平成３０～３４年度
放射線障害防止法に係る運用管理システム
の更新及び賃貸・運用保守

要件定義書

平成３０年５月

原子力規制委員会原子力規制庁
長官官房技術基盤グループ
放射線規制部門

目次

１．　業務要件の定義

１．１　業務実施手順に関する事項

（１）　業務の範囲（業務機能とその階層）

本業務の対象となる２つのシステムにて、運用されている業務範囲は以下のとおりである。なお、システムの更新業務は「②放射線源登録管理システム」のみ、保守業務は「①放射線障害防止総合管理システム」及び「②放射線源登録管理システム」が対象である。

①放射線障害防止総合管理システム

- 放射線障害防止法に基づいて各事業所より提出される申請・届出書類を基に、各審査官が当該システムのデータベースに入力を行い、データベースの更新・維持及び共有を行う。
- 維持されたデータベースを基に、許可（承認）証の印刷、主任者免状の印刷、検査用資料の出力、統計資料の元データの出力、事業者情報の管理・比較を行う。
- 定期的に放射線源登録管理システムとの情報連携作業を行うとともに、当該システムのデータと放射線源登録管理システムのデータの照合を適宜行う。

②放射線源登録管理システム

- 法令で定められた特定の放射能以上の密封された放射線源について、各事業所より、受払情報、在庫情報、輸出入情報、廃棄情報、製造情報等の報告を受け、報告内容の確認とシステム内のデータベースとの照合を行う。
- 報告された輸出入情報に関して、国内法令及び国際原子力機関（ＩＡＥＡ）の行動規範に照らし、適切に実施されているか確認を行う。
- 報告期日（受払情報であれば１５日以内）を過ぎた事業所に対し、確認と注意喚起を行う。
- 定期的に放射線障害防止総合システムとの情報連携作業を行うとともに、当該システムのデータと本システムのデータの照合を適宜行う。

（２）　業務フロー図

閲覧資料を参照すること。

（３）　業務の実施に必要な体制

①放射線障害防止総合管理システム

実施体制	組織概要	補足
原子力規制庁職員	窓口における各種申請・届出等の受付及び審査を行う。	
	上記審査を踏まえ、放射線障害防止総合管理システムのデータベースに反映すべき情報を反映する。	
	放射線障害防止総合管理システムのデータベースを基に、必要に応じ許可（承認）証の印刷、主任者免状の印刷、検査用資料の出力、統計資料の元データの出力、事業者情報の管理・比較を行う。	

運用保守業者	定期的に放射線源登録管理システムとの情報連携作業等を行うとともに、当該システムのデータと放射線源登録管理システムのデータの照合等を適宜行う。	

②放射線源登録管理システム

実施体制	組織概要	補足
原子力規制庁職員	窓口における各種報告等の受付及び内容確認、放射線源登録管理システム内のデータベースとの照合を行う。	
	上記確認の結果、放射線源登録管理システムのデータベースに反映すべき情報を反映する。	
	各種報告の期日（受払情報であれば 15 日以内）を過ぎた事業所に対し、確認と注意喚起を行う。	
運用保守業者	定期的に放射線障害防止総合管理システムとの情報連携作業等を行うとともに、当該システムのデータと放射線源登録管理システムのデータの照合等を適宜行う。	

（4） 入出力情報項目及び取扱量

業務処理	画面・帳票名	画面・帳票概要	入出力の区分	主な入出力情報項目	取扱量	利用目的	補足
事業者登録	―	―	入力/出力	登録事業者	約 17,500 件		
報告受付	―	―	入力/出力	報告情報	約 60 万件		

1．2 規模に関する事項

（1） システムの利用者数

①放射線障害防止総合管理システム

利用者	主な利用拠点	主な利用時間帯	利用者数	補足
原子力規制庁職員	本庁	8:30～18:15 ※土日祝日及び年末年始を除く	30 名	

②放射線源登録管理システム

利用者	主な利用拠点	主な利用時間帯	利用者数	補足
放射線源利用事業者	事業者拠点	24 時間 365 日	約 500 社	
原子力規制庁職員	本庁	8:30～18:15 ※土日祝日及び年末年始を除く	1 名	

（2） 単位（年、月、日、時間等）当たりの処理件数

本業務の単位あたりの処理件数は次の表のとおりである。

表１－２－２　処理件数

項目	処理件数		補足
	定常時	ピークの特性	
申請及び届出、登録の件数（平成 28 年度）	約 16000 件/年（放射線障害防止総合管理システム） 約 6000 件/年（放射線源登録管理システム）	年度末に集中	

１．３ 時期・時間に関する事項

（1） 業務の時期・時間

	実施時期・期間	実施・提供時間	補足
通常期	4、5、7～3 月	8:30～18:15	放射線源登録管理システムの受付は 24 時間 365 日
繁忙期	6 月	8:30～18:15	放射線源登録管理システムの受付は 24 時間 365 日

１．４ 場所等に関する事項

（1） 実施場所

場所名	実施体制	実施業務	所在地	補足
本庁（六本木ファーストビル）	原子力規制庁職員	放射線障害防止総合管理システム及び放射線源登録管理システムを用いた業務	東京都港区六本木１－９－９	システムを使用する端末及び場所が、規制庁内に限定されることとなる。
庁外データセンター	行政ＬＡＮ運用事業者	行政ＬＡＮに関わる公開サーバ等の運用	神奈川	
請負者	請負者	保守用のリモート接続端末から庁外データセンターに接続する。運用監視、各種ログ取得、ホームページ告知掲載等を実施する	請負者	
		問い合わせの保守受付窓口を設置し、障害対応及び操作支援等の運用保守業務を実施する	請負者	

（2） 設備、物品等資源の定義方法

ア. 放射線障害防止総合管理システム

種類	量	補足
ラック	1	既存のものを活用 なお、クローズド LAN 環境のラック等については、規制庁が準備したものを利用する
LAN 環境	1 式	
AC 電源	2KVA（容量）、2 箇所、2 系統	
空調装置	1 式	

イ. 放射線源登録管理システム

種類	量	補足
ラック	1	既存のものを活用 なお、行政 LAN 運用事業者が運用する庁外データセンターのラック、電源設備、空調設備、基幹スイッチ、DNS、NTP、SMTP 等については、行政 LAN 運用事業者が準備したものを利用する
電源	1 式	
空調装置	1 式	
基幹スイッチ	2 式	
外部用 DNS	1 式	
内部用 DNS	1 式	
NTP	1 式	
SMTP	1 式	

１．５ 管理すべき指標に関する事項

本システムの管理すべき指標は次の表のとおりである。

No.	指標	目標値	計測方法	計測周期
1	【性能指標】 平均応答時間	平常時、概ね 3 秒以内 ピーク時、概ね 8 秒以内	システム調査	1 回／年
2	【信頼指標】 稼働率	24 時間 365 日稼働 稼働率 99.5% （停止時間：年間 44 時間）	（稼働予定時間－停止時間）／稼働予定時間×100	1 回／年
3	【信頼指標】 平均復旧時間 MTTR	主任者情報へのアクセス記録管理を適正化する	復旧時間合計／復旧回数合計	1 回／年

１．６ 情報システム化の範囲に関する事項

（1）放射線障害防止総合管理システム

・ 法令に基づいて各事業所より提出される申請・届出書類を基に、各審査官が当該

システムのデータベースに入力を行い、データベースの更新・維持及び共有を行う。

- 維持されたデータベースを基に、許可（承認）証の印刷、主任者免状の印刷、検査用資料の出力、統計資料の元データの出力、事業者情報の管理・比較を行う。
- 定期的に放射線源登録管理システムとの情報連携作業等を行うとともに、当該システムのデータと放射線源登録管理システムのデータの照合等を適宜行う。

（２）放射線源登録管理システム

- 法令で定められた特定の放射能以上の密封された放射線源について、各事業所より、受払情報、在庫情報、輸出入情報、廃棄情報、製造情報等の報告を受け、報告内容の確認とシステム内のデータベースとの照合を行う。
- 報告された輸出入情報に関して、国内法令及びＩＡＥＡの行動規範に照らし、適切に実施されているか確認を行う。
- 報告期日（受払情報であれば１５日以内）を過ぎた事業所に対し、確認と注意喚起を行う。
- 定期的に放射線障害防止総合システムとの情報連携作業等を行うとともに、当該システムのデータと本システムのデータの照合等を適宜行う。

２．　機能要件の定義

２．１　機能に関する事項

２．１．１　放射線障害防止総合管理システム

放射線障害防止総合管理システムは、以下３つのサブシステムから成り立っており、サブシステムは、それぞれ専用のアプリケーションソフトウェア（（１）放射線障害防止総合管理サブシステム、（２）申請書閲覧サブシステム、（３）ファイル共用サブシステム）により運用される。

（１）放射線障害防止総合管理サブシステム

①職員認証機能

職員のログイン認証

②メニュー機能

システムのメニュー表示

③主任者運用機能

放射線取扱主任者に関する管理（資格所有者氏名・免状番号・取得日など）

④事業所運用機能

放射性同位元素の使用等の許可や届出の内容等を管理（事業所に関する事項（名称・所在地など）・許可届出の内容（核種・数量など）・予防規程届出日・主任者選任解任など）

⑤立入検査機能

立入検査結果に関する管理（検査者・結果等のデータ）

⑥管理状況報告書機能

毎年６月３０日までに提出される当該報告書に関する管理

⑦申請書管理機能

氏名等に係る変更届に関する管理

⑧統計処理機能

システム内にある事業所の統計に関する管理

⑨マスタ保守機能

システム内にある普遍的なデータ等に関する管理

⑩連携データ出力機能

放射線源登録管理システムとの連携データを出力

（２）申請書閲覧サブシステム

申請者イメージファイルの検索・閲覧

（３）ファイル共用サブシステム

申請書データ等のデータ共用

２．１．２　放射線源登録管理システム

放射線源登録管理システムは、報告対象となる事業者が本制度に係る報告をオンライン上で行えるようにするための Microsoft 社製 EXCEL（以下「エクセル」という。）報告様式サブシステム及び事業者側サブシステム、並びに規制当局が報告情報等を管理するための職員側サブシステムの３つのサブシステムを備えており、専用のアプリケーションソフトウェア（放射線源登録管理システム）により運用される。

（１）エクセル報告様式サブシステム

①報告用電子データフォーム入力機能

報告データの入力

②報告用電子データ生成機能

報告用電子データの生成

（２）事業者側サブシステム

①使用者等認証機能

使用者等のログイン認証

②報告用電子データ送信機能

報告用電子データの送信・登録

③お知らせ内容表示機能

お知らせ情報の閲覧

④様式ダウンロード機能

報告用電子データ生成ツールのダウンロード

（３）職員側サブシステム（平成３０年３月よりサービス停止中。）

①職員認証機能

職員のログイン認証

②メニュー機能

線源職員側サブシステムのメニュー表示

③事業者向けお知らせ情報の掲載機能

上述の「（３）職員側サブシステム」は、メーカーサポート切れのフレームワーク（「Apache Struts 1.2」）を利用していたため、「平成２９年度放射線障害防止法に係る運用管理システム　アプリケーション等の改修業務」において、サービスを停止した。

このフレームワークの更新業務は本件の所掌外だが、アプリケーション及びデータの移行と運用時における事業者向けお知らせ情報の掲載については本調達に含める。

２．２　画面に関する事項

「放射線障害防止総合管理システム」、「放射線源登録管理システム」とも画面に関する変更はないため取扱い事項は定義しない。

２．３　帳票に関する事項

「放射線障害防止総合管理システム」、「放射線源登録管理システム」とも帳票に関する変更はないため取扱い事項は定義しない。以下、参考まで帳票の名称一覧を記す。帳票ソフトウェアは「Crystal Reports」を利用しており、クライアントＰＣのランタイム環境により動作する。

２．３．１　放射線障害防止総合管理システム

１．第１種放射線取扱主任者免状
２．第２種放射線取扱主任者免状（一般）
３．特定第２種放射線取扱主任者免状
４．第３種放射線取扱主任者免状
５．第２種放射線取扱主任者免状
６．事業所一覧
７．検査履歴一覧

８．検査カード
９．検査カード裏
１０．管理カード
１１．主任者情報
１２．予防規程受付年月日
１３．放射性同位元素等使用許可証
１４．放射性同位元素等使用承認証
１５．放射性同位元素使用届受理通知
１６．放射性同位元素販売業許可証
１７．放射性同位元素等廃棄業許可証
１８．放射性同位元素賃貸業許可証
１９．略称許可証
２０．貯蔵能力（密封されていない放射性同位元素）
２１．貯蔵能力（密封されている放射性同位元素）
２２．使用数量等（密封されていない放射性同位元素）
２３．密封されていない放射性同位元素
２４．使用数量等（密封されている放射性同位元素）
２５．使用数量等（密封されている放射性同位元素）
２６．密封されている放射性同位元素の種類
２７．放射線発生装置
２８．『放射線管理状況報告書』申請書１
２９．『放射線管理状況報告書』申請書　１　の別紙－Ⅰ
３０．『放射線管理状況報告書』申請書　１　の別紙－Ⅱ
３１．『放射線管理状況報告書』申請書　１　の別紙－Ⅲ
３２．『放射線管理状況報告書』申請書２
３３．『放射線管理状況報告書』申請書２の別紙－Ⅱ
３４．『放射線取扱主任者選任・解任』申請書
３５．『届出使用に関する氏名等の変更届』申請書１
３６．『届出使用に関する氏名等の変更届』申請書２
３７．事業所数の許認可別統計
３８．事業所数の都道府県別統計
３９．事業所数の利用形態別統計
４０．密封貯蔵能力の事業所数統計
４１．密封貯蔵能力の数量統計
４２．非密封貯蔵能力の事業所数統計
４３．非密封貯蔵能力の数量統計
４４．装置機器の使用許可台数統計

４５．放射線発生装置の使用許可台数統計
４６．従事者機関別統計
４７．従事者分布別統計
４８．主任者機関別統計
４９．主任者一覧
５０．主任者受講状況一覧

２．３．２　放射線源登録管理システム
１．報告線源詳細情報
２．放射線源固有情報
３．放射線源の所持に関する情報
４．在庫確認情報
５．カテゴリ毎・事業者一覧
６．カテゴリ毎・線源一覧
７．核種毎・事業者一覧
８．核種毎・線源一覧
９．核種毎・放射線源登録数（線源数及び所有事業所数）
１０．カテゴリ毎・放射線源報告数
１１．核種毎・放射線源報告数
１２．利用通知書
１３．仮データベース一覧
１４．本データベース一覧
１５．放射線源一覧
１６．線源カタログ一覧
１７．装備機器カタログ一覧
１８．事業所一覧
１９．事業所詳細
２０．特定放射性同位元素に係る報告書（エクセル版）

２．４　情報・データに関する事項

「放射線障害防止総合管理システム」、「放射線源登録管理システム」とも情報・データに関する変更はないため取扱い事項は定義しない。万が一、請負者の作業により情報・データに削除・修正などの変更が生じた場合には、請負者の責任と負担により情報・データを復旧させること。

２．５　外部インタフェースに関する事項

「放射線障害防止総合管理システム」、「放射線源登録管理システム（庁内設置部分）」

とも外部インタフェースに関する変更はないため取扱い事項は定義しない。なお、現行の「放射線源登録管理システム（庁外設置部分)」は庁外データセンター内に設置されており、一部機能を庁外データセンター内の他システムと共有しているため、本調達の作業により他システムに影響を与えないこと。万が一、他システムに影響を与えた場合には、請負者の責任と負担において影響を取り除くこと。

3． 非機能要件の定義

3．1 ユーザビリティ及びアクセシビリティに関する事項

（1） 情報システムの利用者の種類、特性

No.	利用者区分	利用者の種類	特性
1	原子力規制庁職員	当該システム利用者	・現行システムに習熟している。 IT リテラシーが高くない職員も存在する。

（2） ユーザビリティ

No.	ユーザビリティ分類	ユーザビリティ要件
1	効率性	職員の業務効率性を考慮し、現行のシステムから大幅に使い勝手を変えないこと。セキュリティ対策等の理由により使い勝手に変化が生じる場合は、職員の特性を踏まえた上で極力平易に使えるよう手立てを講じること。
2	ヘルプ	・利用者が必要とする際に、ヘルプ情報やマニュアル等を参照できるようにすること。 ・ヘルプ情報やマニュアル等は、職員の特性を踏まえ、平易に理解できるよう配慮すること。

（3） アクセシビリティ要件

No.	アクセシビリティ分類	アクセシビリティ要件
1	日本語対応	・サーバを構成する全てのハードウェア、ソフトウェアにおいて、日本語の処理ができること。 ・ただし、BIOS 設定画面を除く。 ・利用運用上において実質的に支障がないと原子力規制委員会が認めた部分については、この限りではない。

3．2 システム方式に関する事項

当システムの主要部分は原子力規制委員会原子力規制庁内に設置されたクローズドＬＡＮ内に構築されており、既存である。「放射線源登録管理システム」の庁外データセンター機器の更新にあたっては、以下の方針・方式に基づき実施すること。

（1） 情報システムの構成に関する全体の方針

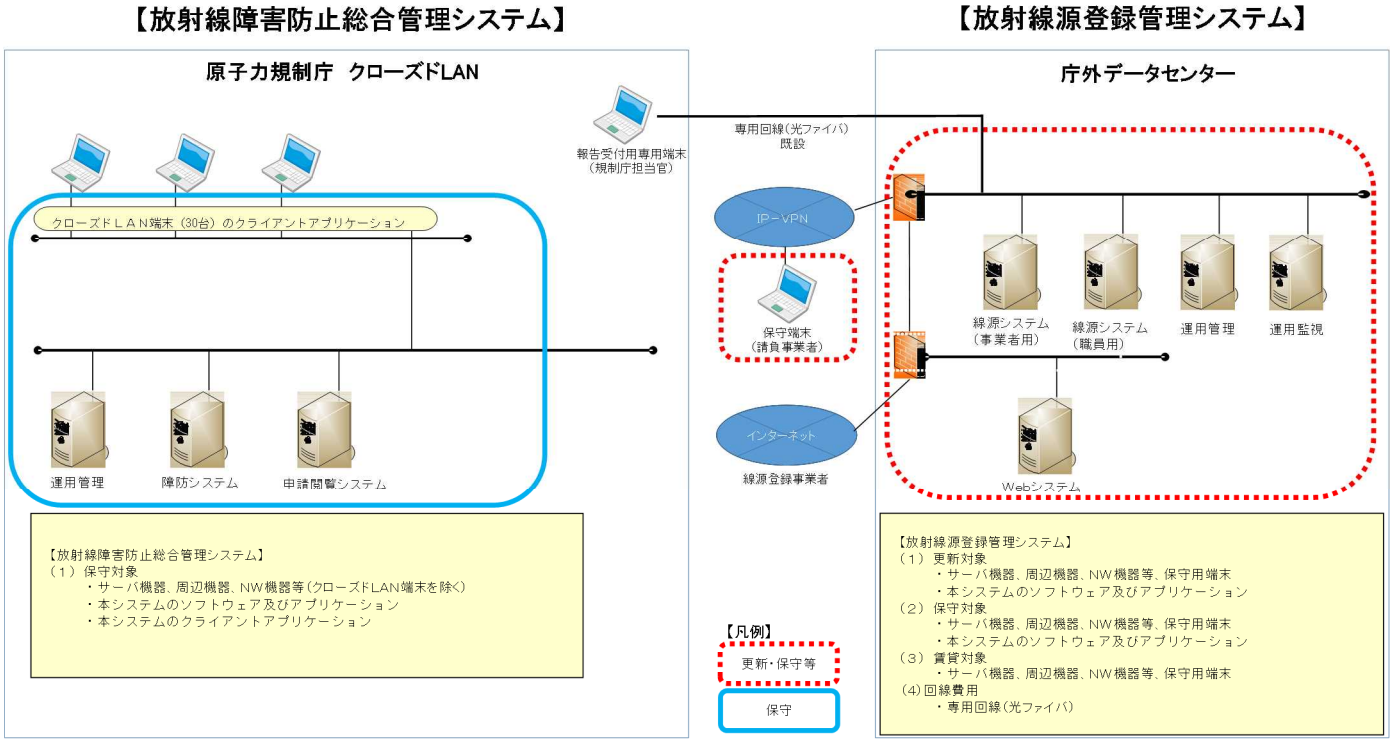
情報システムの構成に係る全体の方針は次の表のとおりである。

全体方針の分類	全体方針
システムアーキテクチャ	・各要件を考慮して最適なものを選択すること。
ソフトウェア製品の活用方針	・広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用する。 ・一部ソフトウェア製品又は製品のバージョンは別添２「ハードウェア及びソフトウェア構成」を参照し構成すること。 ・ソフトウェア製品の指定がない場合、可能な限りオープンソースソフトウェア（ＯＳＳ）製品（ソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア製品）の活用を図る。ただし、それらのＯＳＳ製品のサポートが確実に継続されていることを確認しなければならない。
システム基盤の方針	・システム基盤は、定められた要件に基づきシステム構成を行うこと。(「3.2.(2) システムの全体構成」を参照のこと。)。

（2） システムの全体構成

本システムの全体構成は次の図のとおりである。

【図３．２－１　本システムの全体構成】



（3） 開発方式及び開発手法

放射線源登録管理システムの更新にあたっては、既存のミドルウェア及びデータベース等のソフトウェア製品のバージョンアップ（構築時点での最新化）、及びセキュリティアップデートによる脆弱性対策を行う。その際、放射線源登録管理システムの現行のアプリケーション機能が更新後においても現行システムと同等に動作するよう十分なテストを行い動作保証すること。

新規に導入するネットワーク情報可視化ソフトウェアにおいては、セグメント内におけるトラフィックの流通状態、異常発生、ファイアウォールへの攻撃検知をリアルタイムで把握できるセキュリティ製品を導入し、検知されたイベント情報（セキュリティアラートログ）をもとに通信状況を視覚的（グラフィカル）に把握できるように設定すること。

３．３ 規模に関する事項

（1） 機器数及び設置場所

「放射線障害防止総合管理システム」及び「放射線源登録管理システム」の機器数及び設置場所は下表のとおりである。機器の詳細は現行システムの設計書等を参照すること。

【表３．３－１ 放射線障害防止総合管理システムの機器等】

No	機器の区分	機器数	設置場所	補足
1	AP 兼データベースサーバ	一式	クローズド LAN	
2	運用管理サーバ	一式		
3	ラックコンソール/ラックコンソールスイッチ	一式		
4	イメージファイル用 NAS	一式		
5	バックアップ用 NAS	一式		
6	無停電電源装置	二式		
7	放射線源登録システム専用端末	一式	庁外データセンターと直結	規制庁内 LAN とは接続しない

【表３．３－２　放射線源登録管理システムの機器等】

No	機器の区分	機器数	設置場所	補足
1	仮想基盤（ホスト）	二式	庁外データセンター	更新対象
2	運用管理サーバ	一式		更新対象
3	ストレージ装置	一式		更新対象
4	ネットワーク情報可視化ソフトウェア	一式		新設
5	監視用アプライアンス	一式		更新対象
6	バックアップ装置	一式		更新対象
7	スイッチングハブ	二式		更新対象
8	ファイアウォール	二式		更新対象
9	ラックコンソール	一式		更新対象
10	ＶＰＮ装置	一式		現用
11	終端装置（ＯＮＵ）	一式		現用
12	ＶＰＮ装置	一式	請負者	新設
13	終端装置（ＯＮＵ）	一式		新設
14	保守用端末	一式		新設

仮想基盤のゲストサーバの割り当て想定スペックは、下表のとおりである。

【表３．３－３　仮想基盤のゲストサーバの要求スペック】

No	サーバ名	CPU 割当	メモリ割当	ディスク容量割当
1	Ｗｅｂサーバ	２コア以上	４ＧＢ以上	１００ＧＢ以上
2	ＡＰサーバ	４コア以上	８ＧＢ以上	１２０ＧＢ以上
3	ＤＢサーバ	２コア以上	６ＧＢ以上	１２０ＧＢ以上
4	ログ収集管理サーバ	４コア以上	８ＧＢ以上	１ＴＢ以上

（２） データ量

「１．１業務実施手順に関する事項（４）入出力情報項目及び取扱量」を参照のこと。

（３） 利用者数

「１．２規模に関する事項」を参照のこと。

３．４ 性能に関する事項

「１．５管理すべき指標に関する事項」及び「３．１１情報システム稼動環境に関す

る事項」を参照のこと。「放射線源登録管理システム」の庁外データセンター機器の更新に関する性能については、本文の添付資料『「放射線源登録管理システム」の庁外データセンター機器の更新に関わるハードウェア及びソフトウェアの仕様要件』を参照のこと。

３．５　信頼性に関する事項

「１．５管理すべき指標に関する事項」及び「３．１１情報システム稼働環境に関する事項」を参照のこと。

３．６　拡張性に関する事項

「３．１１情報システム稼働環境に関する事項」を参照のこと。

３．７　上位互換性に関する事項

・ クライアント端末のＯＳ及びウェブブラウザのバージョンアップに備え、ソフトウェア製品の特定バージョンに依存する機能の利用を最低限とすること。
・ 納入する各ソフトウェアの動作をサポートすること。各ソフトウェアのバージョンアップ時に、容易にバージョンアップが可能となるよう本システムで提供する機能に関しては、製品の改変及び特殊な作り込みを排除すること。

３．８　中立性に関する事項

本調達の請負者以外の業者による本システム運用業務の遂行を可能とすることを目的とし、原則として本システムの構成要素（ハードウェア及びソフトウェア等）には、仕様の公開されたプロセッサ及びインタフェース規格等、可能な限りオープンな技術を採用し、特定の業者でなければ導入できない製品及び技術は利用しないこと。

３．９　継続性に関する事項

（１）　災害や事故等が発生した場合において、本業務の継続性を確保するために必要な要件やそのための方策について検討の上、原子力規制庁職員（以下、「担当官」という。）と協議すること。

（２）　大規模な災害が発生し、当庁が被災した場合においては、システムの一時停止もやむを得ないものとする。保守契約の範囲を超える被災時の復旧作業については、本調達の範囲には含めないこととする。

３．１０　　情報セキュリティに関する事項

（１）　情報セキュリティ対策要件

請負者は、下記の点に留意して情報セキュリティを確保するものとする。

【表３．１０－１　情報セキュリティ対策要件一覧】

No.	情報セキュリティ対策	対策に係る要件
1	主体認証	・システムによるサービスを許可された者のみに提供するため、システムにアクセスする主体のうちサービス利用者の認証を行う機能として、識別コード（ID）とパスワードの方式を採用すること。 ・パスワードの定期的な変更や世代管理等の厳格なパスワードポリシーによる管理機能を備えること。
2	権限管理	・主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。 ・システムの利用範囲を利用者の職務に応じて制限するため、システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。 ・アカウントを制御し、各アカウントの証跡の記録と管理をする。 ・特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。
3	システムの構成管理	・情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに、文書どおりの構成とすること。 ・各種製品の脆弱性に関する情報が公開された場合、原子力規制庁に内容を提示し承認を得て改善を実施する。
4	不正プログラムの感染防止	・機器等の開発工程において、府省庁が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。 ・不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。 ・システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を一元管理する機能を備えること。

5	セキュリティ監視・可視化	情報セキュリティ監視のため、リアルタイムでシステム内の通信状況が把握できる仕組みを導入する他、セキュリティインシデントへの対応としてセキュリティアラート等を保存及び表示する仕組みを導入すること。
6	ログの蓄積・管理	・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、収集後のログを改ざん不能な状態で、少なくとも 1 年間の期間保管すること。（最終的な保管期間については、担当官との協議すること。）
7	ログの保護	・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。
8	時刻の正確性確保	・情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。
9	暗号化及び電子署名	・システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存しないこと。

（2） 情報セキュリティ要件

請負者は、下記の点に留意して情報セキュリティを確保するものとする。

ア. システムの開発工程において、原子力規制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. システムに原子力規制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、原子力規制庁と請負先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. 請負者の資本関係、役員等の情報、作業要員の氏名、所属、実績、国籍等の情報が把握できること。

エ. 請負者の情報セキュリティ対策の実施について、以下の要件を満たすこと。

① 情報セキュリティインシデントが発生した場合、原因分析及び対処方法を担当官に報告し、承認を得ること。

② 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担当官に定期的に報告を行うこと。

③ 情報セキュリティ対策の完了後１年以内に請負者側の責め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、請負者は無償で速やかに必要な措置を講ずること。

オ. 請負者は、担当官から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ずること。原子力規制庁より提供された要機密情報は、請負業務以外の目的で利用しないこと。また、本業務において請負者が作成する情報については、担当官からの指示に応じて適切に取り扱うこと。

カ. 請負者は、機密性２を含む要保護情報を取り扱う保守端末について、盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護すること。

キ. 請負者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護すること。

ク. 請負者は、原子力規制委員会情報セキュリティポリシーに準拠した情報セキュリティ対策の履行が不十分と見なされるとき又は請負者において請負業務に係る情報セキュリティ事故が発生したときは、必要に応じて担当官の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。

ケ. 請負者は、担当官から提供された要機密情報が業務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。また、請負業務において請負者が作成した情報についても、担当官からの指示に応じて適切に廃棄すること。

コ. 請負者は、本業務におけるシステムの構築・改良等が完了し運用を開始する前に、請負者の品質管理責任者による品質報告及びセキュリティ報告を実施すること。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「脆弱性検査結果報告書」として作成し、担当官に報告すること。また、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。

サ. 請負者は、本業務の終了時に、本業務で実施した情報セキュリティ対策を書面で報告すること。

（参考）原子力規制委員会情報セキュリティポリシー

https://www.nsr.go.jp/data/000129977.pdf

シ. 請負者は、本業務の終了時に、本業務で実施した情報セキュリティ対策を書面で報告すること。

（３） システムのライフサイクル

請負者は、下記の点に留意してライフサイクルを確保するものとする。

ア.　請負者は、本システムを新規に構築、又は更改する際には、当該情報システム台帳を作成の上、セキュリティ要件に係る内容を記録又は記載し、当該内容について原子力規制庁に報告すること。

イ.　請負者は、所管する本システムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅したシステム関連文書を整備すること。

① システムを構成するサーバ装置及び端末関連情報

② システム構成要素ごとの情報セキュリティ水準の維持に関する手順

③ 情報セキュリティインシデントを認知した際の対処手順

ウ.　請負者は、機器または開発等のライフサイクルで不正な変更が加えられないように管理を行う。また、原子力規制庁が確認できる仕組みを設けること。

エ.　請負者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備し、原子力規制庁に承認を得ること。

オ.　請負者は、原子力規制委員会情報セキュリティポリシーに応じた体制の整備を行うこと。

カ.　請負者は、機器等を調達する場合には、「ＩＴ製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。

キ.　請負者は、基盤となるシステムを利用してシステムを構築する場合は、基盤となるシステム全体の情報セキュリティ水準を低下させることのないように、基盤となるシステムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。

ク.　請負者は、以下の事項を含む事項を適切に実施すること。

① システムのセキュリティ要件の適切な実装

② 情報セキュリティの観点に基づく試験の実施

③ 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

ケ.　請負者は、システムの保守において、「調達仕様書」及び本資料を確認のうえシステムに実装されたセキュリティ対策に従い適切に運用すること。

コ.　請負者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の選定における判断の一要素として活用すること。

サ.　請負者は、システムの構築において、情報セキュリティの観点から必要な措置を講ずること。

シ.　請負者は、構築した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必要な措置を講ずること。

ス.　請負者は、機器等の納入時又は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確認すること。

セ.　請負者は、基盤となるシステムを利用して構築されたシステムを運用する場合は、基盤となるシステムを整備し、運用管理する原子力規制委員会との責任分界に応じた運用管理体制の下、基盤となるシステムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切にシステムの運用設計を行うこと。

ソ.　請負者は、不正な行為及び意図しない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、保守に係る作業についての記録を管理すること。

タ.　請負者は、本システムの更改又は廃棄を行う場合は、当該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、以下の措置を適切に講ずること。

①　本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

②　本システム廃棄時の不要な情報の抹消

チ.　請負者は、本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、監視等の状況により見直しを適時検討し、必要な措置を講ずること。

（4）　情報システムの構成要素

請負者は、下記の点に留意して構成要素を定義するものとする。

ア.　請負者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

イ.　請負者は、要管理対策区域外で要機密情報を取り扱うモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずること。

ウ.　請負者は、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、端末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。

エ.　請負者は、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について定期的に見直しを行うこと。

オ.　請負者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。

カ.　請負者は、端末の契約期間が終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。

キ.　請負者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、将来の見通しも考慮し、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。

ク．　請負者は、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、対策時に原子力規制庁に提示し承認を得ること。

ケ．　請負者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を年１回程度の頻度で確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図ること。

コ．　請負者は、サーバ装置の契約期間が終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること。

３．１１　　情報システム稼働環境に関する事項

（1） ハードウェア・ソフトウェア構成

ア　システム構成図

本システムのハードウェア構成図は「３．２．（２）情報システムの全体構成」及び「３．３規模に関する事項」を参照のこと。

イ　ハードウェア・ソフトウェア要件

「放射線源登録管理システム」の庁外データセンター機器の更新については、本文の添付資料『「放射線源登録管理システム」の庁外データセンター機器の更新に関わるハードウェア及びソフトウェアの仕様要件』を遵守すること。

「放射線障害防止総合管理システム」と「放射線源登録管理システム」の運用支援及び保守業務に係るハードウェア及びソフトウェアの詳細仕様は、現行システムの設計書等を参照すること。

ウ　機器据付要件

「放射線源登録管理システム」の庁外データセンター機器の更新に係る機器据付要件は下記のとおりである。

（ア）基本要件

- 搬入及び据付調整、初期動作確認は、請負者の責任と負担において実施すること。
- 調達に係る機器等の搬入及び据付調整は、担当官及び行政ＬＡＮ運用事業者の指示に従うこと。
- 調達に係る機器等の搬入の日程、方法等については、担当官と協議し、了承を得ること。
- 本調達に係る機器等の搬入及び据付調整等作業による諸設備の破損については、担当官及び行政ＬＡＮ運用事業者の指示に従い、請負者の責任と負担において修復等を実施すること。

（イ）機器据え付け要件

・　下記に記した機器一式の据え付けについては、担当官と協議をし、了承を得た日程に基づき実施すること。
・　機器の梱包材等は請負者の負担のもと、速やかに撤去すること。
・　設置場所への機器の据付に際しては、担当官及び行政ＬＡＮ運用事業者が指定する搬入経路にて実施し、建造物に損傷を与えないよう処置を施すこと。

（ウ）その他要件

・　機器の搬入並びに梱包材等の撤去に係る輸送費用及びサーバ機器のラック搭載に必要な備品等の一切については、請負者の負担により実施するものとする。

（２）　ネットワーク構成

ア　ネットワーク構成図

本システム全体のネットワーク構成図は「３．２.（２）情報システムの全体構成」を参照のこと。

イ　ネットワーク回線の要件

「放射線源登録管理システム」に係るネットワークの要件は下記のとおりである。なお、「放射線障害防止総合管理システム」と「放射線源登録管理システム」の運用保守業務のネットワークの詳細は現行システムの設計書等を参照すること。

・　本調達で導入するサーバ、ネットワーク機器等は庁外データセンターにおける行政ＬＡＮ運用事業者が構築・運用する業務ＬＡＮセグメントに接続すること。
・　接続するにあたっては、行政ＬＡＮ運用事業者の管理するＬ２スイッチとの接続方式、ＬＡＮケーブルの必要本数及びＩＰアドレス等は、原子力規制委員会ネットワーク運用事業者と協議し決定すること。
・　現状、事業者からの線源登録等の報告を受けるための専用端末を原子力規制委員会原子力規制庁内に設置し、庁外データセンターに設置している報告受付サーバ（ＡＰサーバ）と専用回線（光回線）で接続し業務を行っている。これらの専用回線（光回線）の４年間（平成３１年４月１日～平成３５年３月３１日）の継続利用に係る通信費用等を本調達に含めること。
・　なお、新たに専用回線（光回線）を敷設することも可能だが、旧回線の撤去工事、新回線工事及び通信機器手配等も本調達に含めるものとし、行政ＬＡＮ運用事業者及び原子力規制委員会ネットワーク運用事業者と協議のうえ設置すること。旧回線の撤去は、請負者の責任と負担において現行回線事業者に再委託の上実施すること。
・　ＷＡＮ回線は全て「帯域保証」とし、現行の回線と同等帯域を提供すること。

- ＷＡＮ回線は閉域網とし、外部からのアクセスができないものであること。
- ＷＡＮ回線の終端には回線終端装置、ＷＡＮルータ装置を設置すること。
- ＷＡＮ 回線は、イーサネット（レイヤ２）のプロトコルによって制御すること。
- ＷＡＮ回線の帯域を処理可能なルータを提供すること。
- ＷＡＮルータ装置は、ＢＧＰ、ＯＳＰＦ に対応していること。
- ＷＡＮルータ装置、回線終端装置は発注者が指定したラックへ収容するため、事前にサイズ、重量、設置機器台数の情報の提供を行うこと。
- 電源はＯＡタップを利用せず、ラック指定の電源を用いること。電源について発注者にて手配するため、事前に必要な電源口数、消費電力の情報の提供を行うこと。
- ＷＡＮ回線の敷設及びＷＡＮルータ装置の設置に当たって、必要があれば現地調査を実施し、現地調査の結果を報告すること。
- ＷＡＮルータ装置については、設定内容等を踏襲すること。
- 各拠点に回線敷設及び機器設置を実施すること。
- ＷＡＮルータ装置設置後は、対向拠点と疎通試験を実施すること。
- ネットワーク移行後に発注者が実施する業務確認（システム確認）にて正常性が確認されるまで、立会いを行うこと。
- ＷＡＮ回線、ＷＡＮルータ装置含めて２４時間３６５日死活監視を行うこと。
- ＷＡＮ回線及びＷＡＮルータ装置は２４時間３６５日で保守すること。
- ＷＡＮ回線のトラフィック状況を確認でき、発注者がトラフィック状況の情報を求めた場合は、それに応じること。
- ＷＡＮ回線及びＷＡＮルータ装置の障害窓口を２４時間３６５日で用意すること。

（３） 施設・設備要件

「放射線源登録管理システム」の庁外データセンター機器の更新で導入するサーバ、ネットワーク機器等は原子力規制委員会が指定する行政ＬＡＮ運用事業者が運用する庁外データセンターに設置すること。

３．１２　　テストに関する事項

（１） テストの基本要件

- 要件定義書に基づきテスト設計を行い、テスト仕様書で定義した各種テスト及び更新の影響のある機能も含めて正常性を担保すること。
- 現行アプリケーション機能の動作保証をすること。
- 各種テストの実施完了後、原子力規制員会に対してテスト実施結果の報告を行うこと。

・ 情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上、テストを実施すること。

（2） テストの種類毎の要件

本業務における改修作業において、実施すべき各テストの実施内容等を下表に示す。

No.	テストの種類	テストの実施内容等	テスト環境
1	結合テスト	・請負業者へ一時的に納入される機器(ハードウェア及びソフトウェア)に対して構築を行い、機器自体の動作及び設定した機器内の各種サービス機能が設計書通りに正しく動作するかテストする。	請負者内
2	総合テスト	・本番環境と同じような疑似的なシステム環境を整備し、各機器(ハードウェア及びソフトウェア)を接続した状態で、バックアップ・リカバリ、機器間の通信等の動作が運用手順書及び各種マニュアルのとおりに正しく動作するか、異常ケースも含めて総合的にテストする。 ・また、設定された機器上で放射線源登録管理システムの各アプリケーション機能が正しく動作するか総合的にテストする。	請負者内
3	受入テスト	・庁外データセンターに設置後の機器等を試運転させ、正常に動作するか、庁外データセンターの各サービス（時刻同期、ＤＮＳなど）の連携に問題はないか等のテストはもとより、外部（インターネット、原子力規制庁の報告受付用端末、請負者の保守端末）から正常にアクセスできるか確認する。 ・要件定義書に基づいた信頼性、性能・拡張性、セキュリティ等に関する要件が満たされているかを確認する。 ・受入テストにおいて、担当官が確認する作業については、手順書の整備や作業支援を実施すること。	本番環境

３．１３　　移行に関する事項

・ 請負者は、移行対象を明確化し移行方法及び手順、スケジュールや実施体制等については原子力規制庁と調整の上、移行作業を実施すること。

・ 現行システムから移行を行う対象サーバは、本文の添付資料『「放射線源登録管理システム」の庁外データセンター機器の更新に関わるハードウェア及びソフトウェアの仕様要件』に記載する機器を対象とする。
・ 現行基盤踏襲環境のＯＳ及びソフトウェア等について、請負者が必要数を準備すること。

（1） 移行リハーサル及び移行後作業

本システムのシステム移行及びデータ移行の手順は以下のとおりである

ア． 移行リハーサル（移行データの検証、移行時間の測定等）

・ 請負者は原子力規制庁及び行政ＬＡＮ運用事業者と移行データの検証方法に関する認識合わせを行う。また「移行計画書」等に基づき移行リハーサルを実施し、移行リハーサルに向けた移行実施手順、移行スケジュールの検証を行う。なお、システム移行リハーサルは、システムの性格やリハーサルの結果によって、複数回実施する場合がある。

イ． システム移行後作業

・ 運用が安定していることを確認後、データ移行用に準備したデータが存在する場合は原子力規制庁の承認を得て、データの削除を行う。
・ 請負者はシステム移行後、「移行実施結果報告書」を原子力規制庁へ提出すること。

（2） 移行対象データ

「放射線源登録管理システム」の庁外データセンター機器の更新に関わるデータの移行の要否は、次の表のとおりとする。

移行先	対象のサブシステム
本調達で導入するサーバ	・ 線源登録管理システム（事業者向け／職員向け）の各種業務データ（ＤＢ）及びアプリケーション

３．１４ 教育に関する事項

請負者は、「放射線障害防止総合管理システム」と「放射線源登録管理システム」を運用するための「運用管理者マニュアル」に変更が生じる場合は改訂版（あるいは新規版）を作成すること。変更が生じない場合においても、契約期間最終年度において最新版の「運用管理者マニュアル」の最新版を作成すること。作成にあたっては、以下の事項を考慮すること。

・ 担当者の実施する操作に対応した構成であること。

・　画面キャプチャを用いて、表示や遷移のイメージを理解しやすい構成であること。
・　操作マニュアルの利便性を考慮した表記方法や文書ボリュームであること。

３．１５　運用に関する事項

請負者は、本システムの運用を支援するために必要な「運用計画書」及び「運用手順書」、「各種マニュアル」等を作成し、原子力規制庁の承認を受けること。

運用支援業務においては、以下の内容を実施すること。

（1） 運用支援業務内容

本システムの運用支援業務に係る作業内容を以下に示す。

ア　定常時対応

（ア）バックアップ要件

・　既設のサーバ、ネットワーク機器等を用いたシステム（ＯＳ、ミドルウェアを含む。）及びデータのバックアップとリカバリ方法について、運用手順に変更がある場合は改訂した運用手順書を提示した上で実施すること。

（イ）構成管理

・　本システムの機器の構成情報や設定変更情報を管理し、構成に変更が必要な場合は、その理由や影響等を提案書として報告すること。
・　受注者は、構成の変更が行われた場合は、該当するドキュメント類（構成管理台帳等）を更新し、提出すること。
・　本業務は、構成の変更を管理するものであり、構成の変更作業自体は構成管理業務の範囲外とする。

（ウ）セキュリティ管理

・　本システムで使用する各種ソフトウェアのセキュリティ情報等をメーカのサイトから収集し、本システムの運用上、必要なものについては本システムへの影響とあわせて報告し、本システムへのセキュリティパッチ等の適用の要否について担当官と協議すること。ただし、セキュリティパッチ等を適用するにあたり、本システムの開発アプリケーションソフトウェアに改修が必要な場合は、調査報告書を提出するとともに、その対応方法について担当官と協議を行うこと。
・　構成変更に該当するドキュメント類（構成管理台帳等）を更新し、提出すること。

（エ）問合せ対応

・　担当官からの本システムに関する問合せ（例えば、構成管理やセキュリティ管理等）への対応や操作についての支援すること。
・　本システムの利用者からの問合せに関し、担当官からその対応について問合せがあった場合は、これを支援すること。

（オ）セキュリティ監査や各種調査への対応

・　原子力規制委員会が実施するセキュリティ監査等により、設定変更を伴う本システムへの対応指示等を受けた場合には、迅速な調査・検証を実施の上、対応について担当官と協議すること。
・　本システムに関する政府機関からの調査依頼あるいは対応指示事項に関して、担当官等から相談や調査依頼を受けた場合は、遅滞なく助言・参考資料提出等の支援を行うこと。

（カ）主任者管理情報へのアクセス記録の分析（放射線障害防止総合管理システムのみ）

・　データベースに記録されている主任者管理画面での操作ログ（新規登録、更新、削除、検索、参照、印刷）を毎月取得し、アクセス状況の傾向等を分析した結果を報告すること。

イ　報告書の提出

（ア）月次報告書

・　以下に示す項目について、月次で実施した作業の有無、内容等をまとめて報告書を提出すること。
  - システム利用実績
  - 構成管理
  - セキュリティ管理

（イ）年次報告書

年間の登録線源数及び事業者からの報告数を集計した統計資料をまとめた報告書を提出すること。

ウ　事業者向けお知らせ掲示板への情報掲載（放射線源登録管理システムのみ）

・　「放射線源登録管理システム」において、平成２９年度末に職員ＰＣと専用回線で接続している庁外データセンターの線源システム（職員側サブ）の利用を停止した。この影響により担当官による「事業者向けお知らせ掲示板」の操作

が不可能となったため、この代替として、担当官が提示するお知らせ情報を「放射線源登録管理システム」に掲載する作業を受注者が実施すること。

エ　運用支援作業の改善提案

・　受注者は、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、必要に応じて運用・保守計画、運用・保守実施要領に対する改善提案を行うこと。

オ　引継ぎ

・　受注者は、原子力規制委員会が本システムの更改を行う際には、次期システムにおける要件定義支援事業者及び設計・開発事業者等に対し、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。
・　受注者は、本契約の終了後に他の運用・保守事業者が本システムの運用を受注した場合には、次期運用支援事業者に対し、作業経緯、残存課題等についての引継ぎを行うこと。

カ　ＯＤＢ登録用シートの提出

本項は本調達の範囲外であるが、本業務の参考情報として基本事項を以下に示す。

（ア）各データの変更管理

・　情報システムの運用において、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

３．１６　保守に関する事項

請負者は、本システムにおける「保守計画書」及び「保守手順書」等を作成し、原子力規制庁の承認を受けること。

保守業務においては、以下の内容を考慮すること。

（１）保守業務内容

請負者の保守対象は、本調達のハードウェア、ソフトウェア製品とする。システム基盤を利用する各サブシステムの障害時においては、原子力規制庁、原子力規制庁ネットワーク事業者及び行政ＬＡＮ運用事業者と連携の上、原因解析支援、復旧支援を行うこと。

ア　定常時対応

・　請負者は、「保守作業計画書」及び「保守手順書」に基づき、保守作業の内容や工数などの作業実績状況（本システムの脆弱性への対応状況を含む。）、サービスレベルの達成状況、本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「月次報告書」に取りまとめ提出すること。

・　請負者は、月間の保守実績を評価し、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。

（ア）稼働状態の確認

・　本システムの稼働を良好な状態に維持するため、半年に１回以上の頻度で、定期的に本システムの稼働状態等の確認を行うこと。

・　確認の結果、システムに異常又は異常となる前兆が見られた場合は、担当官に報告するとともに、直ちに「イ　障害発生時対応」に示す障害対応の作業を行うものとする。

（イ）申請書閲覧サブシステム用データの登録（放射線障害防止総合管理システムのみ対象）

・　担当官の指示に従い、光ディスクファイル等の外部記録媒体に記録された申請書閲覧サブシステム用のデータを職員端末上で申請書閲覧サブシステムを用いて、申請者イメージファイルの検索・閲覧ができるようにファイル変換等の作業を行うこと。

（ウ）クローズドＬＡＮ端末にインストールしたアプリケーションソフトウェアの保守（放射線障害防止総合管理システムのみ対象）

「放射線障害防止総合管理システム」について、職員の人事異動やクローズドＬＡＮ端末の故障交換等により、本システムの専用アプリケーションソフトウェアの再インストール等が必要になった場合には、担当官と調整の上、速やかに対応すること。

なお、クローズドＬＡＮ端末の仕様については次の表のとおりである。

項目	品名等
OS	・Microsoft Windows7 Professional 32bit （次期更改までサポート契約が可能であることを確認済み）
CPU	・1.6GHz以上
メモリ	・4GB以上

項目	品名等
HDD	・320GB以上
Officeソフト	・Microsoft Office2010 ・一太郎
Webブラウザ	・Internet Explorer 11
ウイルス対策ソフト	・Symantec End point Protection
その他	・ノート型

イ　障害発生時対応

・ 請負者は、本システムの障害発生時（又は発生が見込まれる時）には、原子力規制庁からの連絡を受け、障害発生時保守作業（原因調査、応急措置、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「保守作業計画書」及び「保守手順書」に基づいて行うこと。

・ 請負者は、本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「障害対応報告書」を作成し、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。

（ア）ハードウェア障害対応

・ 障害の原因が本システムの機器にある場合は、速やかに原因の特定、障害部品の交換を行い、４８時間以内を目標にサービスの復旧を行うこと。

・ ハードウェア障害の復旧作業では、必要に応じて次に示す作業を実施すること。

- ✧ システム停止・起動操作
- ✧ ハードウェア復旧確認
- ✧ ハードウェアの環境設定
- ✧ バックアップの設定作業
- ✧ バックアップデータのリストア
- ✧ システム動作確認

・ 上記作業の他、サービスの復旧にあたり必要となる作業が発生する場合には、担当官の承認を得た上で行うこと。

（イ）ソフトウェア障害対応

・ 障害の原因が本システムの機器に搭載されたＯＳ、ミドルウェアにある場合は、速やかに原因の特定を行い、ソフトウェアメーカ等から対策用パッチ又は対応するバージョンアップ版が提供されているときには、その適用

作業を行うこと。

- ソフトウェアメーカ等から対策用パッチが提供されていないときには、対策案の提示を行うこと。ただし、対策用のパッチを適用するにあたり本システムへの影響の有無について確認し報告すること。また、この場合において、本システムのプログラムに改修が必要な場合は、調査報告書を提出するとともに、その対応方法について担当官と協議を行った上で対応を行うこと。
- ソフトウェア障害の復旧作業では、必要に応じて次に示す作業を実施すること。
    - ✧ システム停止・起動操作
    - ✧ ソフトウェア復旧確認
    - ✧ ソフトウェアの環境設定
    - ✧ バックアップの設定作業
    - ✧ バックアップデータのリストア
    - ✧ システム動作確認
- 上記作業のほか、サービスの復旧にあたり必要となる作業が発生する場合には、担当官の承認を得た上で行うこと。

（ウ）本システム用アプリケーションソフトウェア障害対応

- 障害の原因が本システム用のアプリケーションソフトウェアにある場合は、障害の解析結果を特定した上で、当該アプリケーションを復旧すること。
- 本システム用のアプリケーションソフトウェア障害の復旧作業では、本システムを運用継続するために必要となる改修を実施すること。
- ただし、改修に４８時間以上を要する場合には、本システムを運用継続するための代替策（暫定処置を含む。）の提案すること。
- アプリケーションソフトウェアの迅速性に担保がない等障害対応に支障を来す恐れがあると担当官が判断した場合には、請負者の責任と負担においてアプリケーション開発事業者に再委託の上、作業を実施すること。

（エ）外部システムに起因する障害対応

- 障害発生原因が本システム外のシステム（例えばクローズドＬＡＮネットワークシステム等）にある場合は、外部システム向けに解析結果をまとめ提出すること。
- 外部システム障害でその復旧に４８時間以上を要する場合、本システムを運用継続するための対応策（暫定処置を含む。）を検討して提案すること。
- 外部システム側の障害が復旧した後、システムの正常動作を確認すること。

また、外部システムとの切り分け方法やシステムの正常動作の確認方法について具体的な提案をすること。

ウ　報告書の提出

（ア）　障害対応報告書

障害対応作業後、速やかに、障害内容、障害発生から復旧に至るまでの経過、障害発生原因、対応内容を記載した報告書を提出すること。

（イ）　定期メンテナンス報告書

定期メンテナンスを実施した後速やかに、作業の日時、内容、結果、対応者を記載した報告書を提出すること。

（ウ）　月次報告書

以下に示す項目について、月次で実施した作業の有無、内容等をまとめて報告書を提出すること。

- 障害対応報告
- 定期メンテナンス報告

（エ）　年次報告書

年間の保守作業実績をとりまとめた報告書を提出すること。

エ　保守作業の改善提案

- 請負者は、年度末までに必要に応じて「保守作業計画書」及び「保守手順書」に対する改善提案を行うこと。

オ　引継ぎ

- 請負者は、原子力規制庁が本システムの更改を行う際には、次期のシステム更改における請負業者等に対し、作業経緯、残存課題、設計書等に関する情報提供及び質疑応答等の協力を行うこと。

添付資料：
「放射線源登録管理システム」の庁外データセンター機器の更新に関わるハードウェア及びソフトウェアの要件

① 「放射線源登録管理システム」のハードウェア及びソフトウェアの要件を示す。
② 「放射線源登録管理システム」を構成するハードウェア及びソフトウェア等の最低限必要な要求仕様を定義する。
③ なお、ハードウェア及びソフトウェアは賃貸借保守期間中の保守サポート（ライセンス等）を含めるものとする。
④ 「放射線源登録管理システム」を構成するハードウェア等は１ラック４２ユニット構成に収納できること。

No.	サーバ	システム構成	項目	要求仕様
1	仮想基盤（ホスト）	ハードウェア	CPU	CPU 性能は 2.30GHz 相当以上を有すること。
2				各システムに必要な処理性能を割り当てられることが可能な x86 または x64 と同等のアーキテクチャ CPU を備えること。
3			メモリ	各システムに必要な処理性能を割り当てられることが可能なメモリを備えること。
4				メモリのエラー発生時にハードウェアにて自動的に誤りデータを補正できる機能(ECC 機能等)を有すること。
5				メモリモジュールを最台 24 枚搭載可能であること。
6				768GB 以上のメモリを搭載可能であること。
7			ディスク装置	7.2Krpm 以上の回転速度を有すること。
8				RAID アレイ構成を搭載、ディスク装置の障害時にデータを保持できること。
9				RAID 構成は RAID1 以上とすること。
10				3.5 インチハードディスクが搭載可能であること。
11				2.5 インチハードディスクを最大 10 本搭載可能であること。
12			ＯＳブート専用モジュール	システムボード上に OS の起動を高速化するモジュール（SATA Flash モジュール）が搭載可能であること。

13			光学式ドライブ	OS ブート可能な DVD-ROM 及び CD-ROM の読み込みに対応していること。
14				CD、DVD、Bul-ray ディスクへの書き込みは不可能とすること。
15			LAN インタフェース	1000BASE-T/100BASE-TX/10BASE-T インタフェースを 4 ポート以上有し、10GBASE-T を 2 ポート以上有すること。
16				オンボード LAN ポートを用途に応じて選択できること。
17				LAN ポートを最大 16 ポート以上搭載可能であること。
18				8Gbps 以上の転送速度を有すること。
19			サーバ監視機能	管理コンソールは、故障箇所の実機イメージでの表示が可能であること。
20				ハードウェアの監視やエラー通知が可能であること。
21				監視で取得したサーバ情報の過去のデータとの比較が可能であること。
22				仮想サーバの CPU・メモリ・HDD のリソースを定期的に監視し、しきい値を超えた場合にシステム管理者へ通知可能であること。
23				サーバ異常発生時に、警告灯と連携して光や音で異常を通知可能であること。
24		ソフトウェア	ＯＳ等	RedHatLinux Enterprise7 以上とすること。
25				ウイルス対策を行うこと。
26		その他		システムボード上にモジュールやコンポーネントの異常・故障を通知する LED があること。 故障した DIMM が、システムボード上の DIMM スロットの LED 点灯で特定できること。
27				PCI カード故障をボード上で LED 通知が可能であること。
28				SAS アレイコントローラカードの故障をボード上で LED 通知可能であること。
29				通電されていない状態でも、システムボード上にモジュールやコンポーネントの異常・故障を LED 通知できること。

30				システムボード上から、故障したファンの LED 通知が可能であること。
31				外面でファンの故障予兆を通知可能であること。(CSS ランプで故障予兆の表示ができる)

32	運用管理サーバ	ハードウェア	CPU	CPU 性能は 2.30GHz 相当以上を有すること。
33				各システムに必要な処理性能を割り当てられることが可能な x86 または x64 と同等のアーキテクチャ CPU を備えること。
34			メモリ	各システムに必要な処理性能を割り当てられることが可能なメモリを備えること。
35				メモリのエラー発生時にハードウェアにて自動的に誤りデータを補正できる機能(ECC 機能等)を有すること。
36				メモリモジュールを最台 24 枚搭載可能であること。
37				768GB 以上のメモリを搭載可能であること。
38			ディスク装置	7.2Krpm 以上の回転速度を有すること。
39				RAID アレイ構成を搭載、ディスク装置の障害時にデータを保持できること。
40				RAID 構成は RAID1 以上とすること。
41				3.5 インチハードディスクが搭載可能であること。
42				2.5 インチハードディスクを最大 10 本搭載可能であること。
43			ＯＳブート専用モジュール	システムボード上に OS の起動を高速化するモジュール（SATA Flash モジュール）が搭載可能であること。
44			光学式ドライブ	OS ブート可能な DVD-ROM 及び CD-ROM の読み込みに対応していること。
45				CD、DVD、Bul-ray ディスクへの書き込みは不可能とすること。
46			LAN インタフェース	1000BASE-T/100BASE-TX/10BASE-T インタフェースを 4 ポート以上有し、10GBASE-T を 2 ポート以上有すること。
47				オンボード LAN ポートを用途に応じて選択できること。

48				LAN ポートを最大 16 ポート以上搭載可能であること。
49				8Gbps 以上の転送速度を有すること。
50			サーバ監視機能	・管理コンソールは、故障箇所の実機イメージでの表示が可能であること。
51				・ハードウェアの監視やエラー通知が可能であること。
52				・監視で取得したサーバ情報の過去のデータとの比較が可能であること。
53				・仮想サーバの CPU・メモリ・HDD のリソースを定期的に監視し、しきい値を超えた場合にシステム管理者へ通知可能であること。
54				・サーバ異常発生時に、警告灯と連携して光や音で異常を通知可能であること。
55		ソフトウェア	ＯＳ等	RedHatLinux Enterprise7 以上とすること。
56				ウイルス対策を行うこと。
57		その他		システムボード上にモジュールやコンポーネントの異常・故障を通知する LED があること。 故障した DIMM が、システムボード上の DIMM スロットの LED 点灯で特定できること。
58				PCI カード故障をボード上で LED 通知が可能であること。
59				SAS アレイコントローラカードの故障をボード上で LED 通知可能であること。
60				通電されていない状態でも、システムボード上にモジュールやコンポーネントの異常・故障を LED 通知できること。
61				システムボード上から、故障したファンの LED 通知が可能であること。
62				外面でファンの故障予兆を通知可能であること。 (CSS ランプで故障予兆の表示ができる)
63	ストレージ	ハードウェア	メモリ	停電時にはシステムメモリ上のキャッシュデータを不揮発メモリに退避し、復電時までデータを保護すること。
64				特定のアクセスでキャッシュを占有しないように制限可能なこと。
65			コントローラ	コントローラ数は２つ以上有すること。

66			ホストインタフェース	最大 10Gbit/s（10GBASE-T）での接続が可能であること。
				iSCSI のインタフェースを 4 ポート以上有すること。
67			ディスク装置	同一インチの異なる種類のディスクドライブを同一ドライブエンクロージャー内に混在搭載可能であること。
68				データストア用ディスクとして、3TB 10Krpm(RAID1+0)を有すること。 バックアップ用ディスクとして、3TB 7.2Krpm(RAID6)を有すること。
69			電力消費量	使用頻度の低いディスクドライブに対し、一定期間ディスク回転を停止させ、消費電力を削減する運用が可能であること。
70				ディスク回転の停止設定は GUI と CLI によりおこなえること。
71				回転停止期間のスケジューリングは、RAID グループごとに設定が可能であること。
72				使用しない時間帯はディスクの回転停止に加え、ドライブへの電源供給を停止し、消費電力を削減する機能を有すること。
73			ディスク管理等	予防交換が必要と判断したディスクドライブについて、冗長性を維持した状態でホットスペアディスクドライブへデータを自動コピーし、コピー完了後に自動切替えを行う機能を有すること。
74				高速リビルド機能を有すること。
75				システム稼働中に、RAID グループへディスクドライブを追加し、論理ボリューム（LUN）の新規作成が可能であること。
76				ワイドストライピング機能により、複数の RAID に跨ったボリュームを作成可能なこと。
77				論理ボリュームを仮想化し、それに割り当てる物理ディスクは実際に使用するだけのストレージ容量とすることで、ストレージ容量の効率的な利用と初期投資の抑制が可能であること。
78				VMware が提供する vStorage APIs for Array Integration(VAAI) をサポートしていること。

79		その他	管理機能	日本語による GUI 管理画面を提供すること。
80				運用者に割り当てられる権限（ロール）は６つ以上に細分化が可能なこと。
81				イベントを外部サーバ（syslog サーバ）へ送信することが可能なこと。
82				不審者からのアクセスを考慮し、管理用 GUI へのアクセスや設定変更情報を監査ログとして外部サーバ送信することが可能なこと。

83	ネットワーク情報可視化ソフトウェア	ハードウェア及びソフトウェア	ＣＰＵ	3.6GHz 8Core(Core i7-4790 相当)以上
84			メモリ	8GB DDR3 1600MHz 以上
85			ディスク	250GB(7200rpm,SATA)以上
86			ビデオカード	NVIDIA Geforce GT720(1024MB)以上
87			ＯＳ	RedHatLinux(CentOS)6 系以上
88			基本仕様	センサー、ゲート、アラート情報収集、可視化機能等が稼働するハードウェアを提供すること。各機能が稼働するのに十分なスペックを有すること。可視化機能用のサーバ以外は、同一サーバ筐体上に構成することでもかまわない。
89				いずれのサーバも、IEEE802.3ab に準拠した 1000BASE-T インタフェースを 2 ポート以上有すること。
90				センサー、ゲート、アラート情報収集、可視化機能はソフトウェアで提供され、本機能専用のハードウェアまたは仮想マシンに実装して提供できること。なお、対象となるセンサー数、ゲート数により費用が増大しないこと。
91				ネットワークセグメント間のネットワークトラフィックを送信元／送信先 IP アドレスを元に通信の軌跡で表示できること
92				ネットワークセングメント間のネットワークトラフィックの流量をパケット数、またはデータ量によりリアルタイムに表示できること。
93				セキュリティ製品等から受信したイベント情報（セキュリティアラートログ）から必要情報を抽出・保存し、アラートが発生した内容を元に表示できること。

94				パケットの詳細として以下の内容が可視化ソフトウェアのマップ画面上に表示できること。(パケットが取得された時間、送信元・送信先 IP アドレス、プロトコル、送信元・送信先ポート番号
95				以下のプロトコルが表示できること。(UDP、TCP SYN、TCP SYN/ACK、TCP ACK、TCP、FIN、TCP RST、TCP PUSH、TCP OTHER (TCP の上記以外)、ICMP)
96				センサーでネットワークトラフィックを取り込む方法として「既存ネットワーク機器のポートミラーリング」、「センサーと既存ネットワーク機器の間に設置した TAP で取り出したトラフィック」及び「sFlow (RFC3176)」が利用可能であること。
97				センサーで受信したネットワークトラフィックデータの中から、データ部分を除いたヘッダー部分のみゲートへ送信することによりゲートへのネットワークトラフィック量を圧縮できること。
98				フィルタリングの設定により、以下に関するネットワークトラフィック表示の選択ができること。(送信元 IP アドレスと送信先 IP アドレスの組合せ、プロトコル、送信元ポート番号と送信先ポート番号の組合せ、プロトコルと送信先／送信元ポート番号の組合せ)
99				1 つのネットワークセグメントが 256 個のブロックで表現され、その 1 つのブロックを選択することにより、選択したネットワークの下位ネットワークが表示されること。また、マウス操作により上位ネットワークが描画できること。
100				可視化ソフトウェアで受信したトラフィック情報の 1 パケットずつネットワークオブジェクトとしてマップ画面上に描画し、ネットワークトラフィックの流れ、流量の混み具合が識別できること。
101				ネットワークトラフィックの流量の多寡に従い、軌跡を色分けして表示できること。また、軌跡の高低、太さにより、流量を表示できること。
102				過去に取得した pcap 形式のファイルを入力データとして、オンラインの場合と同様にオフラインでも可視化ソフトウェアのマップ画面上で描画でき

				ること。
103				マップ画面は、マウス操作により 3 次元で動かすことができること。
104				セキュリティ製品等から受信したイベント情報の内容に応じたレベル付けが可能なこと。
105				マップ画面上へレベル付けされたアラートオブジェクトが描画されること。
106				可視化ソフトウェアのマップ画面上で入力として受けたイベント情報（セキュリティアラートログ）が、全イベントまたはセキュリティ製品単位で確認できること。
107				可視化ソフトウェアのマップ画面上に表示されたイベント情報(セキュリティアラートログ)の表示位置（上下)、大きさ、または回転等によって、発生箇所（アラート発生元／発生先)、アラート数やアラート鮮度が識別できること。
108				独自に作成したマップ画面を可視化ソフトウェアに取り込んで、そのマップ画面上にトラフィック情報やイベント情報が描画できること。
109				フィルタリング設定で、以下に関するトラフィックまたはイベント情報の選択ができること。(受信したセキュリティ製品の種類、現在時刻から過去、設定した秒数以内のアラート、指定したアラートレベル以上のアラート、指定したプロトコル（TCP,UDP,ICMP,その他)、指定したアラートメッセージ、送信元 IP アドレスと送信先 IP アドレスの組合せ、送信元ポート番号と送信先ポート番号の組合せ)

110	監視アプライアンス	ハードウェア	インタフェース	eSATA （SATA II)のポートを１つ以上有し 、10/100/1000Base-T での接続が可能なこと。
111			内部ストレージ	256GB 以上を有すること。
112		基本仕様	監視機能	Ping 監視が可能であること。
113				VMware 環境の自動監視が可能なこと。

114			グラフィカル表示機能	Web によるステータス表示と監視設定が可能なこと。
115				リアルタイムグラフ表示、グラフ一覧表示が可能なこと。
116			障害検知、通知機能	障害項目、イベント履歴の表示が可能であること。
117				メール通知が可能であること。
118			その他	監視設定のバックアップ機能を有すること。

119	バックアップ装置	ハードウェア	筐体・構成	1TB カートリッジ（RDX）を８本以上搭載できること。
120			インタフェース	最大 10Gbit/s（10GBASE-T）での接続が可能であること。
121				iSCSI のインタフェースを有すること。
122		ソフトウェア	バックアップ	仮想サーバ（ゲスト）のバックアップに対応できること。

123	ファイアウォール	ハードウェア	スループット	ファイアウォールスループットは最大 2.5 Gbps が可能なこと。
124				DMZ/LAN とセグメントを分割、公開サーバへのアクセス許可や冗長等の設定が可能なこと。
125		その他		GUI 管理画面を提供すること。
126				UTM 機能を有すること。
127				高可用性（HA）構成に対応できること。

128	スイッチングハブ	ハードウェア	構成	冗長構成とすること。
129			インタフェース	10/100/1000Base-T での接続が可能で２４ポートを有すること。
130				1000BASE-T/10GBASE-T ポートに６ポート以上拡張が可能なこと。
131			基本仕様	スタック構成が可能であること。
132				標準 MIB による監視が可能であること。

133	ラックコンソール	ハードウェア	基本仕様	KVM スイッチを本装置後部に 1 台搭載すること。ホットキーによりサーバを切り替えられること。
134				17 インチ TFT（SXGA）モニタを搭載すること。
135				OADG 準拠の 109A 日本語キーボードを搭載するこ

				と。
136				ポインティングデバイス（タッチパッド）を搭載すること。

137	保守用機器	ハードウェア及びソフトウェア	請負者用ＰＣ端末 請負者用VPN装置 請負者用終端装置	・請負者が庁外データセンターに接続しリモート環境で保守可能な機器及びソフトウェアを検討すること。 ・ＰＣ端末生体認証等のアクセス制限をかけていること。 ・ウイルス対策を行うこと。 ・設置場所は保守関係者のみが入室可能なセキュリティ認証（認証番号やカードキー等）を設けた執務環境とすること。