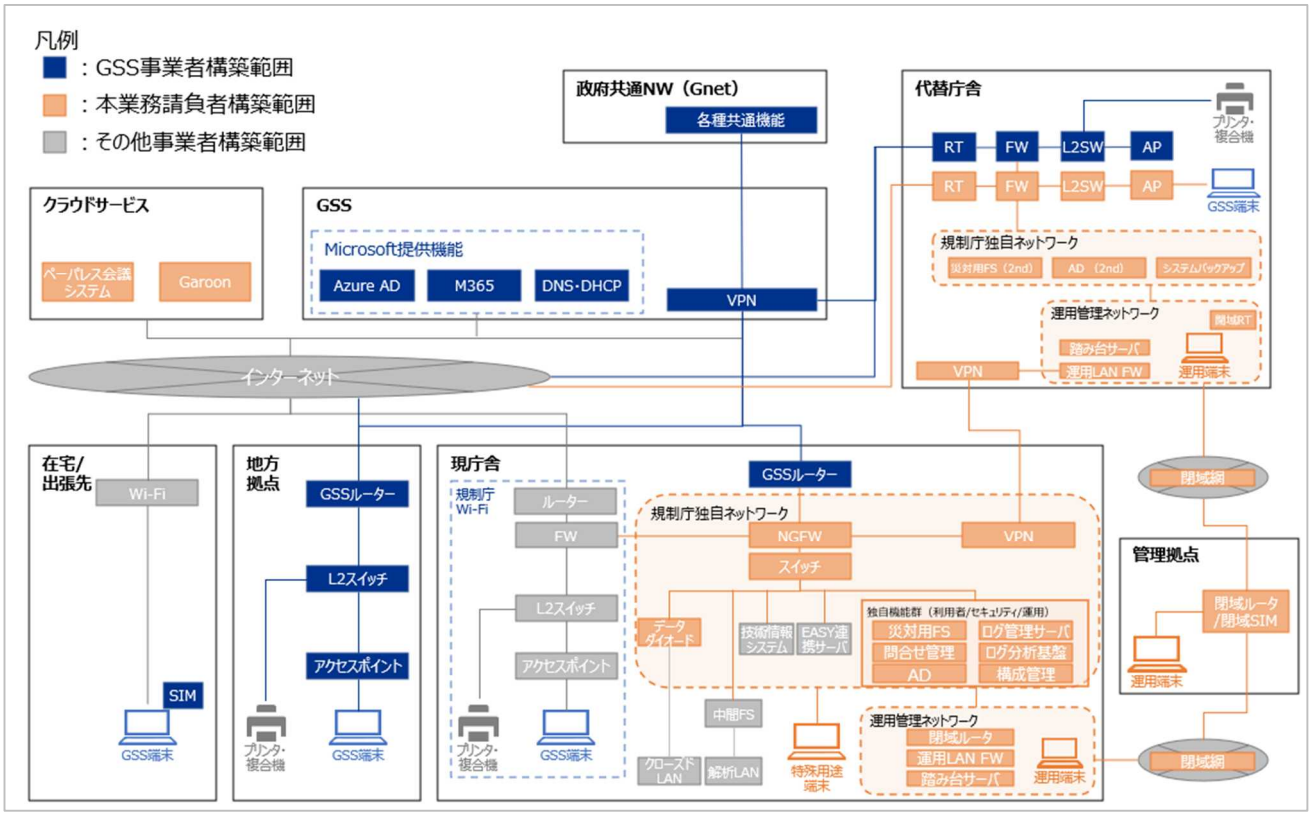

図 1 システム構成

（5） 契約期間

契約締結日から令和 12 年3月 31 日までとする。なお、賃貸借期間はシステムの運用開始日から令和 12 年3月 31 日までとする。

（6） 作業スケジュール

作業スケジュールは以下を想定している。

設計工程については、同時期にデジタル庁が GSS 標準機能の設計・構築（本庁舎内のネットワーク含む）を行うため、デジタル庁から問い合わせ等があった場合に対応することを想定する。また、試行については、一部の職員が GSS を先行して利用することで、デジタル庁が整備する標準機能のトライアルや、GSS ヘルプデスクとの連携を含めた本業務請負者の統合運用窓口の習熟を図ることを目的とする。

なお、当庁が GSS に移行する令和8年7月末（予定）までは第3次行政 LAN が運用している。関連する調達案件について、「2.(2) 調達案件及びこれと関連する調達案件」を参照すること。また、設計・構築に係るスケジュールは、デジタル庁の計画を踏まえた上で、担当職員と協議し、変更してもよい。

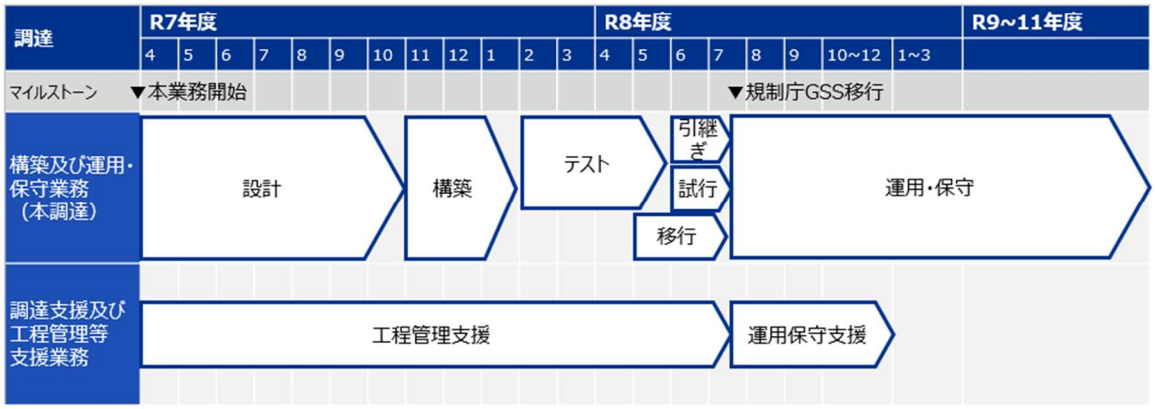

図 2 作業スケジュール

52
53 （7） 用語集
54 本書で使用する用語の定義を以下に示す。
55
56 表 1 用語集

No.	分類	用語	定義
1	情報システム	行政 LAN	原子力規制委員会ネットワークシステム。 原子力規制庁本庁舎及び全国に所在する地方拠点を結び、庁内の IT 基盤として原子力規制庁職員等の利用者に一般行政事務向けのサービスを提供するためのシステム。
2		ガバメントソリューションサービス（GSS）	デジタル庁が一般行政事務を遂行するために必要なツールや機器等を、府省庁共通的に提供する業務実施環境の総称
3		GSS 標準機能	本書において、GSS が提供する機能を指す。Microsoft 365（E5）を基盤とする機能、本庁及び地方拠点のネットワークや端末等を含む
4		第 4 次行政 LAN（規制庁独自機能）	本業務請負者が設計構築及び運用保守を行うネットワークシステム。第 3 次行政 LAN の機能のうち、GSS に移行できない一部の利用者機能並びに付随するセキュリティ機能及びネットワークを指す
5		第 3 次行政 LAN（現行行政 LAN）	令和 4 年 1 月に運用を開始した当委員会における庁内ネットワークシステム。令和 8 年 7 月末までの運用を想定している
6		第 5 次行政 LAN	令和 12 年 4 月に運用開始を予定する第 4 次行政 LAN の後継システム
7		個別システム	当委員会の各課室が所管する個別の施策等を実現するために利用しているシステムの総称
8		安全研究用解析ネットワークシステム（解析 LAN）	安全研究分野の解析業務で用いるクライアント端末、サーバやネットワーク等で構成される独立したネットワークシステム。GSS を介し在宅からのリモートアクセスを可能とする
9		高機密性情報ネットワークシステム（クローズド LAN）	機密性の高い情報をインターネット環境及び他システムから隔離して管理するためのクライアント端末、サーバやネットワーク等で構成される独立したネットワークシステム
10		統合原子力防災ネットワークシステム（統原防 NW）	原子力災害等発生時に、内閣府・原子力発電施設・オフサイトセンター・原子力規制庁本庁舎等の間での通信を可能とする独立したネットワークシステム
11		内閣府防災システム（NISS）	防災関係機関が横断的に情報共有を行うために内閣府が整備しているシステムの総称。令和 9 年度更改予定の次期 NISS では、システム管轄元が規制庁に移管
12	端末・機器	GSS 端末	デジタル庁が整備する、職員等が一般行政事務に利用する端末（PC）
13		運用管理端末	本業務請負者が第 4 次行政 LAN の運用・保守業務に利用する端末（PC）
14		特定用途端末	職員等が一部の業務に用いる端末（PC）。当庁の業務に伴う特殊なソフトウェアの利用や端末の運用の実現のために、原子力規制庁が調達し、本業務請負者がセットアップ等を行う
15		スタンドアロン端末	特定用途端末のうち、GSS、第 4 次行政 LAN、解析 LAN、クローズド LAN に接続せず、各課室が業務に使用している端末

No.	分類	用語	定義
16		公用スマートフォン	当庁から貸与を受けて、職員等が行政 LAN に接続して利用するスマートフォン
17		公用タブレット	職員等及び組織外関係者が、会議における資料閲覧等の目的で、当庁から貸与を受けて利用するタブレット
18		BYOD 端末	当庁の許可を得た上で、職員等が行政 LAN に接続して利用する私用のスマートフォン及びタブレット
19		通信回線装置	通信回線間又は通信回線と情報システムの接続のために設置され、回線上を送受信される情報の制御等を行うための装置（ハブ、スイッチ、ルータ等のほか、ファイアウォール等も含まれる）
20	拠点	本庁舎（現庁舎）	原子力規制庁がある六本木ファーストビルのこと
21		新庁舎	令和 9 年度に移転を予定している本庁舎のこと
22		地方拠点等	各地域にある原子力規制庁の事務所のこと
23		代替庁舎	首都直下地震等発生時に本庁舎の使用が困難となった場合、一時的に代替するための庁舎のこと。代替庁舎は東京都多摩地域中部に位置する
24	ネットワーク	GSS ネットワーク	本書において、デジタル庁が整備する、本庁舎（新庁舎）、地方拠点及び GSS を接続する広域ネットワークを指す
25		規制庁独自ネットワーク	本庁舎及び新庁舎に構築する、規制庁独自機能や個別システムを接続するための LAN ネットワーク
26		運用管理 LAN	第 4 次行政 LAN の運用・保守業務を実施するための独立したネットワーク
27		規制庁 Wi-Fi	本庁舎内に設置されたインターネット接続用のネットワーク。本庁舎から新庁舎に移転するまでの間、暫定的に GSS 端末を接続し、GSS（M365 等）やインターネットへの接続に用いる。当該ネットワークは、本案件と同時期に帯域の増強等を行う（本調達の範囲外）
28	組織等	職員等	行政 LAN を利用して業務を実施する、当委員会の委員、原子力規制庁の職員及び組織外を含む業務関係者（第 4 次行政 LAN の運用事業者含む）
29		担当職員	行政 LAN を所管する原子力規制庁総務課情報システム室の担当者であり、行政 LAN の PJMO メンバー
30		LAN 担当者	各課室に配置された、行政 LAN 運用に係る一部の業務を担当する職員
31		本業務請負者	本調達において、第 4 次行政 LAN の構築及び運用・保守業務を提供する事業者
32		庁内ネットワーク構築事業者	本庁舎内のインターネット回線（規制庁 Wi-Fi）を整備する事業者
33		デジタル庁	GSS を所管する政府機関
34		GSS ヘルプデスク	デジタル庁が所管する GSS の利用に係る問い合わせ等を受け付ける窓口
35		CSIRT（Computer Security Incident Response Team）	情報セキュリティインシデントに対処するため、当庁に設置された体制をいう

57

58

2　調達案件及び関連調達案件の調達単位、調達の方式等

（1）調達範囲

調達案件の調達単位、調達の方式、実施時期は次の表のとおりである。

表 2 調達範囲

No	調達案件名	調達の方式	実施時期
1	令和7～11 年度第4次原子力規制委員会ネットワークシステムの構築及び運用・保守業務	一般競争入札（総合評価落札方式（技術点と価格点の配点割合を3：1とする加算方式））	・意見招請（官報公示）：令和6年 10 月 15 日 ・入札公告（官報公示）：令和7年1月（予定） ・落札者決定：令和7年3月（予定）

なお、原子力規制庁では、令和9年度に本庁舎の移転を予定している。移転に係る作業は本業務に含めないが、第4次行政 LAN の運用・保守期間中に移転することとなった場合には協力すること。

（2）調達案件及びこれと関連する調達案件

調達案件及びこれと関連する調達案件の調達単位、実施時期等は次の図のとおりである。

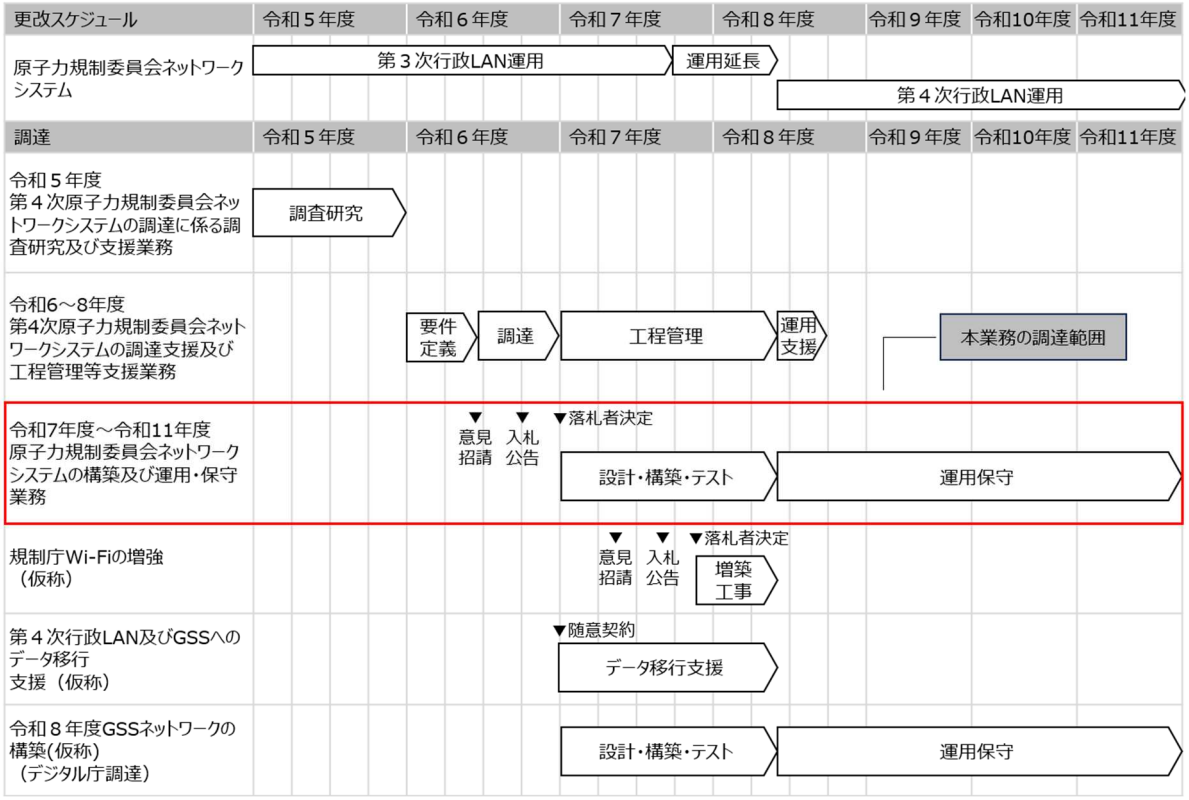

図 3 調達案件及びこれと関連する調達案件の調達単位、実施時期等

（3） 調達案件間の入札制限

相互牽制の観点から、「令和7～11 年度第4次原子力規制委員会ネットワークシステムの構築及び運用・保守業務」と「令和6～8年度第4次原子力規制委員会ネットワークシステムの調達支援及び工程管理等支援業務」は、相互に入札制限の対象とする。

3　情報システムに求める要件

本業務の実施に当たっては、要件定義書の各要件を満たすこと。

4　作業の実施内容

4．1　設計・構築業務

（1） 設計・構築実施計画書等の作成

設計・構築実施計画書等の作成に係る基本的な要件を以下に示す。

ア. 本業務請負者は、プロジェクト計画書及びプロジェクト管理要領と整合をとりつつ、担当職員の指示に基づき、工程管理支援業務請負者と調整の上、設計・構築実施計画書及び設計・構築実施要領の案を作成し、担当職員の承認を受けること。

イ. 設計・構築実施計画書及び設計・構築実施要領の記載内容は「デジタル・ガバメント推進標準ガイドライン」（令和6年5月 31 日、デジタル社会推進会議幹事会決定。以下「標準ガイドライン」という。）の「第3編 ITマネジメント／第7章　設計・開発」で定義されているものとすること。

ウ. 付属文書として作業項目、作業内容、スケジュールをより詳細に階層化し、担当者等を記載した WBS を作成すること。

エ. 情報資産管理標準シート及び情報システム台帳の更新に係る資料の提出時期を記載すること。

オ. 本業務請負者は、設計・構築実施計画書等の案について必要に応じて、担当職員とともに関係機関と調整すること。

（2） 設計

本システムの設計に係る基本的な要件を以下に示す。

ア. 本業務請負者は、調達手続き開始後の事情の変化、本業務請負者の提案等を踏まえ、要件定義の内容に関する認識に可能な限り相違が生じないよう、必要に応じて、担当職員とともに関係機関、情報システムの利用者、関係事業者と、要件定義の内容について確認及び調整を行うこと。また、これに伴い、必要に応じ、プロジェクト計画書の更新案を作成すること。

イ. 本業務請負者は、要件定義書の機能要件及び非機能要件を満たすための基本設計及び詳細設計を行い、成果物について担当職員の承認を受けること。その際、プロジェクトが円滑に実施されるよう、必要に応じて、担当職員とともに関係機関、情報システムの利用者、関係事業者と、要件

定義の内容について確認及び調整を行うこと。また、これに伴い、必要に応じ、プロジェクト計画書の更新案を作成すること。

ウ. 本業務請負者は、基本設計及び詳細設計を行うにあたり、第5次行政 LAN への更改の妨げとなる独自の仕様を含めないよう留意するとともに、担当職員の確認を受けること。

エ. 本業務請負者は、サプライチェーン・リスクに係る確認のため、提案書提出時及び契約締結以降の調達機器決定後に、導入するクラウドサービス、通信回線装置、サーバ装置、端末、プリンタ、特定用途機器、ソフトウェア、周辺機器及び外部電磁的記録媒体は、製造業者名、製造業者の法人番号、製品名及び型番、並びに再委託先の情報等（以下「機器・役務リスト」という。）を提出すること。なお、提出された様式2「機器・役務リスト（案）」について、担当職員がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、当該リスクに対応するため、代替品又はリスク低減対策の提出を求めることがあるので、速やかに応じること。

（3） 構築・テスト

本システムの構築・テストに係る基本的な要件を以下に示す。

ア. 本業務請負者は、構築にあたり、第4次行政 LAN の構築及び保守・運用を効率的に実施するため、構築やテスト等の標準（例：何をインプット（設計書等）として作業を行い、インプット情報に示された事項を確実に実装しテストしたことを記録するルールや第4次行政 LAN の各機能の重要度に応じたテストの網羅性と密度の設定ルール、さらにはテストの中に占めるセキュリティテストの網羅性と密度等の設定ルール等、設計されたものが確実に実装され適切な品質を保つことを可能とする構築及び運用・保守に係る標準）を定め担当職員の確認を受けること。本標準は、業務毎（構築標準等）に分けて策定しても良い。

イ. 本業務請負者は、構築に当たり、情報セキュリティ確保のためのルール遵守や成果物の確認方法（例えば、上記標準遵守の確認、インストール・設定内容の検査、現場での抜き打ち調査等についての実施主体、手順、方法等）を定め、担当職員の確認を受けること。

ウ. 本業務請負者は、単体テスト、結合テスト及び総合テストについて、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載したテスト計画書を作成し、担当職員の承認を受けること。

エ. 本業務請負者は、テストの実施において、検証と妥当性確認の両方の観点で行うこと。すなわち、要件定義や設計のとおり構築されたか評価を行う「検証」だけでなく、構築されたシステムがプロジェクト本来の目的を満たしているか評価する「妥当性確認」も行うこと。

オ. 本業務請負者は、設計工程の成果物及びテスト計画書に基づき、第4次行政 LAN の構築、テストを行うこと。

カ. 本業務請負者は、テスト計画書に基づき、各テストの実施状況を担当職員に報告すること。

キ. 本業務請負者は、構築・テストにあたって実運用環境やインターネットと接続する場合、事前に十分なセキュリティ対策を行い、かつ実データ等に影響を与えないよう配慮すること。

ク. 本業務請負者は、将来の保守や更改時におけるテスト工程の合理化に資するため、テストシナリオ・スクリプト、テストデータ等を保存し、保守後等の動作確認等において、それらを一部改変して再利用出来るようにすること。

（4） 受入テスト支援

本システムの受入テスト支援に係る基本的な要件を以下に示す。

ア. 本業務請負者は、担当職員が受入テストのテスト計画書を作成するに当たり、情報提供等の支援を行うこと。

イ. 本業務請負者は、担当職員が受入テストを実施するに当たり、環境整備、運用等の支援を行うこと。

ウ. 本業務請負者は、担当職員の指示に基づき、担当職員以外の情報システム利用者のテスト実施も含めて、テスト計画書作成の支援を行うこと。

エ. 本業務請負者は、受入テストの結果を踏まえ、担当職員による課題等の指摘または指導に対する対策を実施すること。

（5） 情報システムの移行

本システムの移行に係る基本的な要件を以下に示す。

ア. 本業務請負者は、担当職員が実施する第三次工程レビューの実施に先立ち、レビューに必要な情報の提供や資料の作成等の支援を行うこと。

イ. 本業務請負者は、本番環境へのシステム移行およびデータ移行に備えて、移行の方法、環境、ツール、段取り等を記載した移行計画書を作成し、担当職員の承認を受けること。その際、移行のリスクを低減するため、必要に応じ、担当職員とともに関係機関、関係事業者等と調整を行うこと。

ウ. 本業務請負者は、担当職員の移行判定を受けて、移行計画書に基づく移行作業を行い、移行結果を担当職員に報告すること。

エ. 本業務請負者は、第3次行政 LAN からのデータ移行に当たり、第4次行政 LAN のデータ構造を明示し、保有・管理するデータの変換、移行方法、例外データ等の処理方法等に関する手順書を作成し、担当職員の承認を受けること。

オ. 上記手順書に従い、データを変換・移行した後は、移行後のデータだけでなく、例外データ等についても確認を行い、データの信頼性の確保を図ること。

カ. 本業務請負者は、第3次行政 LAN から第4次行政 LAN への段階的な移行を計画・実施し、職員等が第3次行政 LAN を利用し行っている業務への影響の最小化を図ること。また、移行作業は、夜間帯や週末等を基本として計画・実施すること。

（6） 試行

本システムの試行に係る基本的な要件を以下に示す。

ア. 本業務請負者は、本システムへの切り替えに先立ち、一部の職員が本システムを先行して利用できる環境を提供すること。

イ. 試行期間において職員からの問い合わせに対応する体制を設けること。また、運用・保守業務やセキュリティ運用を行うこと。

ウ. 試行期間において利用者機能や運用等に係る課題が検出された場合、担当職員と改善方法及び時期を協議し、解消に向けて対応すること。

（7） 引継ぎ

本システムの引継ぎに係る基本的な要件を以下に示す。

ア. 本業務請負者は、設計・構築の設計書、作業経緯、残存課題等を文書化し、運用チーム、保守チーム及び情報セキュリティチームに対して確実な引継ぎを行うこと。

イ. 本業務請負者は要件定義書（4.2.2.3（エ） 教育）に示す、利用者、LAN 担当者に対する教育を行い、教育結果を担当職員に報告すること。

ウ. 本業務請負者は、担当職員が第5次システムに更改を行う際には、第5次行政 LAN における要件定義支援事業者及び設計・構築事業者等に対し、作業経緯、残存課題等に関する情報提供及び質疑応答等の協力を行うこと。

（8） 定例会等の実施

本システムの定例会等に係る基本的な要件を以下に示す。

ア. 本業務請負者は、定例会を適切な頻度で開催するとともに、業務の進捗状況を作業実施要領に基づき報告すること。

イ. 本業務請負者は、担当職員から要請があった場合、又は、本業務請負者が必要と判断した場合、必要資料を作成の上、定例会とは別に会議を開催すること。

ウ. 本業務請負者は、会議終了後、3 日以内（行政機関の休日（行政機関の休日に関する法律（昭和 63 年法律第 91 号）第1条第1項各号に掲げる日をいう。）を除く。）に議事録を作成し、担当職員の承認を受けること。

（9） 情報資産管理標準シート及び情報システム台帳の更新に係る資料等の提出

本システムの情報資産管理標準シート情報システム台帳の更新に係る資料提出に係る基本的な要件を以下に示す。

ア. 受注者は、標準ガイドラインの「別紙2 情報システムの経費区分」に基づき区分等した契約金額の内訳を記載した契約金額の内訳を記載した資料及び担当職員が提示するフォーマットに必要事項を記載した情報資産管理標準シートを契約締結後速やかに提出すること。なお、契約金額の内訳資料については、原子力規制庁における物品・資産管理のうえで必要に応じて追加の情報提供を求めることがある。

イ. 受注者は、当委員会から求められた場合は、スケジュールや工数等の計画値及び実績値について記載した資料を提出すること。

ウ. 受注者は、次に掲げる事項について記載した情報システム台帳の更新に係る資料を、設計・開発実施要領において定める時期に、提出すること。

（ア）開発規模の管理

情報システムの開発規模（工数、ファンクションポイント等）の計画値及び実績値

（イ）ハードウェアの管理

情報システムを構成するハードウェアの製品名、型番、ハードウェア分類、契約形態、保守期限等

（ウ）ソフトウェアの管理

情報システムを構成するソフトウェア製品の名称（エディションを含む。）、バージョン、ソフトウェア分類、契約形態、ライセンス形態、サポート期限等

（エ）回線の管理

情報システムを構成する回線の回線種別、回線サービス名、事業者名、使用期間、ネットワーク帯域等

（オ）クラウドサービス及び業務委託サービスの管理

情報システムを構成するクラウドサービス及び業務委託サービス利用形態、使用期間等

（カ）施設の管理

情報システムを構成するハードウェア等が設置され、又は情報システムの運用業務等に用いる区域を有する施設の施設形態、所在地、耐久性、ラック数、各区域に関する情報等

（キ）公開ドメインの管理

情報システムが利用する公開ドメインの名称、DNS 名、有効期限等

（ク）取扱情報の管理

情報システムが取り扱う情報について、データ・マスタ名、個人情報の有無、格付等

（ケ）情報セキュリティ要件の管理

情報システムの情報セキュリティ要件

（コ）指標の管理

情報システムの運用及び保守の間、把握すべき KPI 名、KPI の分類、計画値等の案

4．2　運用・保守業務

（1）中長期運用・保守計画の確定支援

本システムの中長期運用・保守計画の確定支援に係る基本的な要件を以下に示す。

ア．本業務請負者は、基本設計及び詳細設計に基づき運用設計及び保守設計を行うこと。なお、運用設計にはセキュリティ運用設計も含む。

イ．セキュリティ運用設計は、「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」（サイバーセキュリティ対策推進会議）に基づくリスクアセスメント結果に基づき行うこと。

ウ．本業務請負者は、運用設計及び保守設計に基づき、情報システムの第5次更改までの間に計画的に発生する作業内容、その想定される時期等を取りまとめた中長期運用・保守計画の案を作成し、担当職員の確認を受けること。

（2）運用・保守計画及び運用・保守実施要領の作成支援

本システムの運用・保守計画及び運用・保守実施要領の作成支援に係る基本的な要件を以下に示す。

ア．本業務請負者は、運用設計及び保守設計に基づき、定常時における月次の作業内容、その想定スケジュール、障害発生時における作業内容等を取りまとめた運用計画及び保守計画の案を作成し、担当職員の確認を受けること。

イ．運用計画及び保守計画の策定にあたっては、情報システム全体のセキュリティ水準が低下することのないように、第 4 次行政 LAN に対する脅威分析を実施したうえでセキュリティ要件を適切に策定し、情報セキュリティに関する各種機能（アクセス制御、識別コード、主体認証情報の付与、定期的な脆弱性情報の把握と対策、標的型攻撃対策及びログの取得、管理等）が有効に機能するようにすること。また、附属文書として、監視項目、定期保守項目、運用・保守業務フローなどの作業項目、作業内容、スケジュール、担当者等について記載すること。

ウ．本業務請負者は、運用計画及び保守計画の策定において、定常的に実施する脆弱性への対策として、以下に示す対応を記載すること。

（ア）調査

導入機器及びソフトウェアの一覧を整備するとともに、緊急性の高い脆弱性情報は随時、その他の脆弱性の情報は月次で調査すること。

（イ）評価

前項で把握した脆弱性に対し、第4次行政 LAN での発生可能性及び影響を評価し、その根拠とともに評価結果を担当職員に報告すること。その際、広く一般的に用いられている基準等の評価値を併せて報告すること。

（ウ）計画

脆弱性の評価値に基準を設定し、基準を超過した脆弱性に対しては、第4次行政 LAN に

おいて可能な防御策を確認の上、パッチの適用や設定変更等を行うよう計画し、担当職員に報告すること。

本業務請負者又は担当職員が、緊急性が高いと判断した脆弱性については、直ちにパッチの適用や設定の変更等を計画すること。なお、緊急性が高い脆弱性に対し、運用・保守担当及びセキュリティ担当が一体となって迅速に対応できるよう、運用・保守に係る業務の優先順位を整理するとともに、必要な体制を整備すること。

（エ）試験

第4次行政 LAN のサーバ及びネットワーク機器へのパッチの適用や設定変更に先立ち、検証環境を用いて試験を実施すること。検証環境は要件定義書「3.2.4 検証環境の設計・構築」に定める環境を整備すること。

本案件にて調達する端末や公用タブレット等については、担当職員が動作確認を実施する。担当職員が指定する端末に対し、先行してパッチの適用や設定の変更等を実施し、試験用端末として担当する職員等に提供すること。

（オ）導入

導入機器又はソフトウェアにパッチ適用や設定変更を行い、結果を担当職員に報告すること。業務や運用等に変更が発生する場合、手順書やマニュアル等の関連する資料を併せて修正すること。

エ. 本業務請負者は、運用計画及び保守計画の策定において、セキュリティインシデントを含む障害の発生に備え、以下に示す事項を記載すること。

（ア）体制

障害発生時において、運用チーム、保守チーム及び情報セキュリティチームを統括し、各担当者への指示、対応状況の把握、担当職員への報告や問い合わせに対応するリーダを置くこと。

（イ）役割

本業務請負者は、導入機器やソフトウェア等に対して必要な対策及び対策の実施に伴う業務への影響をとりまとめ、担当職員の確認を受けること。

オ. 本業務請負者は、運用設計及び保守設計に基づき、運用・保守業務の管理方法や手順、遵守事項等について定めた運用実施要領及び保守実施要領の案を作成し、担当職員の確認を受けること。

カ. 運用実施要領及び保守実施要領は、プロジェクト計画書の実施計画や運用計画及び保守計画における作業内容、スケジュール等との整合性を図った上で作成すること。また、運用業務及び保守業務を管理する上での具体的な方法等を示した運用手順書及び保守手順書、各種マニュアル、チェックリストも併せて作成すること。

キ. 運用計画及び保守計画には、以下の項目について記述すること。また、付属文書として作業項目、作業内容、スケジュールをより詳細に階層化し、担当者等を記載した WBS を作成すること。

（ア）作業概要

運用・保守の対象範囲、作業概要等について記載する。

（イ） 作業体制に関する事項

担当職員及び本業務請負者のみならず、運用・保守に関連する全ての関係者について、その体制、関係者間の関係性、役割分担・責務等について記載する。

（ウ） スケジュールに関する事項

作業内容、スケジュール、マイルストーン等について記載する。

（エ） 成果物に関する事項

運用・保守によって納品される成果物、品質基準、担当者、納入期限、納入方法、納入部数等について記載する。

（オ） 運用・保守形態、運用・保守手法、運用・保守環境、運用・保守ツール等

運用・保守において採用する運用・保守方法（オンサイト（常駐）、オンサイト（駆付け）、リモート、センドバック等）、運用・保守ツール等を必要に応じて記載する。

（3） 定常時対応

本システムの定常時対応に係る基本的な要件を以下に示す。

ア. 本業務請負者は、要件定義書（第5章 保守に関する要件）に示す、保守業務における定常時対応を行うこと。

イ. 本業務請負者は、要件定義書（第4章 運用支援に関する要件）に示す、運用業務における定常時対応を行うこと。その際必要に応じて、業務の一部を保守業務として保守チームが分担してもよい。

ウ. 保守業務及び運用業務の定常時における具体的な実施内容・手順は担当職員が定める運用計画及び保守計画に基づいて行うこと。

エ. 統合運用窓口は、行政 LAN（GSS が提供する機能含む）、解析 LAN、技術情報システム及びクローズド LAN 等の個別システムを利用する職員等及び LAN 担当者からの問い合わせを受け付け、所管する運用チームに連携すること。

オ. 本業務請負者は、情報システム室や他の課室が所管するシステムの機器更改や構成変更によって、行政 LAN の設定変更が必要な場合、各ネットワークシステム事業者と連携して対応すること。また、GSS の機器等に設定変更が必要な場合、GSS のヘルプデスクに依頼すること。

カ. 本業務請負者は、運用計画及び保守計画、運用実施要領、保守実施要領に基づき、保守業務及び運用業務の内容や工数などの作業実績状況（情報システムの脆弱性への対応状況や情報セキュリティ監視状況を含む。）、サービスレベルの達成状況、情報システムの定期点検状況、リスク・課題の把握・対応状況について月次で運用報告書及び保守報告書を取りまとめること。

キ. 本業務請負者は、月間の運用・保守実績を評価し、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。

ク. 本業務請負者は、月例の定期運用会議を開催し、運用報告書及び保守報告書の内容を報告すること。

（4） 障害発生時対応

本システムの異常時対応に係る基本的な要件を以下に示す。

ア. 本業務請負者は、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、自らの障害検知又は担当職員からの連絡を受け、その緊急度及び影響度を判断の上、要件定義書（第5章 保守に関する要件）に示す、保守業務における障害発生時対応を行うこと。

イ. 本業務請負者は、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、速やかに担当職員に報告するとともに、その緊急度及び影響度を判断の上、要件定義書に示す運用業務における障害発生時対応を行うこと。その際必要に応じて、業務の一部を保守業務として保守チームが分担してもよい。

ウ. 本業務請負者は、情報システムの障害が GSS に起因または GSS の機能に影響するおそれがある場合、担当職員に報告するとともに、GSS のヘルプデスクに連携すること。

エ. 保守業務、運用業務の障害発生時における具体的な実施内容や手順は担当職員が定める運用計画及び保守計画、運用実施要領、保守実施要領に基づいて行うこと。

オ. 本業務請負者は、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。

（5） 情報システムの現況確認支援

本システムの現況確認支援に係る基本的な要件を以下に示す。

ア. 受注者は、年1回以上、担当職員の指示に基づき、情報資産管理標準シート及び情報システム台帳と情報システムの現況との突合・確認を支援すること。

（6） 運用・保守の改善提案

本システムの運用業務及び保守業務の改善提案に係る基本的な要件を以下に示す。

ア. 本業務請負者は、年度末までに、年間の運用・保守実績を取りまとめるとともに、必要に応じて中長期運用・保守計画及び運用計画、保守計画、運用実施要領、保守実施要領に対する改善提案を行うこと。

イ. 本業務請負者は、セキュリティ環境の変化に合わせて、導入したセキュリティ対策製品のチューニングを実施すること。

ウ. 本業務請負者は、ア及びイの他に、担当職員が以下を例とする本システムの拡充や変更を求めた場合、計画を立案し、担当職員に確認を受けたうえで実施すること。

（ア） 本システムが利用するクラウドサービスの機能追加に併せた本システムの拡充

（イ）本システムの利用者機能、情報セキュリティ機能及び運用支援に関する機能の改善
（ウ）本庁舎の庁舎内のハードウェアやネットワークの変更

エ. 本業務請負者は、前項ウの対応に要する工数を3人月／年分確保すること。

オ. 本業務請負者は、担当職員が求める拡充又は変更が前項エの工数を超過する場合、担当職員と協議し、対応方針を決定すること。

カ. 本業務請負者は、担当職員が求める拡充又は変更が前項エの工数を満たさない場合、担当職員の依頼を受け、行政 LAN が具備する機能を用いた業務改善に資するアプリケーションを設計・構築すること。

キ. 要件定義書「4.2.3.2 セキュリティ障害対応」に示すフォレンジック分析等の作業について、担当職員と協議の上で、費用を前項エの工数に充当することを可能とする。

（7） 引継ぎ

本システムの引継ぎに係る基本的な要件を以下に示す。

ア. 本業務請負者は、担当職員が第5次更改を行う際には、第5次行政 LAN における調達支援業務請負者及び構築・保守業務請負者等に対し、作業経緯、残存課題等に関する情報提供及び質疑応答等の協力を行うこと。

（8） 情報資産管理標準シート及び情報システム台帳の更新に係る資料提出

本システムの情報資産管理標準シート及び情報システム台帳の更新に係る資料提出に係る基本的な要件を以下に示す。

ア. 受注者は、標準ガイドライン「別紙2 情報システムの経費区分」に基づき区分等した契約金額の内訳を記載した情報システム台帳の更新に係る資料を契約締結後速やかに提出すること。

イ. 受注者は、当委員会から求められた場合は、スケジュールや工数等の計画値及び実績値について記載した情報システム台帳の更新に係る資料を提出すること。

ウ. 受注者は、次に掲げる事項について記載した情報システム台帳の更新に係る資料を、運用実施要領及び保守実施要領において定める時期に、提出すること。

(ア)各データの変更管理

情報システムの運用・保守において、開発規模の管理、ハードウェアの管理、ソフトウェアの管理、回線の管理、外部サービスの管理、施設の管理、公開ドメインの管理、取扱情報の管理、情報セキュリティ要件の管理、指標の管理の各項目についてその内容に変更が生じる作業をしたときは、当該変更を行った項目

(イ)作業実績等の管理

情報システムの運用・保守中に取りまとめた作業実績、リスク、課題及び障害事由

４．３　プロジェクト管理に係る業務

本システムのプロジェクト管理に係る業務の基本的な要件を以下に示す。

ア．本業務請負者は「５．（４）作業の管理に関する要領」に記載されたプロジェクト管理業務を実施すること。

４．４　成果物

本業務の成果物、納品期日等を次の表に示す。

No	成果物名	納品期日	補足
1	設計・構築実施計画書	2025/4 下旬	
2	設計・構築実施要領	2025/4 下旬	
3	情報管理計画書	2025/4 上旬	
4	要件定義書（更新案）	2025/4 下旬	
5	設計書	2025/12 下旬	各ジョブネットのプログラム関連図や各スクリプトのフローチャート図といった詳細設計書、セキュリティ対策実装方式書も含む。なお、テストを実施した結果、設定等を変更した場合は、変更を反映した上で納品すること。
6	プロジェクト計画書（更新案）	2025/6 下旬	
7	プロジェクト管理要領（更新案）	2025/6 下旬	
8	構築標準、保守標準、運用標準	2025/6 下旬	
9	セキュリティルール	2025/6 下旬	
10	テスト計画書	2026/3 下旬	
11	単体テスト結果報告書	2026/2 下旬	
12	結合テスト結果報告書	2026/3 下旬	
13	総合テスト結果報告書	2026/4 下旬	
14	脆弱性診断結果報告書	2026/4 下旬	
15	テスト項目表、テスト手順書（テストシナリオ・スクリプト）、テストデータ、セキュリティ対策結果報告書	2026/5 下旬	受入テストのテスト項目表やテスト手順書も含む
16	移行計画書、移行ガイドライン、移行データ調査結果報告書	2026/5 下旬	
17	移行手順書、移行マニュアル、移行ツール、移行リハーサル計画書、移行リハーサル結果報告書	2026/5 下旬	
18	移行結果報告書	2026/7 上旬	
19	引継ぎ文書	2026/7 下旬	

No	成果物名	納品期日	補足
20	研修用資料（利用者マニュアル、統合窓口利用マニュアル、拠点運用マニュアル）	2026/5 下旬	
21	教育結果報告書	2026/6 下旬	
22	ライセンス関連情報 等	2026/7 下旬	
23	ソースコード	2026/7 下旬	
24	実行プログラム、マスタイメージ	2026/7 下旬	
25	ソフトウェア製品パッケージ	2026/7 下旬	
26	情報資産管理標準シート、情報システム台帳の更新に係る資料等	2026/7 下旬	外部機関からの照会に応じるため、更新が発生することがある
27	機器・役務リスト（案）	2026/9 下旬	
28	運用設計書	2025/12 下旬	
29	保守設計書	2025/12 下旬	
30	中長期運用・保守計画（案）	2025/12 下旬	
31	運用計画（案）	2025/12 下旬	
32	保守計画（案）	2025/12 下旬	
33	運用実施要領	2025/12 下旬	
34	保守実施要領	2025/12 下旬	
35	各種管理台帳（様式） 等	2025/12 下旬	
36	保守手順書、各種マニュアル、チェックリスト	2025/12 下旬	
37	運用手順書、各種マニュアル、チェックリスト	2025/12 下旬	
38	運用報告書（月次）	2026/8 以降（月次）	
39	保守報告書（月次）	2026/8 以降（月次）	
40	運用作業報告書	2026/8 以降（都度）	
41	保守作業報告書	2026/8 以降（都度）	
42	各種管理台帳等	2026/8 以降（都度）	
43	障害報告書	2026/8 以降（都度）	
44	運用報告書（年間）	2026/8 以降（毎年 3 月末）	
45	保守報告書（年間）	2026/8 以降（毎年 3 月末）	
46	情報管理計画書に基づく年次報告書	2026/8 以降（毎年 3 月末）	
47	中長期運用・保守計画（改善案）	2026/8 以降（毎年 3 月末）	
48	運用計画（改善案）	2026/8 以降（毎年 3 月末）	

No	成果物名	納品期日	補足
49	保守計画（改善案）	2026/8 以降 （毎年 3 月末）	
50	運用実施要領（改善案）	2026/8 以降 （毎年 3 月末）	
51	保守実施要領（改善案）	2026/8 以降 （毎年 3 月末）	
52	引継ぎ文書	2029/3 下旬	
53	棚卸し結果報告書	2026/8 以降 （毎年 6 月末、12 月末）	
54	ライセンス関連情報	都度	
55	ハードウェアとソフトウェアの関連図 等	都度	
56	マスタイメージ	都度	

成果物の納品方法

- 成果物は、全て日本語で作成すること。
- 用字・用語・記述符号の表記については、「公用文作成の要領（昭和 27 年 4 月 4 日内閣閣甲第 16 号内閣官房長官依命通知）」を参考にすること。
- 情報処理に関する用語の表記については、日本産業規格（JIS）の規定を参考にすること。
- 成果物は担当職員から特別に示す場合を除き、原則納品物を格納した電磁的記録媒体を 2 部納品すること。
- 電磁的記録媒体による納品について、ソースコード、実行プログラム以外は現行の原子力規制委員会ネットワークシステムが対応しているファイル形式（Microsoft Word、Microsoft Excel、Microsoft PowerPoint、で作成し、CD-R または DVD-R の媒体に格納して納品すること。
- ソースコード、実行プログラムについては、該当するソフトウェアの標準ファイル形式で作成し、CD-R または DVD-R の媒体に格納して納品すること。
- 構築期間中または運用期間中に納品する成果物は、ペーパーレス推進の観点から紙媒体を極力減らし電子データでの納品を可とする。ただし、会議で紙媒体を配布した方が明らかに有意であると考えられる等の場合は、適宜紙媒体を活用すること。
- 納品後担当職員において改変が可能となるよう、図表等の元データも併せて納品すること。
- 成果物の作成に当たって、特別なツールを使用する場合は、担当職員の承認を得ること。
- 成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。
- 電磁的記録媒体について、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。

成果物の納品場所

原則として、成果物は次の場所において引渡しを行うこと。ただし、担当職員が納品場所を別途指示する場合はこの限りではない。

〒106-8450
東京都港区六本木 1 丁目 9 番 9 号
原子力規制委員会原子力規制庁長官官房総務課情報システム室

５　作業の実施体制・方法

（1）作業実施体制

プロジェクトの推進体制及び本業務請負者の作業実施体制は次の図及び表のとおりである。なお、本業務請負者内のチーム編成については想定であり、受注決定後に協議の上、決定する。また、本業務請負者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。

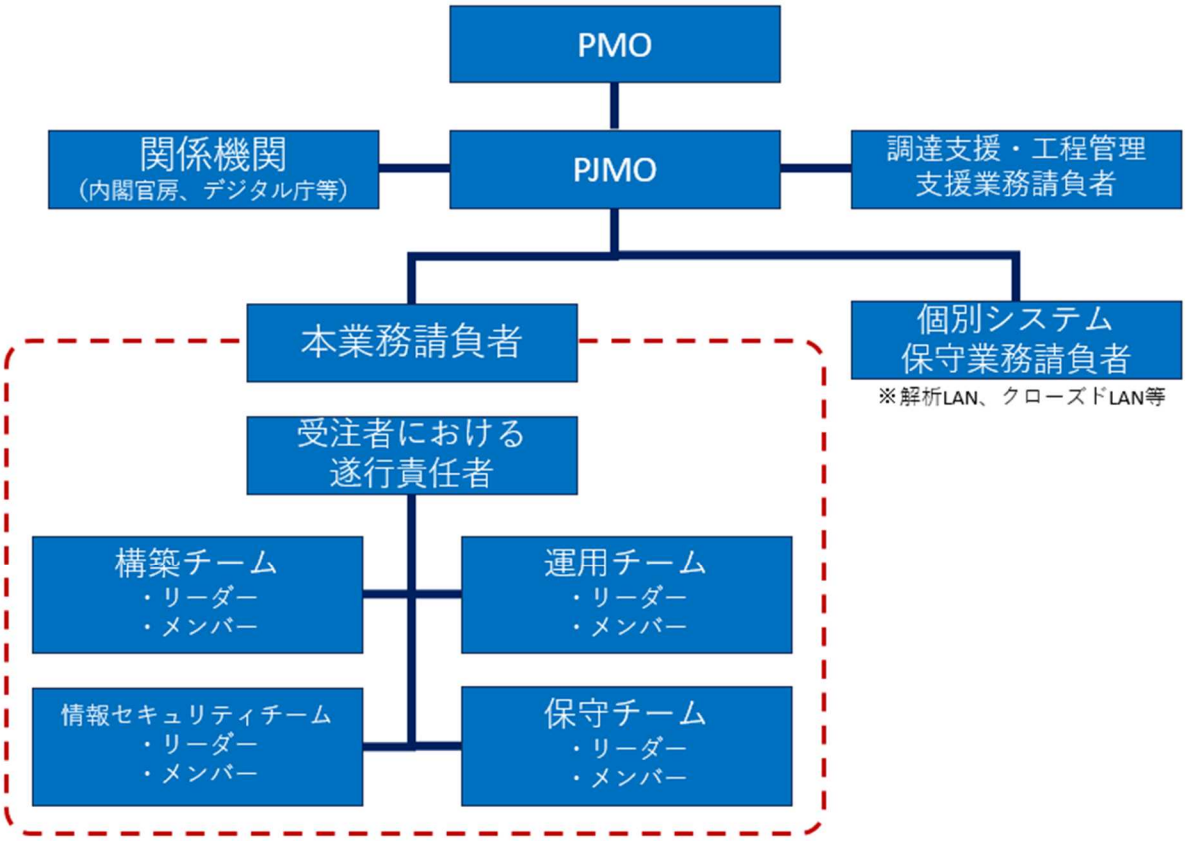

図 4 本業務の推進体制及び本業務請負者の作業実施体制

表 3 本業務における組織等の役割

No	組織又は要員	役割
1	本業務請負者における遂行責任者	本業務全体を統括し、必要な意思決定を行う。また、各関連する組織・部門とのコミュニケーション窓口を担う。 原則として全ての進捗会議及び品質評価会議に出席する。 本業務の構築期間中は専任でこれに当たるものとする。
2	構築チーム	第4次行政 LAN に関する設計・構築・テスト、受入テスト支援、移行、引き継ぎを担う。
3	構築チームリーダ	構築チーム内において作業状況の監視・監督を担うとともに、チーム間の調整を図る。 本業務の構築期間中は専任でこれに当たるものとする。
4	保守チーム	第4次行政 LAN に関するハードウェア保守、ソフトウェア保守を担う。
5	保守チームリーダ	保守チーム内において作業状況の監視・監督を担うとともに、チーム間の調整を図る。
6	運用チーム	行政 LAN に関するシステム運用を担う。
7	運用チームリーダ	運用チーム内において作業状況の監視・監督を担うとともに、チーム間の調整を図る。
8	情報セキュリティチーム	セキュリティ運用のうち、情報セキュリティ監視業務を担当する。運用業務に関与する要員とは独立して構成する。
9	情報セキュリティチームリーダ	情報セキュリティチーム内において作業状況の監視・監督を担うとともに、チーム間の調整を図る。
10	PJMO	プロジェクトを統括し、推進する立場から、設計・構築の各工程に関与し、設計・構築事業者の作業を管理する。
11	調達支援・工程管理支援業務請負者	プロジェクトの全部又は一部におけるプロジェクトの管理上生ずる作業について、PJMOの支援を行う。

（2） 作業要員に求める資格等の要件

本業務に参画する作業要員は、以下に示す資格等の要件を満たすこと。また、作業要員に求める資格等の要件に対応する、過去の業務経験を証明する資料や各資格試験の合格証を証跡として提出すること。

ア. 本業務請負者における遂行責任者は、本システムと同規模以上のネットワークシステムまたは類似システム（端末数 1,500 以上かつ拠点数 10 以上かつバックアップサイトを備えるシステム）の構築業務遂行責任者としての経験を有すること。また、EVM による進捗管理に精通し、活用経験を有すること。

イ. 本業務請負者における遂行責任者は、デジタル庁が整備する GSS または GSS を利用する府省庁システムの設計・構築または運用業務の経験を有することが望ましい。

ウ. 本業務請負者における遂行責任者は、情報処理の促進に関する法律（昭和 45 年 5 月 22 日法律第 90 号）に基づき実施される情報処理技術者試験のうちプロジェクトマネージャ試験の合格者又は Project Management Institute (PMI) が認定する PMP の資格を有すること。ただし、当該資格保有者等と同等の能力を有することが経歴等において明らかな者については、これを認める場合がある（その根拠を明確に示し、担当職員の理解を得ること。）。

エ. 構築チームのチームリーダは、本システムと同規模以上のネットワークシステムシステムまたは類似システム（端末数 1,500 以上かつ拠点数 10 以上かつバックアップサイトを備えるシステム）の構築プロジェクトにおいて構築業務のチームリーダとしての経験を有すること。

オ. 構築チームのチームリーダは、デジタル庁が整備する GSS または GSS を利用する府省庁システムの設計・構築の経験を有することが望ましい。

カ. 構築チームのチームリーダは、情報処理の促進に関する法律に基づき実施される情報処理技術者試験のうちプロジェクトマネージャ試験の合格者又は Project Management Institute (PMI) が認定する PMP の資格を有すること。ただし、当該資格保有者等と同等の能力を有することが経歴等において明らかな者については、これを認める場合がある（その根拠を明確に示し、担当職員の理解を得ること。）。

キ. 構築チームのメンバーは、次に掲げる試験の合格者又は資格保有者を1名以上含むこと。なお、同一人が全ての試験区分に合格していることを求めるものではない。また、これらの資格保有者等と同等の能力を有することが経歴等において明らかな者については、これを認める場合がある（その根拠を明確に示し、担当職員の理解を得ること。）。

（ア） 情報処理の促進に関する法律に基づき実施される情報処理技術者試験のうちネットワークスペシャリスト試験（または旧オンライン情報技術者試験、旧テクニカルエンジニア（ネットワーク）試験）

（イ） 情報処理の促進に関する法律に基づき実施される情報処理技術者試験のうち情報処理安全確保支援士（登録セキスペ）試験（または情報セキュリティスペシャリスト試験、旧テクニカルエ

ンジニア（情報セキュリティ）試験、旧情報セキュリティアドミニストレータ試験）、または ISACA が認定する公認情報セキュリティマネージャー（CISM）、または国際情報システムズセキュリティ認証コンソーシアムが認定する情報システムのセキュリティ専門家認定 （CISSP）

（ウ）情報処理の促進に関する法律に基づき実施される情報処理技術者試験のうちシステムアーキテクト試験（または旧特種情報技術者試験、旧アプリケーションエンジニア試験）

ク. 運用チームのチームリーダは、本システムと同規模以上の情報システム（端末数 1,500 以上かつ拠点数 10 以上かつバックアップサイトを備えるシステム）のシステム運用業務においてリーダとしての経験を 2 年以上有すること。

ケ. 運用チームのチームリーダは、デジタル庁が整備する GSS のシステム運用業務または GSS を利用する府省庁のシステム運用業務においての経験を有することが望ましい。

コ. 運用チームのチームリーダは、次に掲げるいずれかの試験の合格者又は資格保有者であること。ただし、これらの資格保有者等と同等の能力を有することが経歴等において明らかな者については、これを認める場合がある（その根拠を明確に示し、担当職員の理解を得ること。）。

（ア）情報処理の促進に関する法律に基づき実施される情報処理技術者試験のうち IT サービスマネージャ試験（または旧システム運用管理エンジニア試験、旧テクニカルエンジニア（システム管理）試験）

（イ）情報処理の促進に関する法律に基づき実施される情報処理技術者試験のうち情報処理安全確保支援士（登録セキスペ）試験（または情報セキュリティスペシャリスト試験、旧テクニカルエンジニア（情報セキュリティ）試験、旧情報セキュリティアドミニストレータ試験）、または ISACA が認定する公認情報セキュリティマネージャー（CISM）、または国際情報システムズセキュリティ認証コンソーシアムが認定する情報システムのセキュリティ専門家認定 （CISSP）

（ウ）情報処理の促進に関する法律に基づき実施される情報処理技術者試験のうちネットワークスペシャリスト試験（または旧オンライン情報技術者試験、旧テクニカルエンジニア（ネットワーク）試験）

（エ）ITIL 資格認定機関が認定する ITIL 認定のうちエキスパートまたはマスター

サ. 運用チームは、次の全ての試験の合格者又は資格保有者を 1 名以上擁すること。ただし、これらの資格保有者等と同等の能力を有することが経歴等において明らかな者については、これを認める場合がある（その根拠を明確に示し、担当職員の理解を得ること。）。

（ア）情報処理の促進に関する法律に基づき実施される情報処理技術者試験のうちネットワークスペシャリスト試験（または旧オンライン情報技術者試験、旧テクニカルエンジニア（ネットワーク）試験）又はシスコシステムズが認定する Cisco Certified Network Professional（CCNP）

（イ）情報処理の促進に関する法律に基づき実施される情報処理技術者試験のうち情報処理安全確保支援士（登録セキスペ）試験（または情報セキュリティスペシャリスト試験、旧テクニカルエンジニア（情報セキュリティ）試験、旧情報セキュリティアドミニストレータ試験）、または国際情報システムズセキュリティ認証コンソーシアムが認定する情報システムのセキュリティ専門家認定 （CISSP）

シ. 運用チームは、以下の全ての技術分野について、1 年以上の業務経験及び専門知識を有する者を 1 名以上擁すること。

（ア）Windows クライアント OS、Windows サーバ OS

（イ）サーバ用途 Linux ディストリビューション（Red Hat Enterprise Linux 等）

（ウ）サーバ仮想化製品（VMware vSphere 等）

（エ）業務向けデータベース製品（PostgreSQL、Oracle Database 等）

（オ）Active Directory、 DNS 等のインフラ系サーバ（Windows、 Linux）

（カ）ネットワーク機器全般

ス. 情報セキュリティチームのメンバーは、セキュリティ全般に精通し、サイバー攻撃に対する監視、分析、評価、対策立案といった一連の業務経験を 3 年以上有する者を1名以上含むこと。

（3） 作業場所

本業務の作業場所は以下とする。

ア. 本業務の作業場所及び作業に当たり必要となる設備、備品及び消耗品等については、本業務請負者の責任において用意すること。また、必要に応じて担当職員が現地確認を実施することができるものとする。

イ. 運用業務については担当職員が貸与する執務室を利用すること。なお、リモートで対応する場合はこの限りではない。

（4） 作業の管理に関する要領

本業務における作業の管理に関する要領は以下とする。

ア. 本業務請負者は、担当職員が承認した設計・構築実施要領に基づき、設計・構築業務に係るコミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

イ. 本業務請負者は工程管理において、当初定めたスケジュール内に完了するために適切なマイルストーン（チェックポイント）を定め、マイルストーンから逆算した各タスクの期間設定及び完了条件を定めておくこと。更に、スケジュールが遅延した場合に備え、常にコンティンジェンシープランを検討すること。

ウ. 本業務請負者は、リスク管理において下流工程で起こり得るリスクについても検討し、リスク低減に向けた検討・確認ポイントを明確にしたうえで担当職員へ報告すること。

エ. 本業務請負者は、変更管理（仕様管理）を適切に行うべく、プロジェクト計画書、要件定義書、調達仕様書の各要件に対して、実現箇所、実現方法等を追跡・管理するために、要件をトレース管理する仕組みを導入すること。

オ. 本業務請負者は、担当職員が承認した運用実施要領及び保守実施要領に基づき、保守業務、運

用業務に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

カ. 本業務請負者は、保守業務及び運用業務の実施にあたり、サービスレベルの維持管理を目的とし、システム運用状況の確認と問題点共有及び解決策の検討を実施するために、月次報告会を実施すること。報告会に係る要件は以下の通り。

（ア）月次報告書を作成し、業務報告会を開催すること。

（イ）主な報告内容は、業務実績総括（サービスデスク実施、システム運用管理）、サービスデスク実施詳細（問合せ状況、機器管理状況、等）、システム運用管理業務詳細（対応状況、サーバリソース集計、ウイルス検出集計、セキュリティパッチ適用状況、内部ファイアウォール確認状況、回線帯域の使用状況、等）、サービスレベル達成状況、イベント予定等とする。

（ウ）具体的な報告内容や様式、効率的な会議運営を行うための報告方法について提案すること。（前月分の作業項目別、要員別の作業実績時間の添付を必須とする。）

（エ）作業報告書が必要な業務に関しては作業実施後に報告書を作成の上、担当官へ報告すること。

キ. 本業務請負者は、保守業務及び運用業務の実施にあたり、以下に示す情報共有・連絡方法を確立すること。

（ア）本業務請負者は、担当職員への資料の提出や連絡票の授受及び課題事項やその回答等について、一元的に管理し、関係者との間で円滑な情報共有を図ること。

（イ）本業務請負者は、提出書類、会議議事録及び取り交わした情報を担当官の求めに応じて適宜提示すること。

（ウ）本書に定める運用管理業務の実施に当たっては、全てにおいてその実施事項に関する作業項目とスケジュールを明らかにし、担当官に提出すること。

（エ）作業スケジュール作成にあたっては月間及び年間を通じた観点で担当職員がその全体を把握できるように工夫すること。

（オ）サーバに管理される資料や実施事項管理で作成するスケジュールや連絡事項等については、プロジェクトメンバ全員で共有し、タスクの効率的な実行、必要な連携の徹底を図ること。

6　作業の実施に当たっての遵守事項

（1）機密保持、資料の取扱い

ア. 本業務請負者は、本業務に係る情報の取扱いにおいて、「4．4　成果物」「情報管理計画書」に具体的な取り扱い内容を記し提出すること。なお、以下の要件を満たすこと。

（ア）原子力規制庁から本業務の実施に係る要機密情報を提供された場合には、当該情報の機密性の格付けに応じて適切に取り扱うための措置を講じ、担当職員の了承を得ること。また、提供された要機密情報は、本業務以外の目的で利用しないこと。

なお、「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5年度版）」のうち、情報の格付けについて機密性2情報に該当する。

（イ）本業務の実施において作成する情報についても同様に、当該情報の機密性の格付けに応じて適切に取り扱うための措置を講じ、担当職員の了承を得ること。また、作成した要機密情報は、本業務以外の目的で利用しないこと。

（ウ）原子力規制庁から提供された要機密情報が本業務の終了等により不要になった場合には、確実に返却し又は廃棄すること。返却または廃棄方法については担当職員の了承を得ること、本業務において作成した情報の廃棄方法についても、担当職員の了承を得て適切に廃棄すること。

（エ）本業務の実施において知り得た情報を第三者へ開示や漏えいをしないこと。

（2）個人情報の取扱い

ア. 個人情報の取扱いに係る事項について担当職員と協議の上決定し、書面「4．4　成果物」「情報管理計画書」にて提出すること。なお、以下の事項を記載すること。

（ア）個人情報取扱責任者が情報管理責任者と異なる場合には、個人情報取扱責任者等の管理体制

（イ）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）

イ. 本業務の作業を派遣労働者に行わせる場合は、労働者派遣契約書に秘密保持義務など個人情報の適正な取扱いに関する事項を明記し、作業実施前に教育を実施し、認識を徹底させること。なお、本業務請負者はその旨を証明する書類を提出し、担当職員の了承を得たうえで実施すること。

ウ. 個人情報を複製する際には、事前に担当職員の許可を得ること。なお、複製の実施は必要最小限とし、複製が不要となり次第、その内容が絶対に復元できないように破棄・消去を実施すること。なお、本業務請負者は廃棄作業が適切に行われた事を確認し、その保証をすること。

エ. 本業務請負者は、本業務を履行する上で個人情報（生存する個人に関する情報であって、当該情報に含まれる氏名、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こととなるものを含む。）をいう。以下同じ。）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、直ちに被害の拡大を防止等のため必要な措置を講ずるとともに、担当職員に事案が発生した旨、被害状況、復旧等の措置及び本人への対応等について直ちに報告すること。

オ. 個人情報の取扱いにおいて適正な取扱いが行われなかった場合は、本業務の契約解除の措置を受けるものとする。

（3）法令等の遵守

ア. 当該調達案件の業務遂行に当たっては、法令等を遵守し履行すること。

イ. 環境省においては、率先して温室効果ガス削減その他の環境負荷の低減、資源の消費量の削減を含む3Rの取組の推進等、環境省の環境方針を定めており、本調達においても「より環境にやさしいネットワークシステム」を調達の基本としている。したがって、可能な限り環境への負荷（「環境

基本法」（平成5年法律第 91 号）第2条第1項に規定する環境への負荷をいう。以下同じ。）を軽減したものであることを基本要件とする。

ウ. 物品の調達に当たっては、環境への負荷の低減に資する原材料又は部品を使用していること、使用に伴い排出される温室効果ガス等による環境負荷が少ないこと、使用後にその全部又は一部の再利用又は再生利用がしやすいことにより廃棄物の発生を抑制することができることその他の事由により、より環境への負荷の低減に資する製品を調達する。

エ. 納入成果物のうち、「令和5年環境物品等の調達の推進を図るための方針」に掲げる特定調達物品等に該当するものは、「環境物品等の調達の推進に関する基本方針」令和5年 12 月 22 日変更閣議決定。以下「基本方針」という。）の判断の基準を満たすこと。その他の納入成果物についても可能な限り基本方針の判断の基準を満たすものを導入すること。

オ. 本業務の履行に当たっては、「障害を理由とする差別の推進に関する法律（平成 25 年法律第 65 号）第 9 条第 1 項」に基づく「原子力規制委員会における障害を理由とする差別の解消の推進に関する対応要領第 3 条」に規定する合理的配慮について配慮すること。

（4） 標準ガイドラインの遵守

本業務の遂行に当たっては、標準ガイドラインに基づき、作業を行うこと。具体的な作業内容及び手順等については、「デジタル・ガバメント推進標準ガイドライン解説書」（以下「解説書」）を参考とすること。なお、「標準ガイドライン」及び「解説書」が改定された場合は、最新のものを参照し、その内容に従うこと。

（5） その他文書、標準への準拠

ア. プロジェクト計画書

当該調達案件の業務遂行に当たっては、担当職員が定めるプロジェクト計画書との整合を確保して行うこと。

イ. プロジェクト管理要領

当該調達案件の業務の管理に当たっては、担当職員が定めるプロジェクト管理要領との整合を確保して行うこと。

ウ. プロジェクト標準

構築に当たっては、「4．1 （3）構築・テスト」にて定める構築標準、運用標準、保守標準に準拠して作業を行うこと。

エ. 原子力規制委員会情報セキュリティポリシー

当該調達案件におけるセキュリティ対策実施に当たっては、原子力規制委員会情報セキュリティポリシーに準拠すること。

オ. その他

本業務請負者は、以下に示す文書、ガイドライン等にも準拠して、各種作業を進めること。

（ア） IT 製品の調達におけるセキュリティ要件リスト

（イ） IT 製品におけるセキュリティ要件リストガイドブック

（ウ）電子政府推奨暗号リスト
（エ）高度標的型攻撃』対策に向けたシステム設計ガイド
（オ）情報システム安全対策基準

（6）規程等の説明等

本業務請負者は、原子力規制委員会情報セキュリティポリシー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。

なお、原子力規制委員会情報セキュリティポリシーは、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（以下「統一基準群」という。）に準拠することとされていることから、受託者は、統一基準群の改定を踏まえて規則が改正された場合には、本業務に関する影響分析を行うこと。

（7）情報システム監査

ア. 本調達において整備又は管理を行う情報システムに伴うリスクとその対応状況を客観的に評価するために、担当職員が情報システム監査の実施を必要と判断した場合は、担当職員が定めた実施内容（監査内容、対象範囲、実施者等）に基づく情報システム監査を本業務請負者は受け入れること （担当職員が別途選定した事業者による監査を含む）。

イ. 情報システム監査で問題点の指摘又は改善案の提示を受けた場合には、対応案を担当部署と協議し、指示された期間までに是正を図ること。

（8）セキュリティ要件

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に基づき、以下の内容について対応すること。

ア. 本業務請負者は、本業務の開始時に本業務に係る「情報セキュリティ対策とその実施方法及び管理体制」について、担当職員に書面「4．4　成果物」「情報管理計画書」で提出すること。

イ. 本業務請負者はサプライチェーン・リスク対策として、以下の要件を満たすこと。

（ア）情報システムの構築業務において、当庁の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。

（イ）情報システムに当庁の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、担当職員と本業務請負者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

（ウ）本業務請負者の資本関係、役員等の情報、作業要員の氏名、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、国籍等の情報が把握できること。

（エ）本業務において導入する機器等の機器・役務リストを提出すること。提出された機器・役務リストについて、原子力規制庁担当官がサプライチェーン・リスクに係る懸念が払拭されないと

判断した場合には、当該リスクに対応するため、代替品又はリスク低減対策の提出を求めることがあるので留意すること。なお、機器リストの機器等を変更する場合には、事前に担当職員の承認を得ること。

ウ. 本業務請負者は情報セキュリティ対策の実施において、以下の要件を満たすこと。

（ア）情報セキュリティ対策は、原子力規制委員会情報セキュリティポリシーおよび本調達仕様書、要件定義書に記載されたセキュリティに係る要件を満たすこと。

（イ）情報セキュリティ対策その他の契約の履行状況について「情報管理計画書」に基づき、担当職員に年次で報告すること。

（ウ）本業務請負者の責により情報セキュリティインシデントが発生した場合は、原因分析及び対処方法を担当職員に報告し、承認を得ること。また、インシデントの発生に伴い損害が発生した場合は、本業務請負者の責任において賠償すること。

（エ）本業務に係る情報セキュリティインシデントが発生した場合や情報セキュリティ対策の履行が不十分と見なされる場合は、必要に応じて当庁が行う情報セキュリティ対策に関する監査を受け入れること。

（オ）当庁がセキュリティ対策の履行が不十分であると判断した場合には、改善策を検討し、担当職員と協議の上、実施すること。

エ. 本業務請負者は、情報システムの構築に係るセキュリティ要件として、以下を満たすこと。

（ア）原子力規制委員会情報セキュリティポリシーおよび本調達仕様書、要件定義書に記載されたセキュリティに係る要件をすべて満たすシステムを構築すること。

（イ）ソフトウェアの開発を行う場合は（独）情報処理推進機構の次の情報を参照し、情報セキュリティ対策を実施すること。「セキュリティエンジニアリング−ソフトウェア開発者向けのページ」
https://warp.ndl.go.jp/info:ndljp/pid/3509096/www.ipa.go.jp/security/awareness/vendor/software.html

（ウ）「セキュリティ対策実装方針書」に以下を実施することを記載のうえ、担当職員に提出し、承認を得ること。また、構築においては、セキュリティ実装方針に従うこと。

- 情報システムのセキュリティ要件の適切な実装
- 情報セキュリティの観点に基づく試験の実施
- 情報システムの開発環境及び開発工程における情報セキュリティ対策

（エ）情報システムに対する脅威分析を行い、担当職員に分析結果を報告し、承認を得ること。また、必要なセキュリティ対策を洗い出した上でセキュリティ設計を行うこと。

（オ）セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビュー及びソースコードレビューの範囲及び方法を定め、これに基づいてレビューを実施すること。

（カ）ソースコードが不正に変更されることを防ぐために、以下の事項を含むソースコードの管理を適切に行うこと。

・　ソースコードの変更管理
・　ソースコードの閲覧制限のためのアクセス制御
・　ソースコードの滅失、き損等に備えたバックアップの取得

（キ）情報セキュリティの観点から、以下を踏まえた試験を実施し、担当職員に報告すること。
・　情報セキュリティの観点から運用中の情報システムに悪影響が及ばないように、運用中の情報システムと分離すること。
・　情報セキュリティの観点から必要な試験がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施すること。なお、試験にあたり GSS 側で対応が必要な場合、デジタル庁と協議すること。
・　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。

（ク）本業務における情報システムの構築が完了し運用を開始する前に、本業務請負者の品質管理責任者による品質報告およびセキュリティ報告を実施すること。なお、セキュリティ報告には、脆弱性診断等の安全点検の結果を添付するとともに、不備が指摘された場合は、運用開始までに適切な対処を実施すること。

（ケ）情報システムの受入れ時において、以下の要件が満たされていることを担当職員へ報告し、承認を得ること。
・　調達時に指定したセキュリティ要件の実装状況を確認すること。
・　ソフトウェア等に不正プログラムが混入していないこと。

オ．本業務請負者は、情報システムに関する脆弱性への対策として、以下を含む対策を実施し、本業務の終了時に「情報セキュリティ対策結果報告書」として実施結果を記載の上、担当職員に報告し、承認を得ること。

（ア）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。

（イ）構築時に情報システムに脆弱性が混入されることを防ぐためのセキュリティ実装方針を策定し、「セキュリティ対策実装方針書」に記載の上、担当職員へ報告し、承認を得ること。

（ウ）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、担当職員へ報告し、修正を施すこと。

（エ）サーバ装置、端末及び通信回線装置の設置又は外部からアクセス可能なインターネットへの接続開始前及び運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。

（オ）クラウドサービスを利用する場合、構築段階からアクセス制御を行うなど、セキュリティ対策を早期に適用すること。

（カ）情報システムを構成するソフトウェアの脆弱性に関して、以下を含む情報を適宜入手し、担当職員へ報告すること。
・　脆弱性の原因
・　影響範囲

・　対策方法
・　脆弱性を悪用する不正プログラムの流通状況

（キ）利用するソフトウェアはサポート期間を考慮して選定し、サポート期間を過ぎたソフトウェアは原則として利用しないこと。

（ク）構成要素ごとにソフトウェアのバージョン等を把握し、脆弱性対策の状況を確認すること。

（ケ）脆弱性対策を実施する場合には、実施日、実施内容及び実施者を含む「作業記録」を取得し、適切に保管すること。

（コ）セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイルは、信頼できる方法で入手すること。

（サ）多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

（シ）本業務請負者は、通信回線を経由して保守作業等を行う際には、送受信される情報が漏えいすることがないような接続を行うこと。

カ. 情報セキュリティ対策の完了後 1 年以内に契約不適合による情報セキュリティ対策の不備が発見された場合には、本業務請負者は無償で速やかに必要な措置を講ずること。

キ. 本業務請負者は、情報システムの運用及び保守に係るセキュリティ要件として、以下を満たすこと。

（ア）運用計画及び保守計画には以下も含めること。また、運用計画及び保守計画に則り、情報システムに実装されたセキュリティ機能を適切に活用すること。
・　情報システムの運用環境に課せられるべき条件の整備
・　情報システムの保守における情報セキュリティ対策
・　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

（イ）運用計画及び保守計画の策定にあたって、情報システム全体のセキュリティ水準が低下することのないように、セキュリティ要件を適切に策定し、情報セキュリティに関する各種機能（アクセス制御、識別コード、主体認証情報の付与、定期的な脆弱性情報の把握と対策、標的型攻撃対策及びログの取得、管理等）が有効に機能するようにすること。また、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定すること。

（ウ）暗号化及び電子署名に使用するアルゴリズムが危殆化した場合を想定した緊急対応手順や、暗号化された情報の複合または電子署名の付与に用いる鍵についての管理手順、ソフトウェアを変更する際の許可申請手順を運用手順書・保守手順書に記載すること。

（エ）運用手順書・保守手順書の付属文書として、監視項目、定期保守項目、運用・保守業務フロー等の作業項目、作業内容、スケジュール担当者等について記載すること。

ク. 本業務請負者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の「措置の実施方法」を検討し、担当職員へ報告のうえ承認を得ること。また、作業完了時には、「作業完了届」を作成し、担当職員へ提出すること。

（ア）情報システム更改時の情報の移行作業における情報セキュリティ対策
（イ）情報システム廃棄時の不要な情報の抹消

7　成果物の取扱いに関する事項

ア．成果物の取扱いに関する事項

（ア）知的財産権の帰属本業務における成果物の原著作権及び二次的著作物の著作権（著作権法第 21 条から第 28 条に定める全ての権利を含む。）は、本業務請負者が本調達の実施の従前から権利を保有していた等の明確な理由によりあらかじめ提案書にて権利譲渡不可能と示されたもの以外は、全て原子力規制委員会に帰属するものとする。

（イ）原子力規制委員会は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改変等し、及びそれらの利用を第三者に許諾することができるとともに、任意に開示できるものとする。また、本業務請負者は、成果物について、自由に複製し、改変等し、及びこれらの利用を第三者に許諾すること（以下「複製等」という。）ができるものとする。ただし、成果物に第三者の権利が帰属するときや、複製等により当庁がその業務を遂行する上で支障が生じるおそれがある旨を契約締結時までに通知したときは、この限りでないものとし、この場合には、複製等ができる範囲やその方法等について協議するものとする。

（ウ）本件プログラムに関する権利（著作権法第 21 条から第 28 条に定める全ての権利を含む。）及び成果物の所有権は、原子力規制委員会から本業務請負者に対価が完済されたとき本業務請負者から原子力規制委員会に移転するものとする。

（エ）納品される成果物に第三者が権利を有する著作物（以下「既存著作物等」という。）が含まれる場合には、本業務請負者は、当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、本業務請負者は、当該既存著作物の内容について事前に当庁の承認を得ることとし、当庁は、既存著作物等について当該許諾条件の範囲で使用するものとする。

（オ）本業務請負者は原子力規制委員会に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。

イ．契約不適合責任

（ア）本業務における成果物等について、種類、品質又は数量が契約書、本調達仕様書その他合意された要件（以下「契約書等」という。）の内容に適合しないもの（以下「不適合」という。）である場合、その不適合が原子力規制庁の責に帰すべき事由による場合を除き、本業務請負者は、自己の費用で、当庁の選択に従い、その修補、代替物の引渡し又は不足分の引渡しによる履行の追完（以下、手段を問わず総称して「履行の追完」という。）をすること。なお、本業務請負者は如何なる場合であっても、当庁の選択と異なる方法で履行の追完をする場合は、当庁の事前の承諾を受けること。

（イ）本業務請負者は、その具体的な履行の追完の実施方法、完了時期、実施により発生する諸制限事項について、当庁と協議し、承諾を得てから履行の追完を実施するものとし、完了時には、その結果について当庁の承諾を受けること。

（ウ）本業務請負者が当庁から相当の期間を定めた履行の追完の催告を受けたにもかかわらず、その期限内に履行の追完を実施しない場合、当庁は、その不適合の程度に応じて代金の減額を請求することができる。ただし、次に掲げる場合、本業務請負者に対して履行の追完の催告なく、直ちに代金の減額を請求することができる。

（エ）履行の追完が不能であるとき。

（オ）本業務請負者が履行の追完を拒絶する意思を明確に表示したとき。

（カ）本業務の性質又は契約書等の内容により、特定の日時又は一定の期間内に履行をしなければ契約をした目的を達することができない場合において、本業務請負者が履行の追完をしないでその時期を経過したとき。

（キ）前 3 号に掲げる場合のほか、前項の催告をしても履行の追完を受ける見込みがないことが明らかであるとき。

ウ. 検収

（ア）本業務請負者は、成果物等について、納品期日までに担当職員に内容の説明を実施して検収を受けること。

（イ）検収の結果、成果物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について担当職員に説明を行った上で、指定された日時までに再度納品すること。

8　入札参加資格に関する事項

（1）競争参加資格

ア. 予算決算及び会計令第 70 条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。

イ. 予算決算及び会計令第 71 条の規定に該当しない者であること。

ウ. 原子力規制委員会から指名停止措置が講じられている期間中の者ではないこと。

エ. 令和04・05・06年度環境省競争参加資格（全省庁統一資格）の「物品の販売」及び「役務の提供等」において、入札時までに「A」、「B」、「C」、又は「D」の等級に格付けされ、競争参加資格を有する者であること。「役務の提供等」の営業品目「ソフトウェア開発」、「情報処理」又は「その他」に登録している者であること。）。なお、令和07・08・09年度の資格を引き続き取得すること。

オ. 入札説明書において示す暴力団排除に関する誓約事項に誓約できる者であること。

（2）公的な資格や認証等の取得

ア. 本調達仕様書に基づく作業を実施する部門又は組織を対象として、JIS Q 27001(又は ISO27001)を基準とした認証を取得していること。

イ. 本調達仕様書に基づく作業を実施する部門又は組織を対象として、JIS Q 15001 を基準としたプライバシーマーク認証を取得していること。

ウ. 本調達仕様書に基づく作業を実施する部門又は組織を対象として、ISO 9001 を基準とした認証を取得していること。

エ. 女性の職業生活における活躍の推進に関する法律(以下「女性活躍推進法」という。)、次世代育成支援対策推進法(以下「次世代法」という。)、青少年の雇用の促進等に関する法律(以下「若者雇用推進法」という。)に基づく認定等(えるぼし認定等、くるみん認定等、ユースエール認定)を取得している場合は、認定等の名称及び認定通知書等の写しを提出すること。ただし、提案書提出時点において認定等の期間中であること。

(3) 受注実績

ア. 応札者は、端末数 2,500 以上かつ拠点数 10 以上かつバックアップサイトを備えるネットワークを構築した実績を有すること。

イ. 応札者は、2,500 名以上の職員が利用し、かつクラウドサービスを利用する情報システムの設計・構築・運用・保守を行った実績を有すること。

(4) 複数事業者による共同入札

ア. 複数の事業者が共同入札する場合、その中から全体の意思決定、運営管理等に責任を持つ共同入札の代表者を定めるとともに、本代表者が本調達に対する入札を行うこと。

イ. 共同入札を構成する事業者間においては、その結成、運営等について協定を締結し、業務の遂行に当たっては、代表者を中心に、各事業者が協力して行うこと。事業者間の調整事項、トラブル等の発生に際しては、その当事者となる当該事業者間で解決すること。また、解散後の契約不適合責任に関しても協定の内容に含めること。

ウ. 共同入札を構成する全ての事業者は、本入札への単独提案又は他の共同入札への参加を行っていないこと。

エ. 共同入札を構成する全ての事業者は、 競争参加資格及び公的な資格や認証等の取得を満たすこと。

(5) 入札制限

「令和6～8年度第4次原子力規制委員会ネットワークシステムの調達支援及び工程管理等支援業務」の受注事業者(再委託先等を含む。)及びこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」(昭和 38 年 11 月 27 日大蔵省令第 59 号)第 8 条に規定する親会社及び子会社、同一の親会社を持つ会社並びに委託先事業者等の緊密な利害関係を有する事業者は、入札には参加できない。

9　再委託に関する事項

(1) 再委託の制限及び再委託を認める場合の条件

ア. 本業務請負者は、業務を一括して又は主たる部分「4. 3プロジェクト管理に係る業務」を再委託してはならない。

イ. 本業務請負者における遂行責任者を再委託先事業者の社員や契約社員とすることはできない。

ウ. 本業務請負者は、再委託先の行為について一切の責任を負うものとする。

エ. 「9.（2）再委託先に係るセキュリティ対策」に示す情報セキュリティの確保については本業務請負者の責任とする。

オ. 本業務請負者は、再委託先に情報セキュリティ対策の履行状況を定期的に確認し、報告すること。

カ. 再委託を行う場合、再委託先が「8.（5）入札制限」に示す要件を満たすこと。

(2) 再委託先に係るセキュリティ対策

ア. 本業務請負者は、再委託においても本業務請負者と同等の情報セキュリティが確保されるよう、以下に記載する事項を再委託先に求めること。なお、再委託の相手方が更に委託を行うなど複数の段階で再委託が行われる場合（以下「再々委託」という。）も同様とする。

- 当委員会から提供する情報の目的外利用の禁止
- 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
- 情報セキュリティインシデントへの対処方法
- 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
- 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
- 当委員会による監査の受け入れ

イ. 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委員会に提供すること。

(3) 承認手続

ア. 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委託する場合には、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額等について記載した、様式1「再委託承認申請書」を当庁に提出し、あらかじめ承認を受けること。なお、必要に応じて従事者の情報を追加で求めることがある。

イ. 再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面を当庁に提出し、承認を受けること。

ウ. 再々委託する場合、当該再々委託の相手方の商号又は名称及び住所並びに再々委託を行う業務の範囲を書面で報告すること。

(4) 再委託先の契約違反等

再委託先において、本調達仕様書の遵守事項に定める事項に関する義務違反又は義務を怠った場合

には、本業務請負者が一切の責任を負うとともに、当庁は、当該再委託先への再委託の中止を請求することができる。

10 その他特記事項

（1） 前提条件等

ア. 本件は、令和7年度の予算成立を条件とする。契約締結日は、本業務に係る令和7年度予算（暫定予算を含む。）が成立した日以降とする。また、暫定予算になった場合、全体の契約期間に対する暫定予算の期間分のみの契約とする場合がある。

イ. 令和8年1月から8年3月の期間は、当庁の繁忙期に当たるため、担当職員のプロジェクトへの関与が十分にできなくなる恐れがあることに留意すること。

ウ. 入札参加前にサプライチェーン・リスクに係る確認のため、提案書の提出期限までに、機器・役務リスト（案）を提出すること。なお、提出された機器・役務リスト（案）について、担当職員がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、当該リスクに対応するため、代替品又はリスク低減対策の提出を求めることがあるので、速やかに応じること。

エ. 本件受注後に調達仕様書（要件定義書を含む。）の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもって当庁に申し入れを行うこと。双方の協議において、その変更内容が軽微（委託料、納期に影響を及ぼさない）かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が記名捺印することによって変更を確定する。

オ. 本調達の入札者は、支出負担行為担当者が別に指定する暴力団等に該当しない旨の誓約書を提出すること。入札に参加した者が、誓約書を提出せず、または虚偽の誓約をし、もしくは誓約書に反することとなったときは、当該者の入札を無効とする。

（2） 入札公告期間中の資料閲覧等

本業務の実施に参考となる過去の類似業務の報告書等に関する資料については、原子力規制庁内にて閲覧可能とする。なお、資料の閲覧に当たっては、必ず事前に担当部署まで連絡の上、閲覧日時を調整すること。

ア. 閲覧場所：原子力規制委員会原子力規制庁長官官房総務課情報システム室

イ. 閲覧期間及び時間：令和7年●月●日～同●月●日 10 時～17 時（12 時から 13 時を除く。）

ウ. 閲覧手続：閲覧希望者は下記の連絡先に連絡し、「閲覧申込書」及び「守秘義務に関する誓約書」を入手する。閲覧希望日の3営業日前までに、閲覧希望者の商号、連絡先、閲覧希望者氏名を記載した「閲覧申込書」を提出すること。また、閲覧日当日までに「守秘義務に関する誓約書」を提出すること。

エ. 閲覧時の注意：最大5名まで。閲覧にて知り得た内容については、提案書の作成以外には使用しないこと。また、本調達に関与しない者等に情報が漏えいしないように留意すること。原子力規制庁のネットワークに接続しない場合に限り、入札者が用意する PC の利用を可とする。閲覧資料の

複写等による閲覧内容の記録は行わないこと。

オ. 連絡先:原子力規制委員会原子力規制庁長官官房総務課情報システム室
電話03－5114－2130

(3) その他

本仕様書について疑義等がある場合は、応札資料作成要領の別紙2「質問状」により質問すること。
なお、質問に対する回答は適宜行うこととする。

11 附属文書

・ 別紙1 参考資料
・ 別紙2 閲覧資料一覧
・ 様式1 再委託承認申請書
・ 様式2 機器・役務リスト(案)

以 上

別紙１

参考資料

No.	資料	備考
1	原子力安全規制に関する組織等の改革の基本方針	https://www.nra.go.jp/data/000068977.pdf
2	独立行政法人原子力安全基盤機構の解散に関する法律	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=425AC0000000082
3	デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/resources/standard_guidelines
4	デジタル・ガバメント推進標準ガイドライン解説書	同上
5	デジタル・ガバメント推進標準ガイドライン実践ガイドブック	同上
6	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	https://www.nisc.go.jp/policy/group/general/risk.html
7	公用文作成の要領（昭和27年4月4日内閣閣甲第16号内閣官房長官依命通知）	https://www.bunka.go.jp/kokugo_nihongo/sisaku/joho/joho/kijun/sanko/koyobun/pdf/yoryo_ver02.pdf
8	環境基本法	https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=405AC0000000091
9	環境物品等の調達の推進を図るための方針	https://www.env.go.jp/press/files/jp/108774.pdf
10	環境物品等の調達の推進に関する基本方針	https://www.env.go.jp/policy/hozen/green/g-law/net/kihonhoushin.html
11	原子力規制委員会情報セキュリティポリシー	https://www.nra.go.jp/data/000129977.pdf
12	IT製品の調達におけるセキュリティ要件リスト	https://www.meti.go.jp/policy/netsecurity/cclistmetisec2018.pdf
13	IT製品の調達におけるセキュリティ要件リストガイドブック	https://www.ipa.go.jp/security/it-product/guidebook.html
14	著作権法	https://laws.e-gov.go.jp/law/345AC0000000048
15	予算決算及び会計令	https://laws.e-gov.go.jp/law/322IO0000000165/
16	工事請負契約等に係る指名停止等措置要領について	https://www.env.go.jp/kanbo/chotatsu/notice/no080410002.pdf
17	一般職の任期付職員の採用及び給与の特例に関する法律	https://laws.e-gov.go.jp/law/412AC0000000125/
18	国と民間企業との間の人事交流に関する法律	https://laws.e-gov.go.jp/law/411AC0000000224/
19	財務諸表等の用語、様式及び作成方法に関する規則	https://laws.e-gov.go.jp/law/338M50000040059/
20	原子力規制委員会業務継続計画	https://www.nra.go.jp/data/000473440.pdf
21	政府情報システムに係るネットワークの再編方針	https://www.soumu.go.jp/main_content/000348747.pdf
22	電子政府推奨暗号リスト	https://www.cryptrec.go.jp/list.html
23	『高度標的型攻撃』対策に向けたシステム設計ガイド	https://warp.da.ndl.go.jp/info:ndljp/pid/12446699/www.ipa.go.jp/security/vuln/newattack.html
24	常用漢字表	https://www.bunka.go.jp/kokugo_nihongo/sisaku/joho/joho/kijun/naikaku/pdf/joyokanjihyo_20101130.pdf
25	情報システム安全対策基準	https://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu03j.pdf
26	産業技術総合研究所の活断層データベース	https://gbank.gsj.jp/activefault/
27	首都直下型地震緊急対策区域	http://www.bousai.go.jp/jishin/syuto/index.html

別紙２

閲覧資料一覧

No.	分類	資料名
1	第3次行政LAN更改時の資料	
2		設計・構築実施計画書
3		設計・構築実施要領
4		情報管理計画書
5		要件定義書
6		設計書・基本計画書
7		設計書・詳細設計書
8		プロジェクト計画書
9		プロジェクト管理要領
10		セキュリティルール
11		テスト計画書
12		単体テスト結果報告書
13		結合テスト結果報告書
14		総合テスト結果報告書
15		脆弱性診断結果報告書
16		テスト項目表
17		移行計画書
18		移行ガイドライン
19		移行データ調査結果報告書
20		移行手順書
21		移行マニュアル
22		移行ツール
23		移行リハーサル計画書
24		移行リハーサル結果報告書
25		移行結果報告書
26		研修用資料
27		教育実施計画書
28		教育実施報告書
29		運用設計書
30		保守設計書
31		中長期運用・保守計画書
32		運用保守計画書
33		運用保守手順書
34		情報資産管理標準シート・情報システム台帳
35		再委託承認申請書（記入例）
36	第3次行政LAN運用・保守関連資料	
37		月次定例報告資料
38		年次報告資料
39	クローズドLAN関連資料	
40		要件定義書
41		設計書・基本計画書
42		設計書・詳細設計書
43		月次運用報告書
44		年次運用報告書
45	解析LAN関連資料	
46		要件定義書
47		設計書・基本計画書
48		設計書・詳細設計書
49		月次運用報告書
50		年次運用報告書
51	技術情報システム関連資料	
52		要件定義書
53		設計書・基本計画書
54		設計書・詳細設計書
55		月次運用報告書
56		年次運用報告書
57	規制庁Wi-Fi関連資料	
58		ネットワーク構成図
59		詳細設計書
60		AP配置図
61	代替庁舎関連資料	
62		フロア図
63		ラック構成図

様式１

再委託承認申請書

令和　　年　　月　　日

支出負担行為担当官
原子力規制委員会
原子力規制庁長官官房参事官　殿

住　　所
商号又は名称
代 表 者 氏 名

契約件名「令和７～11年度第４次原子力規制委員会ネットワークシステムの構築及び運用・保守業務」に関して、再委託をしたく下記のとおり承諾を求めます。

記

再委託の相手方の住所及び社名	
再委託を行う業務の範囲	
再委託を必要とする理由	
契約金額	

（※ 再委託先が複数の場合には、表組みを複製のうえ記入してください。）

以上

様式２

機密性2情報

機関番号	機関名
124	環境省（原子力規制庁）

※　記載欄が足りない場合は行を追加してください。
※　行の加除以外の変更（数式やリンクの貼付等を含む）は行わないでください。

リスト提出日	（規制庁記入欄）
回答希望日	（規制庁記入欄）

登録番号	調達案件名（システム名）	ファイル名	調達業者等	通番	区分	製造業者・役務実施業者	本社所在国	業者の法人番号	製品名・役務実施場所	型番	備考
2	令和7～11年度第4次原子力規制委員会ネットワークシステムの構築及び運用・保守業務	第4次行政LAN機器一覧		1							
				2							
				3							
				4							
				5							
				6							
				7							
				8							
				9							
				10							
		第4次行政LAN再委託先一覧		1							
				2							
				3							
				4							
				5							
				6							
				7							
				8							
				9							
				10							

※「例示」及び記載のない行は削除し、記載欄が足りない場合は行を追加してください。
※　行の加除以外の変更（数式やリンクの貼付等を含む）は行わないようお願いいたします。

リスト確認者	（規制庁記入欄）
担当部局課	（規制庁記入欄）
連絡先メールアドレス	（規制庁記入欄）
連絡先電話番号	（規制庁記入欄）