平成３１～３５年度
緊急時対策支援システムの更改及び運用・保守業務
（機器及びメインシステム）
調達仕様書

平成３１年４月

原子力規制委員会原子力規制庁

目次

１．調達件名 1
２．調達の背景 1
３．目的及び期待する効果 1
４．業務・情報システムの概要 1
５．契約期間 2
６．作業スケジュール 3
７．調達案件及び関連調達案件の調達単位、調達の方式等に関する事項 3
７.１ 調達案件及び関連する調達案件の調達単位、調達の方式、実施時期 3
７.２ 調達案件間の入札制限 3
８．作業内容 4
８.１ 設計・開発 4
８.２ 運用 6
８.３ 保守 8
８.４ ODB 登録用シートの提出に係るその他の記載内容 10
９．納品成果物及び期限 11
９.１ 納入成果物一覧と期限 11
９.２ 納品方法 12
９.３ 納品先 13
１０．満たすべき要件に関する事項 13
１１．作業体制及び作業方法 14
１１.１ 作業実施体制 14
１１.２ 作業要員に求める資格等の要件 16
１１.３ 作業場所 17
１１.４ 作業場所の管理に関する要領 17
１２．作業の実施に当たっての遵守事項 17
１２.１ 機密保持、資料の取扱い 17
１２.２ 遵守する法令等 17
１３．成果物の取扱いに関する事項 19
１３.１ 知的財産権の帰属 19
１３.２ 瑕疵担保責任 19
１３.３ 検収 19
１４．入札参加資格に関する事項 20
１４.１ 入札参加要件 20
１４.２ 入札制限 21
１５．再委託に関する事項 21
１５.１ 再委託の制限及び再委託を認める場合の条件 21
１５.２ 承認手続 21
１５.３ 再委託先の契約違反等 21
１６．その他特記事項 22

１．調達件名

平成３１～３５年度緊急時対策支援システムの更改及び運用・保守業務（機器及びメインシステム）

２．調達の背景

緊急時対策支援システム（Emergency Response Support System：以下、「ＥＲＳＳ」という。）は、災害対策基本法（昭和３６年法律第２２３号）第３４条第１項の規定に基づく防災基本計画（平成２９年４月 中央防災会議）、原子力規制委員会防災業務計画(平成２４年９月１９日原子力規制委員会決定、平成３０年１月３１日修正)及び原子力災害対策マニュアル（平成２４年１０月１９日原子力防災会議幹事会、平成２９年１２月２６日一部改訂)を基に、原子力に関わる緊急事態が発生した場合に、官邸、原子力規制委員会原子力規制庁（以下、「原子力規制庁」という。）緊急時対応センター（以下、「ＥＲＣ」という。）、各地の緊急事態応急対策等拠点施設（オフサイトセンター：以下、「ＯＦＣ」という。）などに、原子力施設の状態等の情報を提供するものとして、原子力規制庁にて整備・運用しているシステムである。

現在運用しているＥＲＳＳ（以下、「現行システム」という。）は平成２６年度より運用を開始したものであり、サーバ等機器のリース期間や保守期限切れに伴う機器等の入れ替えが必要となっている。

３．目的及び期待する効果

本調達の目的を以下に記す。

- システムのライフサイクルを考慮し、また、新規制基準（原子炉等の設計を審査するための新しい基準）等に対応するため、２０２０年度を目途に現行システムを基に、仕様や環境を改良・更新したシステム（以下、「次期システム」という。）へ移行する
- 「世界最先端ＩＴ国家創造宣言」を受け、現行業務の見直しやシステム基盤の関連費用の見直しを行うことにより、更なる業務効率化及びコスト削減を実現する
- 大規模災害時等における行政運営の継続性を確保する

本調達でＥＲＳＳを更改し、運用を継続することで、原子力災害時において必要となる情報を迅速に提供できる環境が維持され、原子力防災対策における有効な支援となることが期待される。

４．業務・情報システムの概要

ＥＲＳＳは、原子力に係る緊急事態（原子力発電所等で重大事故もしくは重大事故に発展する可能性のある事故等、原子力発電所等の立地地区で大規模地震等の災害等）が発生した場合に、ＥＲＣや各地のＯＦＣなどに、主として以下の情報を提供するシステムである。

- 原子力施設の状態を示す情報(原子炉ならば圧力、温度、水位等)
- 原子炉事故の進展予測（燃料被覆管破損や炉心溶融に至る時間等の推定）に資する情報

加えて、軽水炉事故に関する訓練や学習での利用を目的とした、原子炉事故解析により事故時の原子力施設の状態を示す模擬情報を作成、配信する機能を有する。

ＥＲＳＳは複数のサブシステムから構成されるシステムであり、その内、ＥＲＳＳの主機能に係るものは以下の３つのサブシステムである。他には、バックアップやサーバ監視等、ＥＲＳＳのシステム保全に係るサブシステムがある。

・原子力発電所等原子力施設（プラント）から常時伝送されるプラントの状況判断に必要な情報（以下、「プラントデータ」という。）を収集し、データベースに格納する「プラントデータ収集システム」
・収集したプラントデータ等の原子力施設に関する情報をＷｅｂアプリケーションにてＥＲＣやＯＦＣ等に提供する「プラント情報表示システム（Information Collection System：以下、「ＩＣＳ」という。）」
・実在する軽水炉を対象に、シミュレータを使って原子炉事故を計算し、結果を模擬プラントデータとして配信する「訓練データ配信システム（Training data Delivery System：以下、「ＴＤＳ」という。）」

ＴＤＳは、現行システムの二つのサブシステム「解析予測システム」、「模擬データ発生システム」を見直し、次期システムにおいて一つのサブシステムとして新たに開発するものである。ＴＤＳのアプリケーションの開発と運用・保守は別途業務で行うものとし、本業務では、ＴＤＳを運用するハードウェア、ミドルウェアの調達とその運用・保守を行うものとする。

次期システムからＴＤＳアプリケーション関連を除いた残りを「メインシステム」と定義する。

本業務の調達及び運用保守の範囲は、次期システム（ＴＤＳ含む）のハードウェア、ミドルウェア及びメインシステム（開発含む）である。

なお、本業務で調達するハードウェア、ミドルウェア及び原子力規制庁に所有権があるアプリケーションを除くソフトウェアについては、賃貸借契約とする。

以降、特に断りのない限り、ＥＲＳＳと表記する場合は次期システム全体を示すものとし、本システムと表記する場合は次期システムにおける本業務の調達範囲内を示すものとする。

５．契約期間

（１） 契約期間

自：契約締結日

至：２０２４年3月３１日

（２） 賃貸借期間

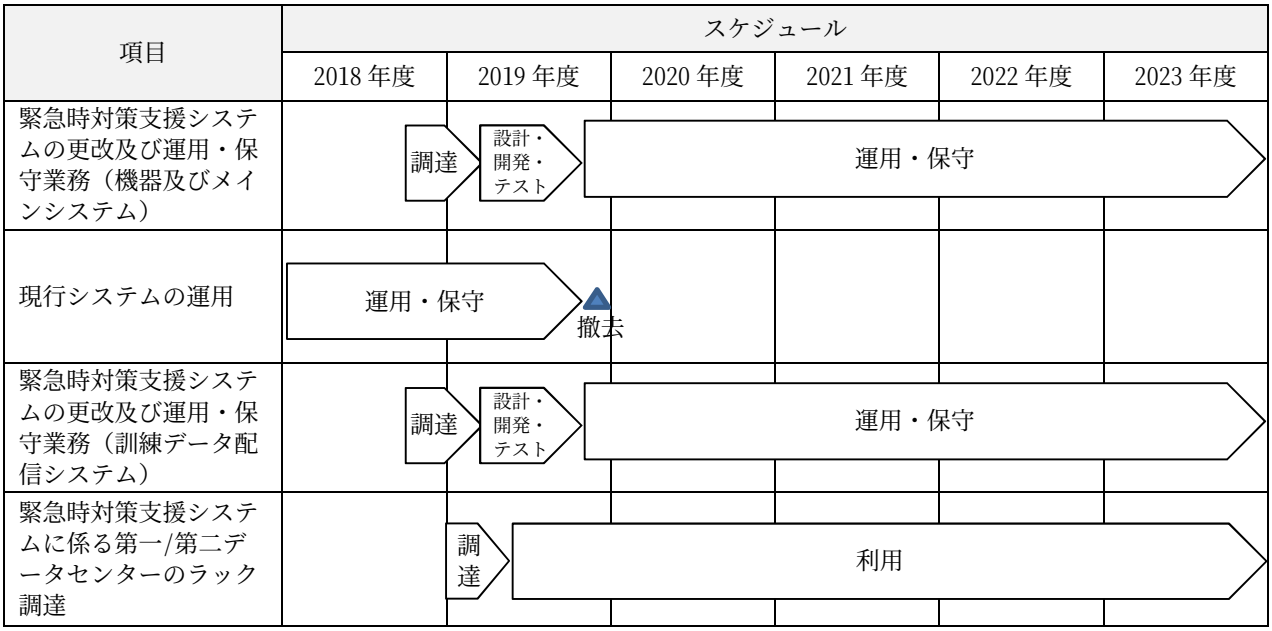
自：２０２０年4月１日

至：２０２４年3月３１日

６．作業スケジュール

想定する作業スケジュールを「表 1 想定作業スケジュール」に示す。合わせて本調達に関連する調達案件等のスケジュールも示す。

表 1 想定作業スケジュール



７．調達案件及び関連調達案件の調達単位、調達の方式等に関する事項.

７.１ 調達案件及び関連する調達案件の調達単位、調達の方式、実施時期

本調達に関連する調達案件の調達単位、調達方式、実施時期を「表 2 関連調達案件一覧」に示す。

表 2 関連調達案件一覧

No.	調達案件名	調達の方式	調達実施時期	補足
1	平成３１～３５年度緊急時対策支援システムの更改及び運用・保守業務（機器及びメインシステム）	一般競争入札（総合評価方式）	2019 年 4 月	本業務
2	平成３１～３５年度緊急時対策支援システムの更改及び運用・保守業務（訓練データ配信システム）	一般競争入札（総合評価方式）	2019 年 4 月	
3	平成３１～３５年度緊急時対策支援システムに係る第一データセンターのラックの賃借	随意契約予定	2019 年 8 月	
4	平成３１～３５年度緊急時対策支援システムに係る第二データセンターのラックの賃借	随意契約予定	2019 年 8 月	

７.２ 調達案件間の入札制限

「表 2 関連調達案件一覧」に記載する調達案件間において、入札制限は設けない。

８．作業内容

８．１ 設計・開発

（１） 設計・開発実施計画書等の作成

ア　受注者は、原子力規制庁の指示に基づき、関連調達受注者と調整の上、設計・開発実施計画書及び設計・開発実施要領の案を作成し、原子力規制庁の承認を受けること。

（２） 設計

ア　受注者は、「別紙　要件定義書」を満たすための基本設計及び詳細設計を行い、成果物について原子力規制庁の承認を受けること。

イ　基本設計及び詳細設計を通じ、要件定義書に大きな変更が発生した場合には、要件定義書の該当箇所を修正し要件定義書の改訂版として原子力規制庁の承認を得ること。

ウ　受注者は、現行システムから次期システムへの移行の方法、環境、ツール、段取り等を記載した移行計画書を作成し、原子力規制庁の承認を受けること。

エ　受注者は、本システムの次期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・保守作業計画の案を作成し、原子力規制庁の承認を得ること。

オ　受注者は、運用設計及び保守設計を行い、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作業計画の案を作成し、原子力規制庁の確認を受けること。

（３） 開発・テスト

ア　受注者は、開発に当たり、アプリケーションプログラムの開発又は保守を効率的に実施するため、プログラミング等のルールを定めた開発標準（標準コーディング規約、セキュアコーディング規約等）を定め、原子力規制庁の確認を受けること。

イ　受注者は、開発に当たり、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、標準コーディング規約遵守の確認、ソースコードの検査、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）をセキュリティルールとして定め、原子力規制庁の確認を受けること。

ウ　受注者は、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、原子力規制庁の承認を受けること。

エ　受注者は、設計工程の成果物及びテスト計画書に基づき、アプリケーションプログラムの開発、調達した機器の導入、テストを行うこと。

オ　受注者は、テスト計画書に基づき、各テストの実施状況を原子力規制庁に報告すること。

カ　データセンター等での機器設置及び設定は、機器設置図面、機器搬入計画書及び機器設定手順書を作成し、原子力規制庁の承認を得たうえで作業を行うこと。作業結果については、機器設定作業報告書を作成し原子力規制庁の承認を得ること。

（４） 受入テスト支援

ア　受注者は、原子力規制庁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　受注者は、原子力規制庁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　受注者は、原子力規制庁の指示に基づき、原子力規制庁職員以外のＥＲＳＳ利用者にて受入テストを実施する場合を含め、テスト計画書作成の支援を行うこと。

（５） 情報システムの移行

ア　受注者は、原子力規制庁の移行判定を受けて、移行計画書に基づく移行作業を行うこと。

イ　受注者は、移行に関する手順書を作成し、原子力規制庁の承認を受けること。

（６） 引継ぎ

ア　受注者は、本契約の終了後に他の運用事業者が本システムの運用・保守を受注した場合には、当該事業者に対し、作業経緯、残存課題等についての引継ぎを行うこと。

（７） ODB 登録用シートの提出

ア　受注者は、次に掲げる事項について記載したＯＤＢ登録用シートを、設計・開発実施要領において定める時期に提出すること。

① 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

② 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

③ 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

④ 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

⑤ 外部サービスの管理

- 情報システムを構成するクラウドコンピューティングサービス等の外部サービスの外部サービス利用形態、使用期間等

⑥ 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

⑦ 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

⑧ 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

⑨ 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

⑩ 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

８.２ 運用

（１） 中長期運用・保守作業計画の作成支援

ア 受注者は、原子力規制庁が「中長期運用・保守作業計画」を確定するに当たり、情報システムの構成やライフサイクルを通じた運用業務及び保守作業の内容について、計画案の妥当性の確認、情報提供等の支援を行うこと。

（２） 運用計画及び運用実施要領の作成支援

ア 受注者は、原子力規制庁が「運用計画書」及び「運用実施要領」を作成するに当たり、具体的な作業内容や実施時間、実施サイクル等に関する資料作成等の支援を行うこと。

（３） 定常時対応

ア 受注者は、「要件定義書」の運用要件に示す定常時運用業務（システム操作、問合せ対応等）を行うこと。具体的な実施内容・手順は運用計画書に基づいて行うこと。

イ 受注者は、運用計画及び運用実施要領に基づき、運用業務の内容や工数などの作業実績状況、サービスレベルの達成状況、情報システムの構成と運転状況（情報セキュリティ監視状況を含む。）、情報システムの定期点検状況、情報システムの利用者サポート、教育・訓練状況、リスク・課題の把握・対応状況について運用報告書を取りまとめること。

ウ 受注者は、運用実績を評価し、性能及び可用性が要件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。また運用報告書の内容について、運用会議等でその内容を報告すること。

エ 受注者は、ソフトウェア製品の保守の実施において、ソフトウェア製品の構成に変更が生じる場合には、原子力規制庁にその旨を報告し、確認を受けること。

（４） 障害発生時対応

ア　受注者は、本システムの障害発生時（又は発生が見込まれる時）には、速やかに原子力規制庁に連絡するとともに、その緊急度及び影響度を判断のうえ、「要件定義書」の運用要件に示す障害発生時運用業務（障害受付、障害発生箇所の切り分け等）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・手順は運用計画書及び運用実施要領に基づいて行うこと。

イ　受注者は、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、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。

ウ　受注者は、大規模災害等の発災時には、原子力規制庁の指示を受けて、情報システム運用継続計画に基づく運用業務を実施すること。

（５） 情報システムの現況確認支援

ア　受注者は、年１回、原子力規制庁の指示に基づき、ＯＤＢ格納データと情報システムの現況との突合・確認（以下、「現況確認」という。）を支援すること。

イ　受注者は、現況確認の結果、ＯＤＢの格納データと情報システムの現況との間の差異がみられる場合は、運用実施要領に定める変更管理方法に従い、差異を解消すること。

ウ　受注者は、現況確認の結果、ライセンス許諾条件に合致しない状況が認められる場合は、当該条件への適合可否、条件等を調査のうえ、原子力規制庁に報告すること。

エ　受注者は、現況確認の結果、サポート切れのソフトウェア製品の使用が明らかとなった場合は、当該製品の更新の可否、更新した場合の影響の有無等を調査のうえ、原子力規制庁に報告すること。

（６） 運用作業の改善提案

ア　受注者は、毎年度末までに、年間の運用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」、「運用計画書」、及び「運用実施要領」に対する改善提案を行うこと。

（７） 引継ぎ

ア　受注者は、原子力規制庁が本システムの更改を行う際には、次期の情報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。

イ　受注者は、本システムの運用業務契約の終了後に他の運用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。

（８） 運用環境の準備

ア　受注者は、本システムの運用を行うための運用環境（運用端末、作業場所、ネットワーク、電話回線及び各種什器等）等について、必要性がある場合は受注者の負担において準備すること。

（9） ODB 登録用シートの提出

ア　受注者は、次に掲げる事項について記載したＯＤＢ登録用シートを、運用実施要領において定める時期に提出すること。

① 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

② 作業実績等の管理

- 情報システムの運用中に取りまとめた作業実績、リスク、課題及び障害事由

8.3 保守

（1） 中長期運用・保守作業計画の作成支援

ア　受注者は、原子力規制庁が「中長期運用・保守作業計画」を確定するに当たり、情報システムの構成やライフサイクルを通じた運用業務及び保守作業の内容について、計画案の妥当性の確認、情報提供等の支援を行うこと。

（2） 保守計画及び保守実施要領の作成支援

ア　受注者は、原子力規制庁が「保守作業計画書」及び「保守実施要領」を作成するに当たり、具体的な作業内容や実施時間、実施サイクル等に関する資料作成等の支援を行うこと。

（3） 定常時対応

ア　受注者は、「要件定義書」の保守要件に示す定常時保守作業（定期点検、不具合受付等）を行うこと。具体的な実施内容・手順は保守作業計画書に基づいて行うこと。

イ　受注者は、保守作業計画及び保守実施要領に基づき、保守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・対応状況について保守作業報告書を取りまとめること。

ウ　受注者は、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。また保守作業報告書の内容について、運用会議等でその内容を報告すること。

（4） 障害発生時対応

ア　受注者は、本システムの障害発生時（又は発生が見込まれる時）には、速やかに原子力規制庁に連絡するとともに、その緊急度及び影響度を判断のうえ、「要件定義書」の保守要件に示す障害発生時保守業務（関連事業者への連絡、復旧確認、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実施要領に基づいて行うこと。

イ　受注者は、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、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。

ウ　受注者は、大規模災害等の発災時には、原子力規制庁の指示を受けて、情報システム運用継続計画に基づく保守業務を実施すること。

（５）　情報システムの現況確認支援

ア　受注者は、年１回、原子力規制庁の指示に基づき、ＯＤＢ格納データと情報システムの現況との突合・確認を支援すること。

（６）　保守作業の改善提案

ア　受注者は、毎年度末までに、年間の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」、「保守作業計画書」及び「保守実施要領」に対する改善提案を行うこと。

（７）　引継ぎ

ア　受注者は、原子力規制庁が本システムの更改を行う際には、次期の情報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。

イ　受注者は、本システムの保守業務契約の終了後に他の保守事業者が本システムの保守を受注した場合には、次期保守事業者に対し、作業経緯、残存課題等についての引継ぎを行うこと。

（８）　保守環境の準備

ア　受注者は、本システムの保守を行うための保守環境（保守端末、作業場所、ネットワーク、電話回線及び各種什器等）等について、必要性がある場合は受注者の負担において準備すること。

（９）　ODB 登録用シートの提出

ア　受注者は、次に掲げる事項について記載したＯＤＢ登録用シートを、保守実施要領において定める時期に提出すること。

① 各データの変更管理

- 情報システムの保守において、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

② 作業実績等の管理

- 情報システムの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

８.４ ODB 登録用シートの提出に係るその他の記載内容

（１） ODB 登録用シートの提出

ア　受注者は、原子力規制庁が指定する区分に基づき契約金額の内訳を記載した ODB 登録用シートを契約締結後速やかに提出すること。

イ　受注者は、原子力規制庁から求められた場合は、スケジュールや工数等の計画地及び実績値について記載した ODB 登録用シートを提出すること。

９．納品成果物及び期限

９．１ 納入成果物一覧と期限

本調達の成果物とその納入期限は「表 3 納入成果物及び納入期限」のとおりとする。

表 3 納入成果物及び納入期限

No	成果物名	内容及び納品数量	納入期日	補足
1	設計・開発実施計画書	紙（正・副）及び電子媒体	契約締結後 2 週間以内	
2	設計・開発実施要領	紙（正・副）及び電子媒体	契約締結後 2 週間以内	
3	設計･開発実施要領に基づく管理資料	紙（正・副）及び電子媒体	契約締結後 2 週間以内	
4	打ち合わせ議事録	紙（正・副）及び電子媒体	打ち合わせ後 1 週間以内	
5	ODB 登録用シート	紙（正・副）及び電子媒体	別途原子力規制庁の指示する期日	
6	標準コーディング規約	紙（正・副）及び電子媒体	契約締結後 2 週間以内	
7	セキュリティルール（※）	紙（正・副）及び電子媒体	契約締結後 2 週間以内	
8	外部（基本）設計書	紙（正・副）及び電子媒体	設計構築完了後遅滞なく	
9	内部（詳細）設計書	紙（正・副）及び電子媒体	設計構築完了後遅滞なく	
10	ソースコード一式	電子媒体	設計構築完了後遅滞なく	
11	実行プログラム一式	電子媒体	設計構築完了後遅滞なく	
12	テスト計画書	紙（正・副）及び電子媒体	テスト開始 2 週間前まで	
13	単体テスト結果報告書	紙（正・副）及び電子媒体	テスト終了後 1 週間以内	
14	結合テスト結果報告書	紙（正・副）及び電子媒体	テスト終了後 1 週間以内	
15	総合テスト結果報告書	紙（正・副）及び電子媒体	テスト終了後 1 週間以内	
16	脆弱性検査結果報告書	紙（正・副）及び電子媒体	脆弱性検査終了後 1 週間以内	
17	テストデータ	電子媒体	テスト終了後 1 週間以内	
18	移行計画書	紙（正・副）及び電子媒体	移行実施 2 週間前まで	
19	移行手順書	紙（正・副）及び電子媒体	移行実施 2 週間前まで	
20	移行結果報告書	紙（正・副）及び電子媒体	移行終了後 1 週間以内	
21	操作手順書	紙（正・副）及び電子媒体	運用保守開始後遅滞なく	
22	研修用資料	紙（正・副）及び電子媒体	運用保守開始後遅滞なく	
23	中長期運用・保守作業計画（案）	紙（正・副）及び電子媒体	運用保守開始 2 週間前まで	
24	運用計画書（案）	紙（正・副）及び電子媒体	運用開始 2 週間前まで	
25	保守計画書（案）	紙（正・副）及び電子媒体	保守開始 2 週間前まで	
26	運用実施要領（案）	紙（正・副）及び電子媒体	運用開始 2 週間前まで	
27	保守実施要領（案）	紙（正・副）及び電子媒体	保守開始 2 週間前まで	
28	運用実施要領に基づく管理資料	紙（正・副）及び電子媒体	運用開始 2 週間前まで	
29	要件定義書（改定案）	紙（正・副）及び電子媒体	設計構築完了後遅滞なく	
30	ソフトウェア製品一式	電子媒体	運用開始後遅滞なく	

No	成果物名	内容及び納品数量	納入期日	補足
31	ソフトウェア･ハードウェア構成表	紙（正・副）及び電子媒体	設計構築完了後遅滞なく	
32	ライセンス関係資料	紙（正・副）及び電子媒体	設計構築完了後遅滞なく	
33	導入機器及びサービス一式	紙（正・副）及び電子媒体	設計構築完了後遅滞なく	
34	機器設置図面	紙（正・副）及び電子媒体	機器搬入実施 2 週間前まで	
35	機器搬入計画書	紙（正・副）及び電子媒体	導入搬入 2 週間前まで	
36	機器設定作業手順書	紙（正・副）及び電子媒体	機器設定 2 週間前まで	
37	機器設定作業報告書	紙（正・副）及び電子媒体	機器設定後１週間以内	
38	運用報告書（月次）	紙（正・副）及び電子媒体	運用開始後毎月翌月末まで（ただし、最終年度の３月分は３月末まで）	
39	運用報告書（年次）	紙（正・副）及び電子媒体	運用開始後毎年度末	
40	保守報告書（月次）	紙（正・副）及び電子媒体	保守開始後毎月翌月末まで（ただし、最終年度の３月分は３月末まで）	
41	保守報告書（年次）	紙（正・副）及び電子媒体	保守開始後毎年度末	
42	定期点検結果報告書	紙（正・副）及び電子媒体	定期点検後２週間以内	
43	保守作業の改善提案書	紙（正・副）及び電子媒体	保守開始後毎年度末	
44	保守計画の改定案	紙（正・副）及び電子媒体	保守開始後毎年度末	
45	外部（基本）設計書及び内部（詳細）設計書（保守運用終了時点の実装内容を反映したもの）	紙（正・副）及び電子媒体	保守運用期間満了時	

※ セキュリティルールとは、「８．１ （３） 開発・テスト」に記載されているとおり、情報セキュリティ確保のためのルール順守や成果物の確認方法を定めたものを指す。

９.２ 納品方法

（１） 提出物は、全て日本語で作成すること。

（２） 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。

（３） 情報処理に関する用語の表記については、日本工業規格(JIS)の規定を参考にすること。

（４） 提出物は紙媒体及び電子媒体により作成し、原子力規制庁から特別に示す場合を除き、紙媒体２部（正・副）及び電子媒体１部を納品すること。

（５） 紙媒体による納品について、用紙のサイズは、原則として日本工業規格 A 列 4 番とするが、必要に応じて日本工業規格 A 列 3 番を使用すること。

（６） 電子媒体による納品について、PDF、WORD、EXCEL、POWER POINT 等のファイル形式で作成し、DVD-R 等の媒体に格納して納品すること。

（７） 納品後原子力規制庁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。

（８） 提出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。
（９） 提出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、提出物の情報セキュリティの確保に留意すること。
（１０） 電子媒体により納品する場合は、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、提出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。
（１１） 運用と保守に関する提出物の内容が密接に係る場合には、１冊に包含してもよい。

９.３ 納品先

東京都港区六本木１ 丁目９ 番９ 号 六本木ファーストビル
原子力規制庁　長官官房総務課情報システム室
なお、詳細については、別途当原子力規制庁担当職員の指示に従うこと。

１０. 満たすべき要件に関する事項

当該調達案件の業務の実施に当たっては、「別紙 要件定義書」の各要件を満たすこと。

１１．作業体制及び作業方法

１１.１ 作業実施体制

（１） 全体体制

プロジェクトの推進体制及び本件受注者に求める作業実施体制は次の図及び表のとおりである。なお、受注者の情報セキュリティ対策の管理体制については、「別紙　要件定義書」のセキュリティ要件を参照のこと。

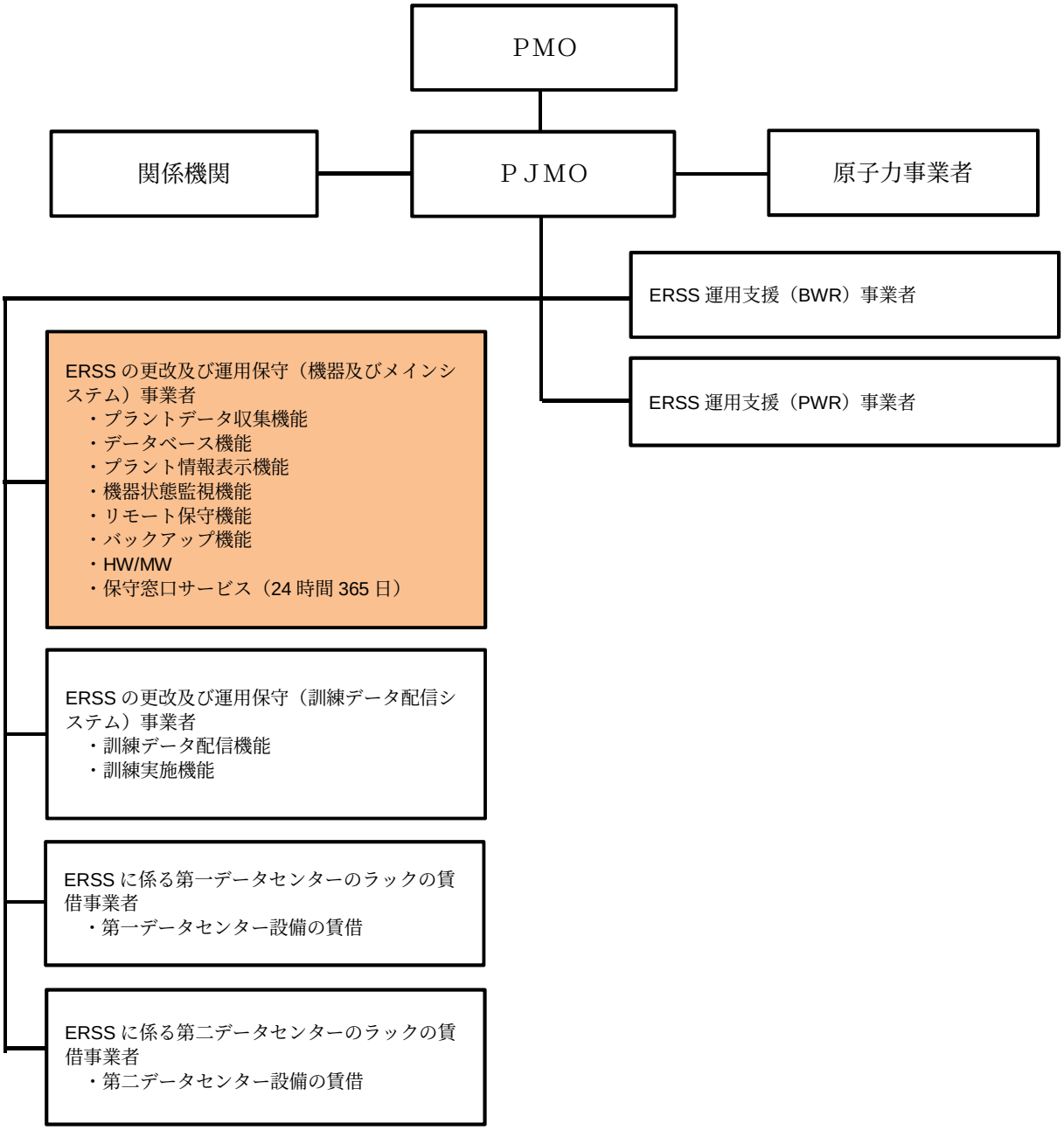


図 1　全体体制図

表４　全体体制における構成メンバーと役割・責任

No.	構成メンバー	役割・責任
1	プロジェクト推進責任者 長官官房総務課　課長	・　統括責任 ・　ＰＭＯへの報告 ・　システム監査の実施 ・　自己点検　等
2	環境省ＣＩＯ補佐官	・　技術支援・助言 ・　要件定義及び調達仕様書の妥当性確認等
3	制度所管部門管理者 長官官房総務課　課長	・　政策目的の明確化 ・　法令改正の情報提供 ・　コンプライアンスチェック　等
4	業務実施部門管理者 長官官房総務課　課長	・　業務の見直し ・　業務の定着 ・　業務の運営と改善　等
5	情報システム部門管理者 長官官房総務課　情報システム室　管理官	・　プロジェクトの推進支援 ・　他情報システムとの調整　等
6	府省内の他のＰＪＭＯのプロジェクト推進責任者	・　府省内で連携する必要のあるプロジェクト間の調整　等
7	その他構成員	・　要件定義のとりまとめ、調達仕様書の作成 ・　調達手続 ・　情報セキュリティ担当　等
8	原子力事業者	・　原子力施設からのデータ伝送に係る仕様の確定 ・　データ伝送に係る通信設備の接続調整
9	ERSS の更改及び運用保守（機器及びメインシステム）事業者（本調達受注者）	・　次期システムに係る機器の導入と賃借 ・　メインシステムの更改と移行 ・　関連調達業務との調整（HW/MW の設定等） ・　次期システムにおける機器及びメインシステムに係る運用と保守
10	ERSS の更改及び運用保守（訓練データ配信システム）事業者	・　訓練データ配信システムの更改と移行 ・　次期システムにおける訓練データ配信システムの運用と保守
11	ERSS に係る第一データセンターの賃借事業者	・　次期システムで使用する第一データセンター設備の初期設定と賃借
12	ERSS に係る第二データセンターの賃借事業者	・　次期システムで使用する第二データセンター設備の初期設定と賃借
13	ERSS 運用支援（BWR）事業者	・　緊急時におけるＥＲＳＳ運用支援 ・　事故進展予測（ＢＷＲ）関連に係るシステムの定期運用点検 ・　事故進展予測（ＢＷＲ）関連に係るドキュメントの整備
14	ERSS 運用支援（PWR）事業者	・　緊急時におけるＥＲＳＳ運用支援 ・　事故進展予測（ＰＷＲ）関連に係るシステムの定期運用点検 ・　事故進展予測（ＰＷＲ）関連に係るドキュメントの整備

（２）　受注者体制

プロジェクトの推進体制及び本件受注者に求める作業実施体制は「表５作業実施体制」のとおりである。なお、受注者内のチーム編成については想定であり、受注者決定後に協議の上、

見直しを行う。また、受注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。情報セキュリティ対策の管理体制の要件は、「別紙　要件定義書」を参照すること。

表 5 作業実施体制

No.	組織又は要員	役割
1	受注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。 ・ 常時、原子力規制庁からの連絡を行える状態(電話等による担当者への指示を含む)にすること。ただし、原子力規制庁の了承を得て、各担当リーダが一時的代理として対応することができる。 ・ 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。
2	受注者における遂行責任者補佐	・ 遂行責任者を補佐する
3	インフラ構築担当チーム	・ 本システムのインフラ構築を担当。
4	インフラ構築担当チームリーダ	・ インフラ構築担当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。 ・ インフラ構築作業期間中は専任でこれに当たるものとする。 ・ チームメンバ約 10 人につき 1 名の割合でサブリーダを配置する。サブリーダの要件はチームリーダと同等とする。
5	機能構築担当チーム	・ 本システムの機能構築を担当。
6	機能構築担当チームリーダ	・ 機能構築担当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。 ・ 機能構築作業期間中は専任でこれに当たるものとする。 ・ チームメンバ約 10 人につき 1 名の割合でサブリーダを配置する。サブリーダの要件はチームリーダと同等とする。

１１．２ 作業要員に求める資格等の要件

（1） 遂行責任者は、特定非営利活動法人 日本プロジェクトマネジメント協会の「プロジェクトマネジメント・スペシャリスト（PMS）」、PMI（Project Management Institute）の「PMP」資格、独立行政法人情報処理推進機構（IPA）の「プロジェクトマネージャ」資格のいずれかを取得していること。

（2） 遂行責任者又は遂行責任者補佐は、本システムと同規模程度のシステムの導入の責任者としての経験を有すること。

（3） チームリーダ全員は、本システムと同規模のシステム設計・開発又はシステム導入等の実務経験を有すること。

（４） 各チームに最低一人は、情報処理技術者試験の資格である高度情報処理技術者（システムアーキテクト、ネットワークスペシャリスト及びデータベーススペシャリストのいずれか）の資格を有する、又はこれと同等の能力がある者を含めること。

１１．３ 作業場所

作業については以下の場所で行うこと。

（１） 統合原子力防災ネットワーク第一・第二データセンター内

（２） 原子力規制庁本庁舎内

（３） 受注者の作業場所

（４） その他原子力規制庁が指定する場所

１１．４ 作業の管理に関する要領

（１） 受注者は、原子力規制庁が承認した設計・開発実施要領に基づき、設計・開発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。

（２） 受注者は、原子力規制庁が承認した運用実施要領に基づき、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。

（３） 受注者は、原子力規制庁が承認した保守実施要領に基づき、保守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。

１２．作業の実施に当たっての遵守事項

１２．１ 機密保持、資料の取扱い

（１） 受注者は、本契約による作業の一切について秘密の保持に留意し、漏えい防止の責任を負うものとする。

（２） 受注者は、本契約終了後においても前項の責任を負うものとする。

（３） 受注者は、原子力規制庁が貸出した資料等については、充分な注意を払い、紛失または滅失しないよう万全の措置をとらなければならない。

１２．２ 遵守する法令等

（１） 法令等の遵守

当該調達案件の業務遂行に当たっては、民法(明治２９年４月２７日法律第８９号)、刑法(明治４０年法律第４５号)、著作権法(昭和４５年５月６日法律第４８号)、不正アクセス行為の禁止等に関する法律(平成１１年８月１３日法律第１２８号)、行政機関の保有する個人情報の保護に関する法律(平成１５年５月３０日法律第５８号)、商法(明治３２年３月９日法律第４８号)、私的独占の禁止及び公正取引の確保に関する法律(昭和２２年４月１４日法律第５４号)等を遵守し履行すること。

（２） その他文書、標準への準拠

① 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、原子力規制庁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。

② 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、原子力規制庁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。

③ 標準ガイドライン

- 当該調達案件の業務遂行に当たっては、「デジタル・ガバメント推進標準ガイドライン」(平成３１年２月２５日各府省情報化統括責任者（ＣＩＯ）連絡会議決定)に準拠して作業を行うこと。

  デジタル・ガバメント推進標準ガイドライン
  https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_20190225.pdf

１３．成果物の取扱いに関する事項

１３.１ 知的財産権の帰属

（１） 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、受注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、全て原子力規制庁に帰属するものとする。

（２） 原子力規制庁は、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（以下、「複製等」という。）ができるとともに、任意に開示できるものとする。

（３） 本業務に関する権利（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、運用開始時に受注者から原子力規制庁に移転するものとする。

（４） 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、受注者は、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、本業務の受注者は、当該既存著作物の内容について事前に原子力規制庁の承認を得ることとする。

（５） 受注者は原子力規制庁に対し、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。

１３.２ 瑕疵担保責任

（１） 受注者は、本調達について検収を行った日を起算日として１年間、成果物に対する瑕疵担保責任を負うものとする。その期間内において瑕疵があることが判明した場合には、その瑕疵が原子力規制庁の指示によって生じた場合を除き（ただし、受注者がその指示が不適当であることを知りながら、又は過失により知らずに告げなかったときはこの限りでない。）、受注者の責任及び負担において速やかに修正等を行い、指定された日時までに再度納品するものとする。なお、修正方法等については事前に原子力規制庁の承認を得てから着手するとともに、修正結果等についても原子力規制庁の承認を得ること。

（２） 前項の瑕疵担保期間経過後であっても、成果物等の瑕疵が受注者の故意又は重大な過失に基づく場合は、前項の内容に係わらず本システムの稼動期間中はその責任を負うものとする。

（３） 原子力規制庁は、前各項の場合において、瑕疵の修正等に代えて、当該瑕疵により通常生ずべき損害に対する賠償の請求を行うことができるものとする。また、瑕疵を修正してもなお生じる損害に対しても同様とする。

１３.３ 検収

（１） 受注者は、成果物等について納品期日までに原子力規制庁に内容の説明を実施して検収を受けること。

（２） 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、変更点について原子力規制庁に説明を行ったうえで指定された日時までに再度納品すること。

１４．入札参加資格に関する事項

１４.１ 入札参加要件

応札希望者は、以下の条件を満たしていること。

（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 平成３１・３２・３３年度環境省競争参加資格（全省庁統一資格）の「役務の提供等（営業品目「ソフトウェア開発」）」の「A」の等級に格付けされた競争参加資格を有する者であること。

エ 暴力団員による不当な行為の防止等に関する法律第２条に規定する暴力団又は暴力団員と関係がないことを誓約できる者であること。

（２） 公的な資格や認証等の取得

情報システムの設計・開発、運用業務において以下に示す全ての資格及び認証を取得している、もしくは同等の品質・セキュリティを確保するための社内規程や組織体制等を構築運用していることを説明できること。

- ISO9001
- ISMS（ISO/IEC 27001、JISQ27001）

（３） 受注実績

ア 本調達と同等規模のシステムを構築・運用した実績を過去５年以内に有すること。

イ 官公庁のシステムを構築・運用した実績を有すること。

（４） 複数事業者による共同提案

ア 複数の事業者が共同提案する場合、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提案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 共同提案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、瑕疵担保責任（解散後も含む）に関しても協定の内容に含めること。

ウ 共同提案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提案への参加を行っていないこと。

エ 共同提案を構成する全ての事業者は、「１４.１ （３） 受注実績」を除く全ての応札条件を満たすこと。ただし、代表者たる事業者は、「１４.１ （３） 受注実績」を有すること。

（５） 第三者により貸付を行う場合

本調達において導入するハードウェア、ミドルウェア及び原子力規制庁に所有権があるアプリケーションを除くソフトウェア等について、第三者により貸付を行うことを予定している場合、提案書にその内容を記載するとともに、契約の締結に当たり、第三者の情報、契約形態、債務の履行体制、債務不履行時の対応等について、第三者と合意した内容を書面にて提出すること。また、その第三者は、「１４．１（１）競争参加資格」のア、イ、オを満たすこと。

１４.２ 入札制限

本調達案件の調達仕様書作成に直接関与した事業者（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、透明性及び公正性の確保の観点から、当該調達案件の入札に参加させないものとする。ただし、競争上何ら有利とならないと認められるときは、この限りではない。

１５．再委託に関する事項

１５.１ 再委託の制限及び再委託を認める場合の条件

（１） 受注者は、本調達の全部及び主要部分を第三者に再委託してはならない。

（２） 受注者における本業務の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。

（３） 受注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。

（４） 再委託を行う場合、再委託先が「１４ ２ 入札制限 」に示す要件を満たすこと。

（５） 再委託先における情報セキュリティの確保については受注者の責任とする。

１５.２ 承認手続

（１） 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再委託承認申請書を原子力規制庁に提出し承認を受けること。

（２） 前項による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原子力規制庁に提出し、承認を受けること。

（３） 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。）には、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。

１５.３ 再委託先の契約違反等

再委託先において、本調達仕様書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、受注者が一切の責任を負うとともに、原子力規制庁は、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。再々委託先においても同じとする。

１６．その他特記事項

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原子力規制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（契約額、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。

平成３１～３５年度
緊急時対策支援システムの更改及び運用･保守業務
(機器及びメインシステム)
要件定義書

平成３１年４月

原子力規制委員会原子力規制庁

変更履歴

版	変更日	内容
1.0	平成 30 年 4 月 5 日	初版

目 次

1. 業務要件の定義 1

1.1. 業務実施手順 3
1.1.1. 業務の範囲（業務機能とその階層） 3
1.1.2. 業務フロー図 6
1.1.3. 業務の実施に必要な体制 6
1.1.4. 入出力情報項目及び取扱量 7
1.2. 規模 8
1.2.1. サービスの利用者数 8
1.2.2. 単位（年、月、日、時間等）当たりの処理件数 8
1.3. 時期・時間 9
1.4. 場所等 9
1.4.1. 実施場所 9
1.4.2. 諸設備、物品等資源の定義方法 10
1.5. 管理すべき指標 10
1.6. 情報システム化の範囲 11
1.7. 業務の継続の方針等 11
1.8. 情報セキュリティ 11

2. 機能要件の定義 12

2.1. 機能に関する事項 12
2.2. 画面に関する事項 14
2.2.1. 画面一覧、画面概要、画面入出力要件・画面設計要件 14
2.2.2. 画面出力イメージ 16
2.2.3. 画面遷移の基本的な考え方 16
2.3. 帳票に関する事項 17
2.3.1. 帳票一覧、帳票概要、帳票入出力要件・帳票設計要件 17
2.3.2. 帳票出力イメージ 17

2.4. ファイルに関する事項 18
2.4.1. ファイル一覧、ファイル概要、ファイル入出力要件・ファイル設計要件 *18*
2.5. 情報・データに関する事項 19
2.5.1. 情報・データ一覧 *19*
2.5.2. 情報・データ処理要件 *19*
2.5.3. データ定義表 *19*
2.6. 外部インタフェースに関する事項 20
3. 非機能要件の定義 21
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 21
3.1.1. 情報システムの利用者の種類、特性 *21*
3.1.2. ユーザビリティ要件 *21*
3.1.3. アクセシビリティ要件 *21*
3.2. システム方式に関する事項 22
3.2.1. 情報システムの構成に関する全体の方針 *22*
3.2.2. 情報システムの全体構成 *23*
3.2.3. 開発方式及び開発手法 *23*
3.3. 規模に関する事項 23
3.3.1. 機器数及び設置場所 *24*
3.3.2. データ量 *24*
3.3.3. 処理件数 *26*
3.3.4. 利用者数 *26*
3.4. 性能に関する事項 26
3.4.1. 応答時間（レスポンスタイム、ターンアラウンドタイム、サーバ処理時間） *26*
3.4.2. スループット *27*
3.4.3. リソースの占有 *27*
3.5. 信頼性に関する事項 27
3.5.1. 可用性要件 *27*
3.5.2. 完全性要件 *29*
3.6. 拡張性に関する事項 29
3.6.1. 性能の拡張性 *29*

3.6.2. 機能の拡張性 *29*
3.7. 上位互換性に関する事項 30
3.8. 中立性に関する事項 30
3.9. 継続性に関する事項 30
3.9.1. 継続性に係る目標値 *30*
3.9.2. 継続性に係る対策 *31*
3.10. 情報セキュリティに関する事項 31
3.10.1. 主体認証 *31*
3.10.2. アクセス制御 *31*
3.10.3. 権限管理 *31*
3.10.4. ログの取得・管理 *32*
3.10.5. 暗号・電子署名 *32*
3.10.6. ソフトウェアの脆弱性対策 *32*
3.10.7. 不正プログラム対策 *33*
3.10.8. 標的型攻撃対策 *33*
3.10.9. 情報セキュリティ対策の管理体制 *33*
3.10.10. 情報セキュリティ対策の実施 *33*
3.10.11. 要機密情報の取り扱い *34*
3.10.12. 情報セキュリティ事故発生時の監査対応 *34*
3.10.13. 要機密情報の返却・廃棄 *34*
3.10.14. 原子力規制委員会情報セキュリティポリシー等の準拠 *34*
3.10.15. ネットワークサービスの情報セキュリティ対策 *34*
3.10.16. サーバ装置の情報セキュリティ対策 *35*
3.10.17. ウェブサーバにおける情報セキュリティ対策 *35*
3.10.18. データベースサーバにおける情報セキュリティ対策 *36*
3.10.19. 通信回線における情報セキュリティ対策 *36*
3.10.20. 品質報告およびセキュリティ報告 *37*
3.10.21. 情報セキュリティ対策の報告 *37*
3.10.22. 情報セキュリティに係るサービスレベルの保証 *37*
3.10.23. 運用管理機能の定義 *37*
3.10.24. 情報セキュリティインシデント発生監視機能の設計・構築 *38*

3.10.25. 情報システムに関する脆弱性への対策 38
3.10.26. セキュリティ対策実装方針書の策定 39
3.10.27. 構築・改修における情報セキュリティ対策 39
3.10.28. 開発工程における情報セキュリティ対策 39
3.10.29. 機器等の納入時又は情報システムの受入れ時の情報セキュリティ対策 40
3.10.30. 運用及び保守実施要領書の策定における情報セキュリティ対策 40
3.10.31. アプリケーション・コンテンツの不正プログラム対応 40
3.10.32. 更改又は廃棄における情報セキュリティ対策 41
3.10.33. リモート環境の構築における情報セキュリティ対策 41
3.11. 情報システム稼働環境に関する事項 42
3.11.1. ハードウェア構成 42
3.11.2. ソフトウェア構成 44
3.11.3. ネットワーク構成 46
3.11.4. 施設・設備要件 46
3.12. テストに関する事項 47
3.12.1. 単体テスト 48
3.12.2. 結合テスト 48
3.12.3. 総合テスト 49
3.12.4. 受入テスト 50
3.13. 移行に関する事項 50
3.13.1. 移行手順 50
3.13.2. 移行要件 53
3.13.3. 移行対象データ 55
3.14. 引継ぎに関する事項 55
3.15. 教育に関する事項 55
3.15.1. 教育対象者の範囲、教育の方法 55
3.15.2. 教材の作成 57
3.16. 運用に関する事項 58
3.16.1. 運用管理・監視等要件 58
3.16.2. 運用サポート業務 61
3.16.3. 業務運用支援 61

3.16.4. 運用実績の評価と改善 61
3.17. 保守に関する事項 62
3.17.1. アプリケーションプログラムの保守要件 62
3.17.2. ハードウェアの保守要件 63
3.17.3. ミドルウェアの保守要件 63
3.17.4. ソフトウェア製品の保守要件 64
3.17.5. データの保守要件 65
3.17.6. 保守実績の評価と改善 65

【別紙】

別紙 1．業務フロー
別紙 2．機能に関する事項
別紙 3．画面に関する事項
別紙 4．画面に関する事項（画面出力イメージ）
別紙 5．画面に関する事項（画面遷移）
別紙 6．帳票に関する事項
別紙 7．帳票に関する事項（帳票イメージ）
別紙 8．ファイルに関する事項
別紙 9．情報・データに関する事項（情報・データ一覧）
別紙 9-01．プラント標準パラメータコード一覧
別紙 9-02．プラント別パラメータコード一覧
別紙 9-03．コード一覧（事業者、発電所、プラント）
別紙 10．システム方式に関する事項（情報システムの全体構成（案））
別紙 11．情報システム稼動環境に関する事項（ソフトウェア構成（案））
別紙 12．情報システム稼働環境に関する事項（ソフトウェア要件（案））
別紙 13．情報システム稼動環境に関する事項（ハードウェア構成（案））
別紙 14．情報システム稼働環境に関する事項（ハードウェア要件（案））

【用語】

No.	用語	略称	説明
1	緊急時対策支援システム	ERSS	Emergency Response Support System：原子力災害発生時における防災対策支援を目的として、原子力規制委員会原子力規制庁において整備し、運用しているシステムのこと。
2	現行システム	-	現在、運用している緊急時対策支援システムのこと。
3	次期システム	-	現行システムを基に、仕様や環境を改良・更新する ERSS の次期システムのこと。
4	プラントデータ	-	原子力発電所等原子力施設（プラント）から常時伝送されるプラントの状況判断に必要な情報のこと。
5	プラントデータ収集システム	-	プラントデータを収集し、データベースに格納するシステムのこと。
6	プラント情報表示システム	ICS	Information Collection System：原子力発電所、再処理施設で重大事故もしくは重大事故に発展する可能性のある事故等が発生した場合に、官邸、原子力規制庁緊急時対応センター、各地の緊急事態応急対策等拠点施設などに、原子力施設の情報を提供するシステムのこと。
7	訓練データ配信システム	TDS	Training data Delivery System：原子炉の解析モデルを基に、事故時の原子力発電所の状態解析を行うシステムのこと。解析結果を訓練データとして、1 分毎に訓練用データベースへ送信することで、ICS 上にて事故を模擬表示することができる。訓練時に利用される。
8	メインシステム	-	次期システムから TDS を除いた部分を示す。
9	緊急時対応センター	ERC	Emergency Response Center：原子力緊急事態の発生時に設置される国の原子力災害対策本部の事務局のこと。
10	オフサイトセンター	OFC	Offsite Center：緊急事態応急対策拠点施設のこと。原子力施設で緊急事態が発生した際には、国、都道府県、市町村及び事業者の防災対策関係者が集合して、「原子力災害合同対策協議会」を組織し、連携の取れた応急対策を講じていく拠点。
11	事態即応センター	-	原子力事業者に設置される事務局のこと。原子力施設事態即応センター。
12	監視機能	-	第一データセンター、第二データセンター及び原子力規制庁本庁舎内に配置する ERSS を構成するサーバ機器等の死活監視やリソース監視を行う機能のこと。
13	次期システム請負事業者	-	TDS を除く ERSS の次期システムの設計・開発・保守・運用を請け負う事業者のこと。
14	TDS 次期システム請負事業者	-	TDS の次期システムの設計・開発・保守・運用を請け負う事業者のこと。
15	システム運用支援業者	-	ERSS の運用支援を行う事業者のこと。
16	システム管理者	-	ERSS の運用管理機能を含むすべての機能を利用でき、管理者として指定された原子力規制庁職員のこと。

1. 業務要件の定義

ERSS は、原子力事業者から送られてくるプラントデータを基に、原子力に係る緊急事態（原子力発電所等での重大事故もしくは重大事故に発展する可性のある事故、原子力発電所等の立地地区での大規模地震等の災害等）が発生した場合に、ERC や各地の OFC などに、主として以下の情報を提供するシステムである。

(1) 原子力施設の状態を示す情報(原子炉ならば圧力、温度、水位等)

(2) 原子炉事故の進展予測（燃料被覆管破損や炉心溶融に至る時間等の推定）に資する情報

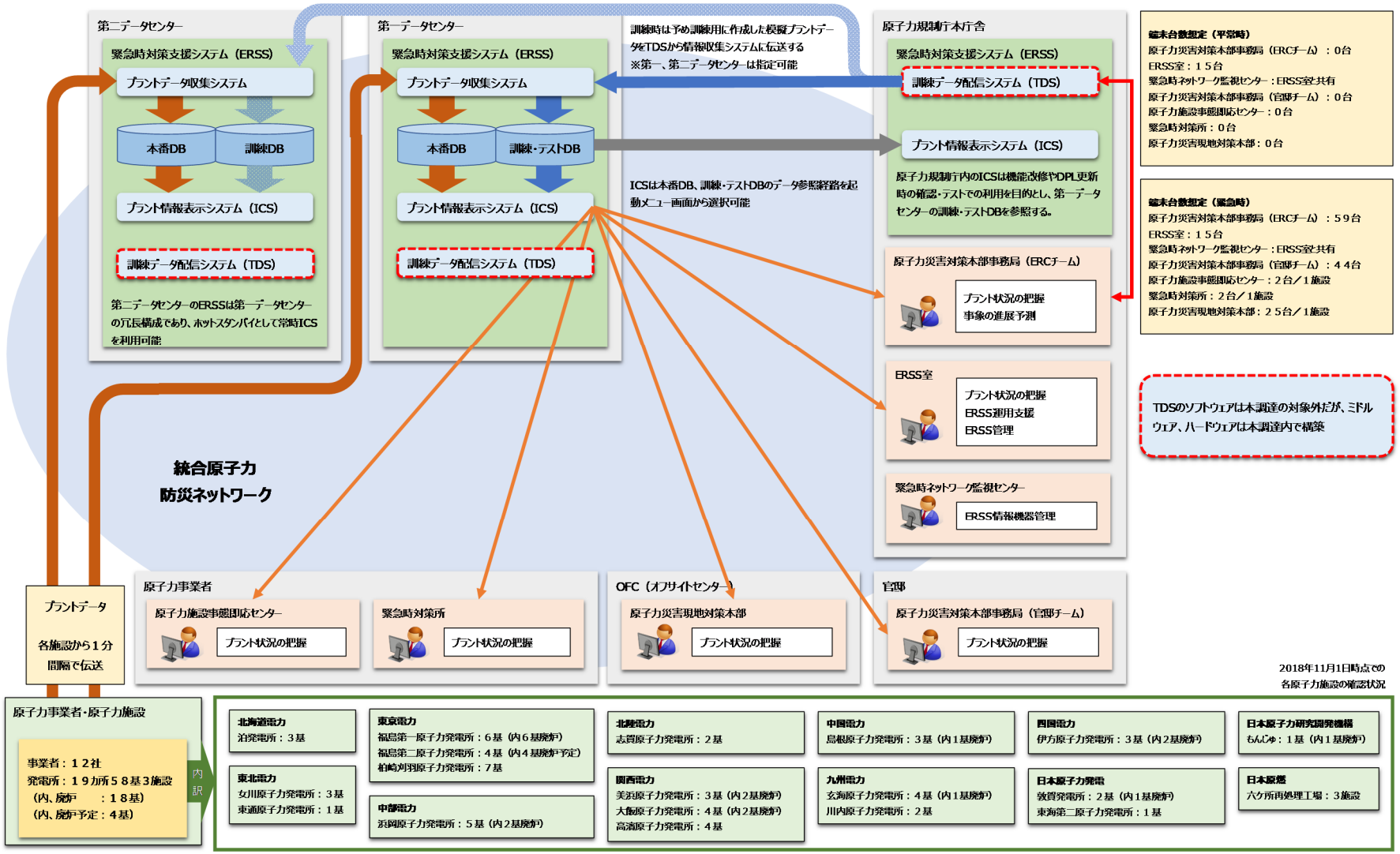
加えて、軽水炉事故に関する訓練や学習での利用を目的とした、原子炉事故解析により事故時の原子力施設の状態を示す模擬情報を作成、配信する機能を有する。

ERSS は、システムのライフサイクルを考慮し、また、新規制基準（原子炉等の設計を審査するための新しい基準）等に対応するため、2020 年度を目途に現行システムを基に、仕様や環境を改良・更新した次期システムへ移行する計画である。

なお特に断りのない場合、以降において ERSS と表記する場合は次期システム全体を示すものとし、本システムと表記する場合は次期システムにおける本業務の調達範囲内を示すものとする。

ERSS の鳥瞰図を以下に示す。

図 1-1 ERSS 鳥瞰図


第二データセンター
緊急時対策支援システム（ERSS）
プラントデータ収集システム
本番DB
訓練DB
プラント情報表示システム（ICS）
訓練データ配信システム（TDS）
第二データセンターのERSSは第一データセンターの冗長構成であり、ホットスタンバイとして常時ICSを利用可能
第一データセンター
緊急時対策支援システム（ERSS）
プラントデータ収集システム
本番DB
訓練・テストDB
プラント情報表示システム（ICS）
訓練データ配信システム（TDS）
訓練時は予め訓練用に作成した模擬プラントデータをTDSから情報収集システムに伝送する
※第一、第二データセンターは指定可能
ICSは本番DB、訓練・テストDBのデータ参照経路を起動メニュー画面から選択可能
原子力規制庁本庁舎
緊急時対策支援システム（ERSS）
訓練データ配信システム（TDS）
プラント情報表示システム（ICS）
原子力規制庁内のICSは機能改修やDPL更新時の確認・テストでの利用を目的とし、第一データセンターの訓練・テストDBを参照する。
原子力災害対策本部事務局（ERCチーム）
プラント状況の把握
事象の進展予測
ERSS室
プラント状況の把握
ERSS運用支援
ERSS管理
緊急時ネットワーク監視センター
ERSS情報機器管理
端末台数想定（平常時）
原子力災害対策本部事務局（ERCチーム）：0台
ERSS室：15台
緊急時ネットワーク監視センター：ERSS室共有
原子力災害対策本部事務局（官邸チーム）：0台
原子力施設事態即応センター：0台
緊急時対策所：0台
原子力災害現地対策本部：0台
端末台数想定（緊急時）
原子力災害対策本部事務局（ERCチーム）：59台
ERSS室：15台
緊急時ネットワーク監視センター：ERSS室共有
原子力災害対策本部事務局（官邸チーム）：44台
原子力施設事態即応センター：2台／1施設
緊急時対策所：2台／1施設
原子力災害現地対策本部：25台／1施設
TDSのソフトウェアは本調達の対象外だが、ミドルウェア、ハードウェアは本調達内で構築
統合原子力防災ネットワーク
プラントデータ
各施設から1分間隔で伝送
原子力事業者
原子力施設事態即応センター
プラント状況の把握
緊急時対策所
プラント状況の把握
OFC（オフサイトセンター）
原子力災害現地対策本部
プラント状況の把握
官邸
原子力災害対策本部事務局（官邸チーム）
プラント状況の把握
2018年11月1日時点での各原子力施設の確認状況
原子力事業者・原子力施設
事業者：12社
発電所：19カ所58基3施設
（内、廃炉　：18基）
（内、廃炉予定：4基）
内訳
北海道電力
泊発電所：3基
東北電力
女川原子力発電所：3基
東通原子力発電所：1基
東京電力
福島第一原子力発電所：6基（内6基廃炉）
福島第二原子力発電所：4基（内4基廃炉予定）
柏崎刈羽原子力発電所：7基
中部電力
浜岡原子力発電所：5基（内2基廃炉）
北陸電力
志賀原子力発電所：2基
関西電力
美浜原子力発電所：3基（内2基廃炉）
大飯原子力発電所：4基（内2基廃炉）
高浜原子力発電所：4基
中国電力
島根原子力発電所：3基（内1基廃炉）
九州電力
玄海原子力発電所：4基（内1基廃炉）
川内原子力発電所：2基
四国電力
伊方原子力発電所：3基（内2基廃炉）
日本原子力発電
敦賀発電所：2基（内1基廃炉）
東海第二原子力発電所：1基
日本原子力研究開発機構
もんじゅ：1基（内1基廃炉）
日本原燃
六ケ所再処理工場：3施設

1.1. 業務実施手順

ERSS の業務実施手順を以下に示す。

1.1.1. 業務の範囲（業務機能とその階層）

原子力規制庁において、原子力に係る緊急事態に備えるため、平時及び緊急時に行う業務を以下の通り一覧化し、ERSS に係る業務を中心に業務フローとして整理した。以下の業務一覧に対して、ERSS を利用する業務は「〇」として表示する。なお、ERSS の利用者は「1.2.1 サービスの利用者数」を参照。

表 1-1 業務一覧

階層 0		階層 1		業務処理		ERSS の利用	補足
No.	名称	No.	名称	No.	名称		
1	平時（運用・保守）	1.1	緊急事態への即応体制	1.1.1	緊急事態の即応体制の構築と維持	×	緊急事態の発生時に必要となる ERSS を使った防災活動への支援業務のための専門知識を有する業者による 24 時間対応の緊急時参集運用支援体制を構築し、維持する
		1.2	ERSS 常時伝送監視、ネットワーク機器の常時監視による機能の維持	1.2.1	ERSS の故障等の連絡窓口	×	緊急時ネットワーク監視センターにて 24 時間体制で行う
				1.2.2	ERSS のデータ伝送の監視･収集・格納	〇（ICS）	緊急時ネットワーク監視センターにて 2 時間間隔で各原子力施設からのデータ伝送の正常性を確認する 「別紙 1　業務フロー図 1」を参照
				1.2.3	現地作業による定期点検	×	現地作業により年間に 2 回の定期点検を行う
				1.2.4	リモートによる定期点検	×	リモート回線を使い月に 1 回のデータベース等の点検を行う
		1.3	ERSS 登録データの最新化	1.3.1	支援情報の登録・更新	〇（ICS）	原子力規制庁からの依頼により、支援情報（画像ファイルや PDF ファイル等）の新規登録又は既存登録情報の最新化を行う
2	平時（防災訓練等のサポート）	2.1	学習会の実施	2.1.1	原子力災害対策本部事務局（ERC チーム）向け学習会の実施	〇（プラントデータ収集システム、ICS、TDS）	ERSS 学習会（基礎）4 回 ERSS 学習会（応用）24 回を行う
		2.2	TDS を使用したブラインド訓練	2.2.1	ERSS（訓練モード）を使用した緊急時運用訓練実施の準備	〇（プラントデータ収集システム、ICS、TDS）	訓練用の模擬データ（訓練データ）を作成し、TDS に登録する 「別紙 1　業務フロー図 2」を参照
				2.2.2	ERSS（訓練モード）を使用した緊急時運用訓練の実施	〇（プラントデータ収集システ	加圧水型原子炉(PWR)運用訓練（年間 12 回）、沸騰水型原子炉(BWR)運用訓練（年間 12 回）、原子力総合防災訓練（プレ訓練、

階層 0		階層 1		業務処理		ERSS の利用	補足
No.	名称	No.	名称	No.	名称		
						ム、ICS、TDS）	本訓練）、原子力事業者が行う防災訓練（ERSS の利用は原子力事業者から使用申請があった場合のみ）を行う 「別紙 1　業務フロー図 3」を参照
		2.3	通信連絡訓練の実施	2.3.1	通信連絡訓練の実施	×	年間に 12 回行う
3	緊急時	3.1	原子力施設の状況等による情報の収集及び共有	3.1.1	原子力災害対策本部事務局（官邸チーム）による情報の収集	○（ICS）	原子力災害対策本部事務局（ERC チーム）、OFC 及び ERSS 等から原子力施設の状況を確認する 「別紙 1　業務フロー図 4」を参照
				3.1.2	原子力災害対策本部事務局（ERC チーム）による情報の収集と共有	○（ICS）	原子力施設事態即応センター、緊急時対策所及び ERSS 等から収集した情報を、ERC 内で共有する。また、原子力災害対策本部事務局（官邸チーム）へ報告する 「別紙 1　業務フロー図 4」を参照
		3.2	原子力施設の状況分析と共有	3.2.1	原子力災害対策本部事務局（ERC チーム）による状況分析	○（TDS）	原子力事業者等から得られた情報を踏まえ、原子力災害対策本部事務局（ERC チーム）は、原子力施設の状況を分析し、必要に応じて事故進展予測を行う 「別紙 1　業務フロー図 4」を参照
				3.2.2	原子力災害対策本部事務局（ERC チーム）による状況分析結果の共有	○（TDS）	結果より得られた周辺地域への影響及び放射性物質の放出源情報（ソースターム等）等について、原子力災害対策本部事務局（官邸チーム）、原子力災害対策本部事務局（ERC チーム内各機能班）、OFC、原子力施設事態即応センター等に情報を提供する 「別紙 1　業務フロー図 4」を参照
				3.2.3	原子力災害対策本部事務局（ERC チーム）による方針決定支援	○（TDS）	上述で得られた情報を基に、官邸での対応方針の決定を支援する。その際、必要に応じ専門家を招聘し、技術的助言を求める 「別紙 1　業務フロー図 4」を参照
		3.3	原子力事業者に対する命令	3.3.1	原子力災害対策本部事務局（ERC チーム）による命令案文の作成及び命令	×	原子力施設の状況分析の結果を踏まえ、原子力事業者が実施する事故収束のための活動について、原子力災害対策本部事務局（官邸チーム）の指示に基づき原子炉等規制法に基づく命令に関して、命令案文の作成や情報収集等の事務手続きを行い、原子力事業者に命令する 「別紙 1　業務フロー図 4」を参照

階層 0		階層 1		業務処理		ERSS の利用	補足
No.	名称	No.	名称	No.	名称		
				3.3.2	原子力事業者による命令の実行とその後の対応	×	原子力災害対策本部事務局（官邸チーム）の命令を実行し、状況を原子力施設事態即応センターに報告する。原子力施設事態即応センターは不測の事態に備え、応援体制を確立する 「別紙１　業務フロー図 4」を参照
		3.4	技術的支援	3.4.1	原子力災害対策本部事務局（ERC チーム）による短期的及び中期的な分析支援	○（ICS）	短期的及び中長期的な分析を行い、緊急事態対策監等を技術的な面から補佐する
				3.4.2	原子力災害対策本部事務局（ERC チーム）によるプラント状況などの解析支援	○（ICS）	プラントの状況などの解析などを行い、緊急事態対策監等及び原子力災害対策本部事務局（官邸チーム）の技術的支援を行う
4	障害発生時	4.1	次期システム請負事業者による障害対応	4.1.1	ERSS の障害を検知した時の対応	○（ICS）	１次切り分けを行い、障害内容に応じて次期システム請負事業者のアプリケーション担当、OS・ミドルウェア担当、ハードウェア担当が復旧作業を行う 「別紙１　業務フロー図 5」を参照
		4.2	計画的な保守点検による伝送停止	4.2.1	原子力事業者によるプラントデータの常時伝送を計画停止する時の対応	×	「別紙１　業務フロー図 6」を参照
				4.2.2	原子力規制庁による ERSS プラントデータ収集システムを計画停止する時の対応	×	「別紙１　業務フロー図 7」を参照
		4.3	障害等による伝送データ異常	4.3.1	原子力事業者が伝送データ異常を確認した場合の対応	○（ICS）	「別紙１　業務フロー図 8」を参照
				4.3.2	原子力規制庁が伝送データ異常を確認した場合の対応	○（ICS）	「別紙１　業務フロー図 9」を参照

1.1.2. 業務フロー図

「1.1.1 業務の範囲（業務機能とその階層）」の業務一覧より平時、緊急時、障害発生時の業務を中心に業務フローを整理した。「別紙 1　業務フロー図」を参照。

1.1.3. 業務の実施に必要な体制

原子力施設での事故発生に敷かれる体制のうち、ERSS に係わる業務の実施に必要な体制を以下に示す。

表 1-2 業務の実施体制

No.	場所名	実施体制	補足
1	官邸・原子力規制庁（ERC）	事象進展に応じて、以下の体制を構築し、業務を実施する。 (1)　原子力事故警戒本部（原子力規制庁・内閣府） (2)　原子力事故対策本部（原子力規制庁・内閣府） (3)　原子力災害対策本部 (4)　原子力災害対策本部事務局（官邸チーム） (5)　原子力災害対策本部事務局（ERC チーム）	原子力災害対策本部事務局は 9 つの機能班（総括班、放射線班、プラント班、医療班、住民安全班、広報班、運営支援班、国際班、実動対処班）から構成される
2	原子力規制庁（ERSS 室）	以下の体制で業務を実施する。 (1)　原子力災害対策本部事務局（ERC チーム） (2)　システム管理者 (3)　システム運用支援業者	
3	原子力規制庁（緊急時ネットワーク監視センター）	以下の体制で業務を実施する。 (1)　緊急時ネットワーク監視センター員	
4	原子力事業者事業所	以下の体制を構築し、業務を実施する。 (1)　原子力施設事態即応センター	
5	緊急時対策所（原子力施設内）	以下の体制で業務を実施する。 (1)　原子力規制事務所長または原子力保安検査官	
6	OFC	事象進展に応じて、以下の体制を構築し、業務を実施する。 (1)　原子力事故現地警戒本部（原子力規制庁・内閣府） (2)　原子力事故現地対策本部（原子力規制庁・内閣府） (3)　原子力災害現地対策本部	

1.1.4. 入出力情報項目及び取扱量

本システムに係る入出力情報項目及び取扱量を以下に示す。一覧のサブシステム、機能名は「2.1 機能に関する事項」を参照。本システムの利用者は「1.2.1 サービスの利用者数」を参照。

表 1-3 入出力情報一覧

No.	サブシステム	機能名	入出力画面・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	取得元／ 提供先	補足
1	プラントデータ収集システム	プラントデータ収集機能	―	入力	プラントデータの取得	1 件／分×61 施設	プラント状況の把握	原子力事業者	原子力施設 61 施設が対象
2	ICS	―	画面キャプチャー	出力	プラントデータ	4 件／時	プラント状況の把握	ERSS の全ての利用者	定時報での主要画面が対象
3		プラント情報表示機能（原子力発電所）	発電所サマリ表示	出力	プラントデータ	1 件／分／ユーザ	プラント状況の把握	ERSS の全ての利用者	
4			ユニット情報表示	出力	プラントデータ	1 件／分／ユーザ	プラント状況の把握	ERSS の全ての利用者	
5			トレンドグラフ表示	出力	プラントデータ	1 件／分／ユーザ	プラント状況の把握	ERSS の全ての利用者	
6			パラメータリスト表示	出力	プラントデータ	1 件／分／ユーザ	プラント状況の把握	ERSS の全ての利用者	
7			時系列表示	出力	プラントデータ	1 件／分／ユーザ	プラント状況の把握	ERSS の全ての利用者	定時確認
8			二次系表示	出力	プラントデータ	1 件／分／ユーザ	プラント状況の把握	ERSS の全ての利用者	PWR かつ新規制基準適合炉が対象
9			電源系統図表示	出力	プラントデータ	1 件／分／ユーザ	プラント状況の把握	ERSS の全ての利用者	PWR かつ新規制基準適合炉が対象
10		プラント情報表示機能（再処理施設）	安全機能データ	出力	プラントデータ	4 件／分／ユーザ	プラント状況の把握	ERSS の全ての利用者	
11		運用管理機能	プラント情報	出力	プラントデータ	1 件／月	プラント状況の把握	システム管理者	定期的な管理作業時

1.2. 規模

本システムの規模に係る要件を以下に示す。

1.2.1. サービスの利用者数

本システムの業務に係る利用者及び利用者数を以下に示す。なお、本システムは緊急時に業務として使用されるため、利用者数の前提として、原子力施設5施設の同時発災を想定して算出した同時利用の可能性がある人数（応援のために他地域のOFC及び原子力事業者での利用する人数を含む）とする。

表 1-4 利用者一覧

No.	利用者	主な実施場所	利用者数	補足
1	原子力災害対策本部参集要員	官邸、ERC、OFC、ERSS室	約225人	原子力災害時等に利用
2	原子力事業者職員	原子力事業者事業所、緊急時対策所、OFC	約100人	原子力災害時等に利用
3	システム管理者	ERSS室	約2人	原子力災害時等に利用
4	システム運用支援業者	ERSS室	約15人	原子力災害時等に利用
5	緊急時ネットワーク監視センター員	緊急時ネットワーク監視センター	約3人	
		合計	約345人	

1.2.2. 単位（年、月、日、時間等）当たりの処理件数

本システムの業務に係る単位当たりの処理件数を以下に示す。

なお、本システムは緊急時での利用を前提とするものであり、下記処理件数は緊急時における想定値である。

表 1-5 処理件数

No.	項目	処理件数		補足
		平常時	緊急時	
1	伝送データ受信件数	1件／分×61施設	1件／分×61施設	原子力発電所58カ所、再処理施設3カ所から1分毎に受信
2	ICS利用台数	約20台	約342台	ICSを利用する想定端末台数1台を1件と想定
3	TDS利用台数	約1台	約10台	システム運用支援業者がTDSを利用する想定端末台数
4	システム監視人数	2人	4人	システム運用支援業者、原子力規制庁職員（緊急時はシステム運用支援業者2名と原子力規制庁職員2人が対応）

1.3. 時期・時間

本システムは、緊急時に即座に利用できなければならないシステムであり、いつでも利用できる状態を維持するため、24 時間 365 日のサービス提供及び監視を行う。平常時は、緊急時を想定した訓練等で利用される。

1.4. 場所等

本システムの場所等に係る要件を以下に示す。

1.4.1. 実施場所

業務の緊急時における実施場所を以下に示す。

なお、原子力施設における事象の進展とともに業務の実施場所や実施体制は変更となるが、以下は緊急時の最終的な業務の実施場所、実施体制を記載する。

表 1-6 実施場所

場所名	実施体制	実施業務	所在地	補足
官邸・原子力規制庁（ERC）	原子力災害対策本部	各種情報の集約及び意思決定を行う。	官邸、原子力規制庁本庁舎内	
	原子力災害対策本部事務局（官邸チーム）	プラント状況の把握を行う。		
	原子力災害対策本部事務局（ERC チーム）	プラント状況の把握を行う。 必要に応じて事故進展予測を行う。		
原子力規制庁（ERSS 室）	原子力災害対策本部事務局（ERC チーム）	プラント状況の把握を行う。	原子力規制庁本庁舎内	
	システム管理者	ERSS の管理業務を行う。		
	システム運用支援業者	ERSS 運用の支援を行う。		
原子力規制庁（緊急時ネットワーク監視センター）	緊急時ネットワーク監視センター員	ERSS のデータ伝送状態及び関連情報機器の監視を行う。	原子力規制庁本庁舎内	
原子力事業者事業所	原子力施設事態即応センター	プラント状況の把握を行う。	各原子力事業者本店等	
緊急時対策所	原子力規制事務所長等	プラント状況の把握を行う。	各原子力施設内	
OFC	原子力災害対策本部	プラント状況の把握を行う。	各オフサイトセンター	
	原子力事業者	プラント状況の把握を行う。		

1.4.2. 諸設備、物品等資源の定義方法

原子力規制庁拠点内で必要となる備品（机、電話等所定の備品）は原子力規制庁が準備する。本業務を遂行するために必要となる体制図、行き先表示板、立ち入り禁止表示などの物品等は次期システム請負事業者で用意する。次期システム請負事業者が用意する作業場所で必要な諸設備、物品等は、次期システム請負事業者が必要なものを準備することとする。

なお、以下に示す諸設備、物品等は原子力規制庁が準備する。

表 1-7 諸設備、物品

種類	量	補足
ラックスペース	ラック 3 台分のスペース（第一データセンター） ラック 3 台分のスペース（第二データセンター） ラック 1 台分のスペース（原子力規制庁本庁舎）	現行システムの既存のラックスペースとは別に、専用のラックスペースを別途契約
運用端末（パソコン）	約 642 台（原子力災害対策本部事務局（官邸チーム）：44 台、原子力災害対策本部事務局（ERC チーム）：59 台、ERSS 室：15 台、OFC：21 台×18 施設、原子力施設事態即応センター：2 台×12 事業者、緊急時対策所：2 台×61 施設）	統合原子力防災ネットワークシステムにより整備された端末を利用する 左記の台数は、本システムを利用する可能性のある端末数とする

1.5. 管理すべき指標

業務の運営上で管理すべき指標を以下に示す。

表 1-8 管理すべき指標

指標の種類	指標名	計算式	単位	目標値	計測方法	計測周期
プロジェクト成果目標	ERSS を使用する業務は、原子力災害発生時にのみ臨時に行われるものであり、通常時は原子力災害発生時を想定した運用訓練のみ実施する。したがって、業務に関する指標は対象外とする。					
業務効果の指標						
業務実施指標						
情報システム効果に関する指標	計画的停止以外での機能の停止回数（原子力事業者等の他システムが原因の停止は除く）	停止回数/年	回/年	0 回/年	機器状態監視機能による計測	常時監視
	情報セキュリティポリシーの遵守率	遵守事項/遵守すべき事項	%	100%	チェックリスト等による確認	毎年

1.6. 情報システム化の範囲

「1.1.1 業務の範囲（業務機能とその階層）」で整理した業務のうち、本システムを用いて実施する業務の範囲について、以下に示す。

表 1-9 情報システム化する機能一覧

機能		対象となるシステム名
プラントデータ収集機能	原子力施設から送られるプラントデータを収集し、データベースに格納する。	プラントデータ収集システム
訓練データ収集機能	訓練データ生成機能から送られる訓練データを収集し、訓練用データベースに格納する。	
管理・共通機能	プラントデータのバックアップやDB登録エラー時のリカバリ等の運用管理を行う。	
プラント情報表示機能	原子力施設から送られるデータをERCや各地のOFCにて、数値またはグラフ化して表示する。また、訓練の際に用意される訓練シナリオに合わせた訓練データを訓練モードで表示する。	ICS
運用管理機能	オフラインパラメータの手入力や訓練データの初期化、しきい値メンテナンス等の管理操作を行う。	
事故訓練支援機能	軽水炉過酷事故時において、事故対策支援のため、原子力施設から送られるデータを基に高速に事故解析を行い、結果を数値またはグラフ化して表示する。	TDS
訓練データ生成機能	訓練の際に用意される訓練シナリオに合わせた訓練データを生成し、1分間隔で訓練データ収集機能に送信する。	

※ ただし、TDS のソフトウェア部分は本調達の対象外であるため、TDS が対象となる上記機能の実装に関する記載は本書の対象外とする。

1.7. 業務の継続の方針等

本システムの業務の継続方針は「3.9 継続性に関する事項」を参照。

1.8. 情報セキュリティ

本システムの情報セキュリティ要件は「3.10 情報セキュリティに関する事項」を参照。

2. 機能要件の定義

次期システムのプラントデータ収集システム、ICS は現行システムの機能を踏襲した上で、原子力規制庁の改善要望に基づき、機能変更及び機能追加を実施する。

本要件定義では、現行システムの仕様書と改善要望を元に、サブシステム別に機能一覧として整理し、変更、追加箇所について整理を行った。

(1) 現行システムの機能は、現行システムの設計書から確認すること。
(2) 現行システムの設計書は、次期システム請負事業者が原子力規制庁より提供を受けること。
(3) 現行システムの改善要望については、「別紙 2　機能に関する事項」を参照。
(4) ICS の画面の同時起動可能数は設計フェーズにて検討すること。

2.1. 機能に関する事項

本システムのサブシステム別の構成機能を以下に示す。

表 2-1 構成機能一覧

No.	サブシステム	構成機能	用途･備考
1	プラントデータ収集システム	プラントデータ収集機能	原子力施設から送信されてくるプラントデータを収集する。常時伝送される原子力施設のプラントデータを受信し、データベースに登録を行う。データ内容の確認を行い、正常ならデータベースに格納し、異常ならその旨ログに出力し、データベースに格納しない。
2		訓練データ収集機能	TDS から送信されてくる訓練データを収集する。訓練等で一時的に伝送される訓練データを、訓練用のデータベースに登録する。データ内容の確認を行い、正常ならデータベースに格納し、異常ならその旨ログに出力し、データベースに格納しない。
3		管理・共通機能	プラントデータのバックアップや DB 登録エラー時のリカバリ等の運用管理を行う。
4	ICS	プラント情報表示機能（共通機能）	原子力発電所と再処理施設のプラント情報表示機能の内、共通で利用する機能。メニュー、グラフ、パラメータリストなど、原子力施設から受信したプラントデータを表示する。また、特定のプラントデータ（炉内圧力、冷却水温度等）のしきい値を超えるデータについて、警報表示する。
5		プラント情報表示機能(原子力発電所)	原子力発電所のプラントからの受信情報を ERC や各地の OFC にて、数値またはグラフ化して表示する。1 分毎に受信する内容で画面表示情報を最新化して表示する。
6		プラント情報表示機能(再処理施設)	再処理施設のプラントからの受信情報を ERC や各地の OFC にて、数値またはグラフ化して表示する。1 分毎に受信する内容で画面表示情報を最新化して表示する。
7		運用管理機能	オフラインパラメータの手入力や訓練データの初期化、しきい値メンテナンス等の管理操作を行う。

なお、上記の構成機能一覧を機能分類で整理した機能数を以下に示す。機能の詳細は「別紙 2　機能に関する事項」を参照。一覧表の別紙№は別紙の項番に紐付く。

機能分類の凡例は以下の通り。

受信	データ受信、およびデータベース登録	**更新**	データベースやファイルの更新処理等
共通	プロセスの起動・停止や暗号化処理等	**管理**	プロセス監視やバックアップに関する処理等
メニュー	メニュー機能	**照会**	データベース保持データの画面表示処理等
出力	システムによるファイル出力処理等	**印刷**	システムからの帳票印刷処理

表 2-2 構成機能の機能数一覧

No.	サブシステム	別紙 No.	構成機能	機能分類	機能数	備考
1	プラントデータ収集システム	1.1	プラントデータ収集機能	受信	2	
				更新	2	
		1.2	訓練データ収集機能	共通	1	
		1.3	管理・共通機能	共通	3	
				更新	2	
				管理	6	
2	ICS	2.1	プラント情報表示機能（共通機能）	メニュー	1	原子力発電所と再処理施設のプラント情報表示機能の内、共通で利用する機能数を集計
				照会	5	
				更新	3	
				出力	3	
				印刷	2	
				管理	1	
		2.2	プラント情報表示機能（原子力発電所）	メニュー	2	全ての原子力発電所に対して共通で利用する機能数を集計。なお、各原子力発電所毎に施設の構成やパラメータ数は異なり、同一機能でも画面内容は同一ではない。画面内容については、後述の「2.2 画面に関する事項」にて整理する
				照会	6	
				出力	1	
				管理	1	
		2.3	プラント情報表示機能（再処理施設）	メニュー	2	全ての再処理施設に対して共通で利用する機能数を集計。なお、各再処理施設毎に施設の構成やパラメータ数は異なり、同一機能でも
				照会	7	
				出力	1	

No.	サブシステム	別紙 No.	構成機能	機能分類	機能数	備考
				管理	1	画面内容は同一ではない。画面内容については、後述の「2.2 画面に関する事項」にて整理する
		2.4	運用管理機能	メニュー	1	
				更新	7	
				出力	2	
				管理	5	
				合計	67	

2.2. 画面に関する事項

本システムの画面に関する事項の要件を以下に示す。

2.2.1. 画面一覧、画面概要、画面入出力要件・画面設計要件

画面に関する各要件（画面 ID、画面分類、画面名、画面概要、画面入出力要件、画面設計要件（変更点）、該当機能）については、「別紙 3　画面に関する事項」にサブシステム別に記載する。また、プラント情報表示システムの要件では、プラント別に画面要否を一覧として整理した。なお、別紙３「2.2. プラント情報表示機能（原子力発電所）」に示す画面のリリース時期は以下の通りとする。

(1) 川内　1号機・2号機、玄海　3号機・4号機、大飯　3号機・4号機、高浜　3号機・4号機、伊方　3号機の画面
2020 年 3 月（次期システム稼働開始時）：新規制基準に対応した全ての画面が実装済みであること（必須）

(2)（1）以外のユニット
2020 年 3 月（次期システム稼働開始時）：現行システムの画面が再現されていること。
2024 年 3 月（本業務終了時）までに：燃料プールが追加された画面が実装済みであること。
原子力事業者側の作業スケジュールと調整し実施すること。原子力事業者側作業が遅れ、本業務終了まで調整できないことが判明した場合は、原子力規制庁の指示に従い実装作業を行うこと。

サブシステム別の構成機能と画面数を以下に一覧表とした。一覧表の別紙№は別紙の項番に紐付く。

画面分類の凡例は以下の通り

メニュー	メニュー画面	**ログイン**	ログイン認証を行う画面
照会	データベース保持データを表示する画面	**更新**	データベースやファイル、画面表示設定等を更新する画面
出力	ファイルを出力する画面	**管理**	パラメータのしきい値やデータのメンテナンス等を行う画面

表 2-3 構成機能の画面数一覧

No.	サブシステム	別紙 No.	構成機能	画面分類	画面数	備考
1	プラントデータ収集システム	-	プラントデータ収集機能	-	0	プラントデータ収集システムには画面はなし
		-	訓練データ収集機能	-	0	
		-	管理・共通機能	-	0	
2	ICS	2.1	プラント情報表示機能（共通機能）	メニュー	1	
				照会	10	
				更新	2	
		2.2	プラント情報表示機能（原子力発電所）	メニュー	2	原子力発電所のプラント数は 58 基（うち稼働・停止中は 36 基、廃炉・廃炉予定は 18 基、廃炉未確定は 4 基)。なお、画面数は「別紙 3　画面に関する事項」表 別紙 3-4 プラント別画面数（プラント情報表示機能（原子力発電所））の総計を参照
				照会	387	
				更新	0	
		2.3	プラント情報表示機能（再処理施設）	メニュー	2	再処理施設のプラント数は 3 基（うち 3 基とも試運転中）。なお、画面数は「別紙 3　画面に関する事項」表 別紙 3-7 プラント別画面数（プラント情報表示機能（再処理施設））の総計を参照
				照会	16	
				更新	0	
		2.4	運用管理機能	ログイン	1	
				メニュー	1	
				照会	1	
				更新	5	
				出力	3	
				管理	9	
				合計	440	

2.2.2. 画面出力イメージ

次期システムの ICS は、現行システムの画面レイアウトを踏襲した上で、原子力規制庁の改善要望に基づき、画面レイアウトの変更を実施する。画面出力イメージは、現行システムを踏襲した代表的な画面と、改善要望に基づき変更を実施する次期システムの画面出力イメージを整理した。詳細は「別紙 4 画面に関する事項（画面出力イメージ）」を参照。なお、「別紙 4　画面に関する事項（画面出力イメージ）」に記載のない画面は現行システムの設計書を確認すること。

2.2.3. 画面遷移の基本的な考え方

本システムの画面遷移の基本的な考え方を以下に示す。画面遷移の詳細は「別紙 5　画面に関する事項（画面遷移）」を参照。

(1) 次期システムの ICS の画面遷移は、現行システムの画面遷移を踏襲すること。
(2) 一連の処理において、画面が遷移しても一度入力した情報が引き継がれるようにし、再入力を不要とすること。
(3) 画面の複数起動を可能とすること。ただし、画面の同時起動可能数は設計フェーズにて検討すること。

2.3. 帳票に関する事項

本システムの帳票に関する事項の要件を以下に示す。

2.3.1. 帳票一覧、帳票概要、帳票入出力要件・帳票設計要件

本システムの帳票について以下に示す。詳細は「別紙 6　帳票に関する事項」を参照。

表 2-4 構成機能の帳票数一覧

No.	サブシステム	構成機能	帳票数	備考
1	プラントデータ収集システム	プラントデータ収集機能	0	
		訓練データ収集機能	0	
		管理・共通機能	0	
2	ICS	プラント情報表示機能（共通機能）	2	原子力発電所と再処理施設のプラント情報表示機能の内、共通で利用する帳票数を集計
		プラント情報表示機能（原子力発電所）	0	
		プラント情報表示機能（再処理施設）	0	
		運用管理機能	0	
		合計	2	

2.3.2. 帳票出力イメージ

本システムの帳票イメージは「別紙 7　帳票に関する事項（帳票イメージ）」を参照。

2.4. ファイルに関する事項

本システムのファイルに関する事項の要件を以下に示す。

2.4.1. ファイル一覧、ファイル概要、ファイル入出力要件・ファイル設計要件

本システムのファイルについて以下に示す。詳細は「別紙 8　ファイルに関する事項」を参照。

表 2-5 構成機能のファイル数一覧

No.	サブシステム	構成機能	ファイル数	備考
1	プラントデータ収集システム	プラントデータ収集機能	2	
		訓練データ収集機能	0	
		管理・共通機能	0	
2	ICS	プラント情報表示機能（共通機能）	3	原子力発電所と再処理施設のプラント情報表示機能の内、共通で利用するファイル数を集計
		プラント情報表示機能（原子力発電所）	1	
		プラント情報表示機能（再処理施設）	1	
		運用管理機能	2	
		合計	9	

2.5. 情報・データに関する事項

システムで取り扱う情報・データについて以下に示す。なお、新規制基準対応のデータが確定していないため、参考として現行システムのデータを記載する。新規制基準対応のデータは、設計フェーズにて取り込みを検討すること。

2.5.1. 情報・データ一覧

本システムで取り扱う情報・データについて以下に示す。詳細は「別紙 9　情報・データに関する事項（情報・データ一覧）」を参照。

表 2-6 情報・データ一覧

No.	サブシステム	情報名	データ名	種類数	備考
1	プラントデータ収集システム	伝送データ	プラントデータ	1	
2		模擬伝送データ	訓練データ	1	訓練用の伝送データ
3	ICS	伝送データ	プラントデータ	1	
4		模擬伝送データ	訓練データ	1	訓練用の伝送データ
			合計	4	

2.5.2. 情報・データ処理要件

本システムの情報・データ処理要件は「別紙 9-01 プラント標準パラメータコード一覧」、「別紙 9-02 プラント別パラメータコード一覧」を参照。

2.5.3. データ定義表

本システムのデータ定義は「別紙 9-01 プラント標準パラメータコード一覧」、「別紙 9-02 プラント別パラメータコード一覧」、「別紙 9-03 コード一覧（事業者、発電所、プラント）」を参照。

2.6. 外部インタフェースに関する事項

本システムの外部インターフェースを以下に示す。詳細については現行システムの設計書「伝送インターフェイス仕様書」を参照。なお、設計書は次期システム請負事業者が原子力規制庁より提供を受けること。

表 2-7 データに関する外部インタフェース一覧

No.	外部 I/F ID	外部 I/F 名	外部 I/F 概要	相手先システム	I/0 区分	送受信データ	送受信タイミング	送受信の条件	補足
1	I0001	プラントデータ	原子力施設から常時伝送されるプラント情報	原子力事業者の伝送サーバ	IN	TCP/IP の Socket 通信でデータ伝送	1 分周期	24 時間 365 日の常時伝送	全ての原子力施設から受信する
2	I0002	訓練データ	訓練時、TDS から伝送される模擬プラント情報	TDS	IN	TCP/IP の Socket 通信で伝送	1 分周期	訓練時、ICS を訓練モードに切り替えて受信	I/F はプラントデータと同様
3	I0003	SEARCH_ABORT_DATE_PROC	伝送日時データを取得するストアドプロシージャ	TDS	OUT	ストアドプロシージャの結果データ	随時	なし	TDS ではプラント毎の最新受信日時を取得するために利用する
4	I0004	SEARCH_ABORT_DATE_TR_PROC	伝送日時データを取得する訓練用のストアドプロシージャ	TDS	OUT	ストアドプロシージャの結果データ	随時	なし	TDS ではプラント毎の最新受信日時を取得するために利用する
5	I0005	SEARCH_PLANT_DATA_OPT_PROC	任意時刻のプラントデータを取得するストアドプロシージャ	TDS	OUT	ストアドプロシージャの結果データ	随時	なし	TDS では指定したプラントの指定時刻のプラントデータを取得するために利用する
6	I0006	SEARCH_PLANT_DATA_OPT_TR_PROC	任意時刻のプラントデータを取得する訓練用のストアドプロシージャ	TDS	OUT	ストアドプロシージャの結果データ	随時	なし	TDS では指定したプラントの指定時刻のプラントデータを取得するために利用する

3. 非機能要件の定義

本システムの非機能要件を以下に示す。

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

本システムのユーザビリティ及びアクセシビリティ要件を以下に示す。

3.1.1. 情報システムの利用者の種類、特性

本システムの利用者の種類、特性の要件は以下の通りとする。

表 3-1 本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	補足
1	一般者	官邸、ERC、OFC、ERSS 室を含む国の原子力災害対策本部参集要員	緊急時、訓練時に ERSS を利用した業務を行う	
2		原子力事業者職員	緊急時、訓練時に ERSS を利用した業務を行う	
3	運用支援者	ERSS の運用支援業者	ERSS の運用支援業務を受注した業者により業務を行う	
4		緊急時ネットワーク監視センター員	24 時間体制で ERSS の常時伝送の監視業務を行う	2 時間間隔の目視確認
5	管理者	ERSS の管理者	ERSS のシステム管理業務を行う	

3.1.2. ユーザビリティ要件

ユーザーインターフェースの設計方針は現行同等とする。

3.1.3. アクセシビリティ要件

ユーザーインターフェースの設計方針は現行同等とする。

3.2. システム方式に関する事項

本システムのシステム方式の要件を以下に示す。

3.2.1. 情報システムの構成に関する全体の方針

本システムの構成に関する全体方針を以下に示す。

3.2.1.1. システムアーキテクチャ

本システムのシステムアーキテクチャは、現行システムを踏襲し Web サーバ型とすること。

3.2.1.2. アプリケーションプログラムの設計方針

アプリケーションプログラムの設計方針は以下の通りとする。

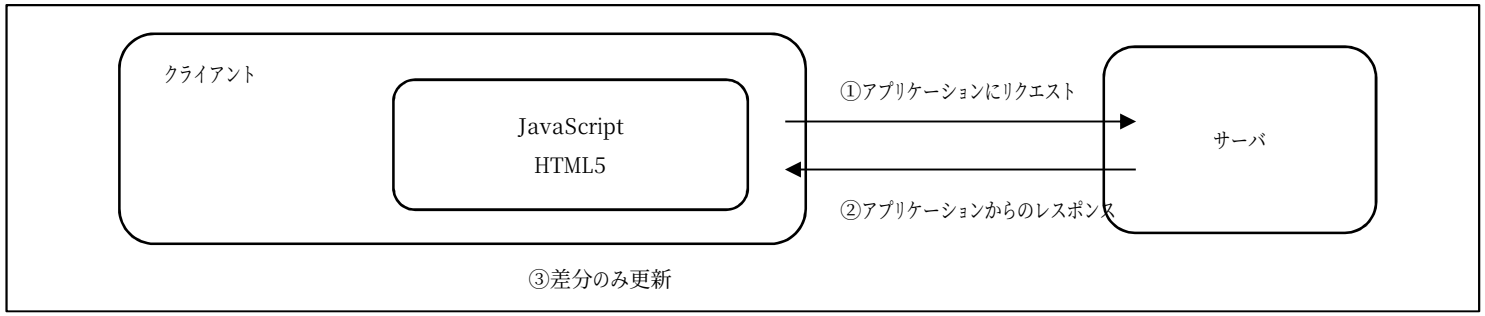
(1) 本システムは各原子力施設から 1 分ごとに受信するプラントパラメーター情報を利用者に表示提供するため、表示情報を頻繁に更新する。このため、初回表示以降はサーバから差分情報のみを取得してクライアント側で表示変更を行うシングルページアプリケーション方式で設計を行うこと。

(2) 開発言語は現行システムで採用していた Flash が保守切れとなるため、よりオープン性の高い HTML5 及び JavaScript などのデファクトスタンダードの言語を採用すること。なお、HTML5 及び JavaScript 以外の言語を採用する場合は、事前に原子力規制庁に確認を行うこと。

(3) 技術の採用に当たっては、採用段階でセキュリティホールが無く、構築後 4 年以上サポートが受けれること、端末へのインストールが不要なことを前提とすること。

(4) 画面上の文言修正などの軽微な修正を容易に反映できる設計としておくこと。

図 3-1 シングルページアプリケーション



3.2.1.3. ソフトウェア製品の活用方針

ソフトウェア製品の活用方針は以下の通りとする。

(1) 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こと。
(2) 構築後 4 年以上サポートが受けられるソフトウェア製品を採用すること。

3.2.1.4. システム基盤の方針

システム基盤の方針は以下の通りとする。

(1) サーバ、ストレージのハードウェア集約を行い、ハードウェアの一元管理ができるようにすること。なお、サーバ環境での自動再生（オートラン）機能は無効化すること。
(2) プラントデータ収集サーバおよびデータベースサーバについては物理サーバとすること。
(3) (2)以外については、仮想化技術等を活用し、可用性に優れたシステム構成とすること。システム構成における可用性確保の具体的方策は問わない。
(4) 第一データセンター、第二データセンターのシステム構成は同一構成とすること。
(5) 原子力施設側のデータ送信先設定は現行から変更がないように、プラントデータ取集サーバ側の受信 IP アドレスは現行と同一の設定で構築すること。
(6) クライアント環境は本調達の対象外のため、既存の端末機器を利用すること。ただし、クライアント環境の OS は Microsoft Windows10 Enterprise とし、稼働保証するブラウザは原子力規制庁規定のブラウザ（Internet Explorer 11）とすること。

3.2.2. 情報システムの全体構成

本システムの全体構成は、「別紙 10　システム方式に関する事項（情報システムの全体構成（案））」を参照。なお、第一データセンター及び第二データセンターを構築するアプリケーション、ハードウェア、ミドルウェア及びソフトウェア（監視含む）は同一製品を採用すること。

3.2.3. 開発方式及び開発手法

本システムの開発方式はスクラッチ開発とする。本システムの開発手法は特に定めないが、基本的に現行システム機能を踏襲し、モックアップやプロトタイプ等の適切な手段を用いて可能な限り早期に原子力規制庁の意見・要求を取り入れ、要件の解釈の違いによる手戻りを最小限とすることが可能な開発手法を採用すること。

3.3. 規模に関する事項

本システムの規模に関する要件を以下に示す。

3.3.1. 機器数及び設置場所

本システムの機器数及び設置場所の要件を以下に示す。

3.3.1.1. 機器数

後述の「3.11.1 ハードウェア構成」に示す通りとする。

3.3.1.2. 設置場所

原子力規制庁が指定する統合原子力防災ネットワーク第一データセンター、第二データセンター及び原子力規制庁本庁舎内とする。

3.3.1.3. 設置条件

設置条件は以下の通りとする。

(1) 電源関係

(a) 電源電圧は、AC100 又は AC200V に対応すること。

(b) 電源の確保については、原子力規制庁の指示に従い、必要に応じ延長コード及びテーブルタップ等を用意すること。

(2) 納入形態

(a) ハードウェア及び装置は、すべて EIA（Electronic Industries Alliance）規格に準拠した 44 ユニット（以下、「U」という）19 インチラック（3 ラック）に搭載すること。

(b) 44U19 インチラックへの搭載部品（ボルト、ナット等）は受注者が用意すること。

3.3.2. データ量

本システムのデータ量の要件を以下に示す。

表 3-2 データ量一覧

No.	区分	データ名	サイズ (KB)	データ数	保持世代	合計 (MB)	余裕率 (※1)	圧縮率 (※2)	必要容量 (MB)	補足
1	プラントデータ収集システムの受信データ	原子力施設からのプラントデータ	3.6	61	4,320 (60 分×24 時間×3 日間)	926.5	1.3	0	1,204.5	送信元プラントは 61 施設。原子力施設からは施設別に 1 分毎に受信する。DB 登録待ちの場合にファイル出力するため 3 日間の退避を想定する サイズ：現行パラメータ長の最大値を元に算出

No.	区分	データ名		サイズ (KB)	データ数	保持世代	合計 (MB)	余裕率 (※1)	圧縮率 (※2)	必要容量 (MB)	補足
2	プラント情報表示システム(ICS)の保存データ	PWR かつ新規制基準に適合した稼働済みプラントのプラントデータ		3.6	9	20,160 (60 分×24 時間×14 日間)	637.9	1.3	0	829.3	送信元プラントは 9 施設。蓄積期間は 2 週間 サイズ：現行パラメータ長の最大値を元に算出
3		上記以外の原子力発電所のプラントデータ		3.6	49	20,160 (同上)	3,472.9	1.3	0	4,514.8	送信元プラントは 49 施設。蓄積期間は 2 週間 サイズ：現行パラメータ長の最大値を元に算出
4		再処理施設プラントデータ		3.6	3	20,160 (同上)	212.7	1.3	0	276.5	送信元プラントは 3 施設。蓄積期間は 2 週間 サイズ：現行パラメータ長の最大値を元に算出
5	支援情報データ	ユニット情報支援情報		700	305	3	625.5	1.3	0	813.2	画像付 PDF ファイルを 700KB と想定し、各ユニットで 5 データずつを 3 世代管理する想定 データ数：5 データ×61 施設=305
6	アプリケーションログ	プラントデータ収集システム受信ログ		30,515.70	61	60 (12 ヶ月×5 年)	109,069.8	1.3	0.9	14,179.1	保管期間は 5 年間とする。ログ 1 行は 700 バイトと想定し、1 分毎に 61 施設からの受領として算出 サイズ：700B×60 分×24 時間×31 日/1024B
7		プラント情報 DB 登録ログ	(正常)	6,539.06	61	60 (12 ヶ月×5 年)	23,372.1	1.3	0.9	3,038.4	保管期間は 5 年間とする。ログ 1 行は 150 バイトと想定し、1 分毎に 61 施設分の登録を行う サイズ：150B×60 分×24 時間×31 日/1024B
8			(エラー)	87,187.50	6	60 (12 ヶ月×5 年)	30,651.9	1.3	0.9	3,984.7	保管期間は 5 年間とする。エラーログ 1 行は 200 バイトとし、10 項目、6 施設に発生することを想定 サイズ：200B×10 項目×60 分×24 時間×31 日/1024B
9		プラント情報表示システムログ	平常時	0.6	42	55 (11 ヶ月×5 年)	1.4	1.3	0.9	0.2	保管期間は 5 年間とする。ログ 1 行は 200 バイトと想定し、起動・終了、エラー時を出力 データ数：通常時の処理件数
10			緊急時	0.6	717	5 (1 ヶ月×5 年)	2.2	1.3	0.9	0.3	同上 データ数：緊急時の処理件数
		合計		－	－	－	168,972.9			28,840.8	

※1. 余裕率について
業務量の増加は 2 施設分（ふげん原子力施設、東海再処理施設）の増加及びプラントデータのパラメータ数の増加を想定して設定する
利用者数に紐づくデータも同様の増加率として設定する

※２．　圧縮率について
　　業務データについては圧縮保管しないため 0%を設定、ログファイルはローテーション時に圧縮保管するためテキストデータの圧縮率 90%を設定

3.3.3. 処理件数
処理件数は「1.2.2 単位（年、月、日、時間等）当たりの処理件数」を参照。

3.3.4. 利用者数
利用者数は「1.2.1 サービスの利用者数」を参照。

3.4. 性能に関する事項
本システムの性能に関する事項の要件を以下に示す。
(1) 応答時間、スループットともに、縮退時も同様の順守率とすること。
(2) 今後の業務量増加はふげん原子力施設と東海再処理施設の 2 施設の増加を想定して余裕率を 1.2 倍に設定すること。
(3) ICS アクセス可能端末より同時アクセス(1 分に１回)が 24 時間継続しても応答時間を順守すること。

3.4.1. 応答時間（レスポンスタイム、ターンアラウンドタイム、サーバ処理時間）
平常時及び緊急時における応答時間の目標値は以下の通り。

表 3-3 応答時間の目標値

No.	システム	設定対象	指標名	目標値	順守率	余裕率	補足
1	プラントデータ収集システム	原子力施設からの受信データの登録処理	ターンアラウンドタイム	10 秒以内	99%	1.2	現行システムと同等目標
2	プラント情報表示システム（ICS）	ユニット情報表示画面の表示	レスポンスタイム	3 秒以内	99%	1.2	現行システムと同等目標

3.4.2. スループット

平常時及び緊急時におけるスループットの目標値は以下の通り。

表 3-4 スループットの目標値

No.	システム	設定対象	目標値	順守率	余裕率	補足
1	プラントデータ収集システム	原子力施設からのデータ受信、データ登録	3 施設分／秒	99%	1.2	現行システムと同等目標
2	プラント情報表示システム（ICS）	ユニット情報の表示	17PV／秒	99%	1.2	現行システムと同等目標

3.4.3. リソースの占有

リソース共有による性能の低下を防ぐため、仮想技術を利用する場合においては各仮想ホストサーバから仮想ゲストに割り当てるリソースは占有とすること。

3.5. 信頼性に関する事項

本システムの信頼性に関する事項の要件を以下に示す。

なお、本システムで取り扱う情報に関する格付けは以下とする。

表 3-5 取り扱う情報の格付け

No.	データ	状態	機密性	完全性	可用性
1	プラント情報（原子力施設より受信した情報）	平常時	2	2	1
		緊急時	1	2	1
2	プラント情報以外	常時	2	2	2

3.5.1. 可用性要件

本システムの可用性に関する事項の要件を以下に示す。

3.5.1.1. 停止許容時間および修理完了時間

(1) 「表 3-6 各サーバの停止許容時間」に示す停止許容時間を遵守すること。なお、本項で言及する「各サーバ」とは、クラスタ等の二重構成とした場合においては当該サーバ群全体を指すものとし、物理的または論理的な単体サーバのことを指すものではない。

(2) 停止許容時間の算定においては、アプリケーション停止は含めないこととし、ハードウェア及びミドルウェアの停止を対象とする。

(3) 駆けつけ保守での対応は、監視上のアラート発報、もしくは障害の連絡から 2 日以内に修理完了とすること。なお、2 日以内には部材搬入時間も含むため、サーバの予備機を事前に設置することは可とする。

表 3-6 各サーバの停止許容時間

システム	サブシステム		サーバ※1	（1 データセンター内における）各サーバの停止許容時間※2	（1 データセンター内における）サーバ故障（部分故障含む）発生時の修理完了時間	要求するシステム稼働率
ERSS	業務システム	プラントデータ収集システム	プラントデータ収集サーバ	—（停止が極めて少ないことを求める）	2 日以内	1 データセンタ内において、99.999%以上
			データベースサーバ	5 分		
		ICS	プラント情報表示サーバ ※3	—（停止が極めて少ないことを求める）		
		TDS	ドメインコントローラサーバ	5 分		-
			XenApp サーバ ※4	5 分		
	運用・監視機能		運用サーバ	2 日 ※5		-
			バックアップサーバ	2 日 ※6		
			仮想管理サーバ ※7	5 分		
			監視サーバ	5 分		
			Syslog サーバ	5 分		
			リモートアクセスサーバ	2 日 ※8		

※1. 「各サーバ」とは、クラスタ等の二重構成とした場合においては当該サーバ群全体を指すものとし、物理的または論理的な単体サーバのことを指すものではない。
※2. 停止許容時間の算定においては、アプリケーション停止は含めないこととし、ハードウェア及びミドルウェアの停止を対象とする。
※3. プラント情報表示サーバは各データセンター4 台以上設置することを基本とする。
※4. XenApp サーバは各データセンター3 台以上設置することを基本とする。
※5. 停止中は管理対象のモジュールへ直接アクセスするなど、代替措置を講ずること。
※6. 日次バックアップまでに障害復旧が間に合わない場合、障害復旧後に手動で日次バックアップを実施すること。
※7. 仮想管理サーバが必要な場合の要件
※8. 必要に応じて現地（原子力規制庁本庁舎）へ入館の上、確認する前提とする

3.5.1.2. 可用性に係る目標値

原則として ERSS の機能停止を生じさせないこととし、第一データセンター、第二データセンターのそれぞれにおいて、単独で稼働率 99.999%を達成することを目標とする。また、データセンターでの障害発生時においては、第一データセンター、第二データセンターのいずれかの環境で業務の継続が可能とすること。

3.5.1.3. 可用性に係る対策

各データセンターに設置する機器のコンポーネントは可能な範囲で冗長化すること。
第一データセンター及び第二データセンターにて機器及びデータを冗長化したシステム構成とし、常時接続先の切り替えを実施できること。
第一データセンターと第二データセンターの監視サーバは、自センター内の各サーバの監視の他、相互に監視サーバ同士の監視を行うこと。

3.5.2. 完全性要件

データの滅失や改変等を防止するため、以下の対策を講じること。

(1) 処理の結果を検証可能とするため、ログ等の証跡を残すこと。
(2) データの複製や移動を行う際に、データが毀損しないよう、保護すること。
(3) データの複製や移動を行う際にその内容が毀損した場合でも、毀損したデータ及び毀損していないデータを特定するための措置を行うこと。
(4) ソフトウェア等の更新時及び設定変更時にシステムのバックアップを取ること。
(5) プラントデータ収集機能にて、データ内容を確認し、正常ならデータベースに格納するが、異常ならその旨ログに出力し、データベースに格納しないこと。

3.6. 拡張性に関する事項

本システムの拡張性に関する事項の要件を以下に示す。

3.6.1. 性能の拡張性

将来的な利用者数の増加やプラントデータの増加に対応するための拡張性を保持するため、以下の要件を満たすこと。

(1) 「3.3 規模に関する事項」、「3.4 性能に関する事項」に示す性能要求を満たせるよう垂直拡張性及び水平拡張性を考慮したシステム構成とすること。
(2) ウェブサーバ及びデータ収集サーバについては負荷分散を用いたクラスタ構成とし、サーバ増加が容易に可能な構成とすること。

3.6.2. 機能の拡張性

関連法令等の改正や原子力事業者によるプラント変更に伴う伝送データ項目の変更への追随性を確保するため、以下の要件を満たすこと。

(1) 利用者ニーズ及び業務環境の変化等に最小コストで対応可能とするため、ERSS を構成するサブシステムの各コンポーネント（ソフトウェアの機能

を特定単位で分割したまとまり）の再利用性を確保すること。

(2) 伝送データ項目の変更等による「プラント情報表示システム（ICS）」のプラント情報表示の変更が容易に行えるような仕組みを導入すること。（例：背景画像とデータ表示の分離等）

3.7. 上位互換性に関する事項

想定される運用期間（機器導入・設置等完了後から 4 年間）中においては OS 及びソフトウェア等のメジャーバージョンアップが必要ないものを選定すること。

3.8. 中立性に関する事項

以下の対策を講じること。

(1) 導入するハードウェアは、特定のベンダーの技術に依存しない、オープンな技術仕様に基づくものとすること。

(2) 導入するハードウェア、ソフトウェア等は、全てオープンなインターフェイスを利用して接続またはデータの入出力が可能であること。

(3) 導入するハードウェア、ソフトウェア等の構成要素は、標準化団体（ISO、IETF、IEEE、ITU、JISC 等）が規程又は推奨する各種業界標準に準拠すること。

(4) 次の情報システム更改の際に、移行の妨げや特定の装置やソフトウェア等に依存することを防止するため、原則として本システム内のデータ形式は XML、CSV 等の標準的な形式で取り出すことができるものとすること。

3.9. 継続性に関する事項

本システムの継続性に関する事項の要件を以下に示す。

3.9.1. 継続性に係る目標値

ハードウェア及びミドルウェアの障害に対しては、24 時間 365 日対応するものとする。

第一データセンター及び第二データセンターの一方又は双方で、本システムの機能がシステム利用者に提供できない障害が発生した場合は、障害を発見した後、直ちに原子力規制庁と対応方法を協議を行い、原子力規制庁の指示に従って速やかに対処するものとする。前記を除く機器の故障については、駆けつけ保守を行うものとし、監視上のアラート発報、もしくは障害の連絡から 2 日以内に修理完了するものとする。これら以外の障害に対しては、原則翌営業日に対応するものとし、可能な限り迅速な復旧を行うものとする。

ディスク障害によるソフトウェアの障害に対しては、システムバックアップ及び日次バックアップを用い、1 日を目途に復旧を行うものとする。

目標復旧地点は、1 日前の時点（１日前の日次バックアップ時点からの復旧等）とする。

災害等発生時の復旧については、規制庁と協議の上、迅速な復旧を行うものとする。
拠点災害などで第一データセンター内 ERSS が業務提供できなくなった場合に備え、第二データセンター内 ERSS は常時切り替え可とする。

3.9.2. 継続性に係る対策

各データセンターに設置する機器は基本冗長化を施し、1 台故障しても機能継続できること(各データセンターで 2 台故障が発生した場合は、他方のデータセンター内 ERSS をホットスタンバイとして機能継続ができること)。
各原子力施設から伝送されるプラントデータは常時、第一データセンターと第二データセンターの双方で受信し、登録すること。
ディスク障害によるソフトウェア障害時にバックアップによる復旧ができること。
本システムの運用管理データのバックアップを各データセンター毎に日次で夜間に取得すること。なお、保持世代は 14 世代以上とすること。

3.10. 情報セキュリティに関する事項

本システムの情報セキュリティに関する事項の要件を以下に示す。

3.10.1. 主体認証

主体認証の実施について、以下の要件を満たすこと。
(1) 本システムの特定の機能を許可された者のみに提供するよう制限する場合、許可された者の認証を行う機能として、十分な強度のパスワード入力を求める等の方式を採用すること。
(2) 主体認証を行う場合、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。
(3) 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。

3.10.2. アクセス制御

アクセス制御の実施について、以下の要件を満たすこと。
(1) 本システムの特性、本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。
(2) 端末からのアクセスに対し、IP アドレスによるアクセス制御ができる機能を設けること。

3.10.3. 権限管理

権限管理の実施について、以下の要件を満たすこと。
(1) 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。

3.10.4. ログの取得・管理

ログの取得・管理の実施について、以下の要件を満たすこと。

(1) 本システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログを取得すること。
(2) 本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、本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、5 年間 の期間保管するとともに、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能等）を備えること。
(3) 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、本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。
(4) 本システムにおいて、その特性に応じてログを取得する目的を設定した上で、ログを取得する対象の機器等、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。
(5) ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざん等の脅威の軽減）のための措置を含む設計とすること。
(6) 本システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。

3.10.5. 暗号・電子署名

暗号・電子署名の実施について、以下の要件を満たすこと。

(1) 暗号化において「電子政府推奨暗号リスト」に記載されたアルゴリズムを用いること。
(2) 暗号化アルゴリズムの危殆化に関する情報を入手して規制庁と共有すること。

3.10.6. ソフトウェアの脆弱性対策

ソフトウェアの脆弱性対策の実施について、以下の要件を満たすこと。

(1) サーバ装置、端末及び通信回線装置の設置又は運用開始時に、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。
(2) 利用するソフトウェアは運用期間（４年）とサポート期間　を想定して選定し、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。
(3) 公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上で採り得る対策がある場合は、当該対策を実施すること。
(4) サーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による本システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。
(5) サーバ装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処すること。

3.10.7. 不正プログラム対策

不正プログラム対策の実施について、以下の要件を満たすこと。

(1) 統合原子力防災ネットワーク側の不正プログラム対応に合わせ、サーバ装置及び端末に不正プログラム対策ソフトウェアの導入等の対策を講ずること。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。

(2) 想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。

3.10.8. 標的型攻撃対策

標的型攻撃対策の実施について、以下の要件を満たすこと。

(1) 本システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。対策として、サーバ装置等の機器において、自動再生（オートラン）機能の無効化、外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定、使用を想定しない USB ポートの無効化を実施すること。

(2) 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。

(3) 本システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講ずること。

3.10.9. 情報セキュリティ対策の管理体制

次期システム請負事業者は、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、原子力規制庁に書面で提出すること。次期システム請負事業者の情報セキュリティ対策の管理体制については、以下の要件を満たすこと。

(1) 本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。

(2) 本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、原子力規制庁と次期システム請負事業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。

(3) 次期システム請負事業者の資本関係、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。

3.10.10. 情報セキュリティ対策の実施

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) 本システムの基盤となる統合原子力防災ネットワーク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、情報セキュリティ対策に関する運用管理規程（原子力規制委員会情報セキュリティポリシー）等に基づいたセキュリティ要件を策定すること。

(2) 情報セキュリティインシデントが発生した際における、対応手順や報告手順等を事前に取り決めておくこと。
(3) 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原子力規制庁に報告し、承認を得ること。
(4) 情報セキュリティ対策の履行状況について原子力規制庁に定期的に報告を行うこと。
(5) 情報セキュリティ対策の完了後 1 年以内に次期システム請負事業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、次期システム請負事業者は無償で速やかに必要な措置を講ずること。

3.10.11. 要機密情報の取り扱い

原子力規制庁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、本業務以外の目的で利用しないこと。また、本業務において次期システム請負事業者が作成する情報については、原子力規制庁からの指示に応じて適切に取り扱うこと。

3.10.12. 情報セキュリティ事故発生時の監査対応

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次期システム請負事業者において本業務に係る情報セキュリティ事故が発生したときは、必要に応じて原子力規制庁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。

3.10.13. 要機密情報の返却・廃棄

原子力規制庁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。また本業務において次期システム請負事業者が作成した情報についても、原子力規制庁からの指示に応じて適切に廃棄すること。電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。

3.10.14. 原子力規制委員会情報セキュリティポリシーの準拠

本システムを構築・改良する業務にあっては、次期システム請負事業者は、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システムを構築すること。

3.10.15. ネットワークサービスの情報セキュリティ対策

ネットワークサービス（通信回線、モバイル、インターネット、データセンター等）提供事業者は（独）情報処理推進機構の下記の情報を参照し、情報セキュリティ対策を実施すること。

(1) 「セキュリティエンジニアリング-ネットワークサービス事業者向けのページ」
http://www.ipa.go.jp/security/awareness/isp/isp.html

3.10.16. サーバ装置の情報セキュリティ対策

サーバ装置における情報セキュリティ対策として、以下を実施すること。

(1) 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、不正な操作、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。

(2) 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。

(3) サーバ装置に対し、定期的に脆弱性診断を実施すること。

(a) サーバ構築時

(ｱ) ハードウェア、ミドルウェア及びソフトウェアに関するセキュリティ情報を確認し、運用開始までに必要な対策（セキュリティパッチの適応等）を行うこと。

(ｲ) アプリケーションについては、開発者側で必要な脆弱性診断を行い、脆弱性が見つかれば運用開始までに解消すること。

(b) 運用・保守フェーズ

(ｱ) ハードウェア、ミドルウェア及びソフトウェアに関するセキュリティ情報を随時確認する。対応が必要な場合、通常は月次報告会で報告し、年 2 回実施する定期点検時に必要な対策（セキュリティパッチの適応等）を行うこと。緊急性がある場合は即時報告とする。緊急性がある対応は別途契約で対応する。

(ｲ) アプリケーションについては、改修のタイミングで開発者側で必要な脆弱性診断を行い、脆弱性が見つかれば改修版の運用開始までに解消すること。

(4) 通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずること。

(5) 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。

(6) 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定期的に確認し、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。

(7) サーバ装置上の不要なサービスの無効化及びサーバにおけるポートの遮断を行うこと。

(8) サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を検知する必要がある場合は、当該サーバ装置を監視するための措置を講ずること。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。

(9) サーバ装置の運用を終了する際に、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。

3.10.17. ウェブサーバにおける情報セキュリティ対策

ウェブサーバにおける情報セキュリティ対策として、以下を実施すること。

(1) ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。

(2) サービスの利用者の個人に関する情報を通信する場合等、通信時の盗聴等による情報の漏えいを防止する必要がある場合は、暗号化の機能及び電子証明書による認証の機能を設けること。

(3) 本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。

(4) 情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。
(5) ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。また、運用時においても、これらの対策に漏れが無いか定期的（年 2 回の定期点検時）に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。
(6) ウェブサーバに対し、定期的に脆弱性診断（「3.10.16 サーバ装置の情報セキュリティ対策 (3)」の脆弱性診断と同様）を実施すること。

3.10.18. データベースサーバにおける情報セキュリティ対策

データベースサーバにおける情報セキュリティ対策として、以下を実施すること。
(1) データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。
(2) データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。
(3) データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。
(4) データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。
(5) データベースサーバに対し、定期的に脆弱性診断（「3.10.16 サーバ装置の情報セキュリティ対策 (3)」の脆弱性診断と同様）を実施すること。

3.10.19. 通信回線における情報セキュリティ対策

通信回線における情報セキュリティ対策として、以下を実施すること。
(1) 通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずること。
(2) 不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離すること。
(3) 通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。
(4) 通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けること。
(5) 要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。
(6) 通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。
(7) 通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。
(8) 通信回線装置を要管理対策区域に設置すること。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにすること。
(9) サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。
(10) サービスの継続性を確保するため、情報システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減

する機能を備えること。
(11) 本システムと統合原子力防災ネットワークとの接続間にファイアウォールを設置し、不要な通信を遮断する機能を備えること。
(12) 通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。
(13) 保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保すること。
(14) 電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、契約時に取り決めておくこと。
(15) 情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずること。
(16) 経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行うこと。
(17) 通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図ること。
(18) 本システムの情報セキュリティの確保が困難な事由が発生した場合には、本システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更すること。
(19) 通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずること。

3.10.20. 品質報告およびセキュリティ報告

次期システム請負事業者は、本システムの構築・改良等が完了し運用を開始する前に、次期システム請負事業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。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。

3.10.21. 情報セキュリティ対策の報告

次期システム請負事業者は、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報告すること。

3.10.22. 情報セキュリティに係るサービスレベルの保証

次期システム請負事業者は、原子力規制庁と協議の上、情報セキュリティに係るサービスレベルの保証について取り決めを行い、これを満たしていることを原子力規制庁に定期的に報告すること。

3.10.23. 運用管理機能の定義

次期システム請負事業者は、本システムの設計を行うに当たり、本システム運用時のセキュリティ監視、真正確認、権限管理等のセキュリティ機能を管理

するための機能、情報セキュリティインシデントの発生時に行う対処及び復旧に係る機能、証跡保全の機能等の運用管理機能を定義し、設計書、セキュリティ対策実装方針書等に記載の上で原子力規制庁に提出し、承認を得ること。

3.10.24. 情報セキュリティインシデント発生監視機能の設計・構築

次期システム請負事業者は、情報セキュリティインシデントの発生を監視するために必要な以下の機能について設計・構築を行い、運用方法・運用手順を設計書、セキュリティ対策実装方針書等に記載して原子力規制庁に提出し、承認を得ること。

(1) サーバ装置等の機器の動作を監視する機能

3.10.25. 情報システムに関する脆弱性への対策

次期システム請負事業者は、本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、情報セキュリティ対策結果報告書に実施結果を記載の上、原子力規制庁に報告し、承認を得ること。

(1) 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本システムの構成要素としないこと。
(2) 開発時に本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、原子力規制庁へ報告し、承認を得ること。
(3) セキュリティ侵害につながる脆弱性が本システムに存在することが発覚した場合に、原子力規制庁へ報告し、修正を施すこと。
(4) サーバ装置、端末及び通信回線装置の設置又は運用開始時に、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。
(5) 本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、原子力規制庁へ報告すること。
  (a) 脆弱性の原因
  (b) 影響範囲
  (c) 対策方法
  (d) 脆弱性を悪用する不正プログラムの流通状況
(6) 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。
(7) 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。
(8) 公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上で採り得る対策がある場合は、当該対策を実施すること。
(9) サーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による本システムへの影響を考慮した上で、以下の内容を含むソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。また、脆弱性対策計画は原子力規制庁に報告し、承認を得ること。
  (a) 対策の必要性
  (b) 対策方法
  (c) 対策方法が存在しない場合の一時的な回避方法

(d) 対策方法又は回避方法が本システムに与える影響
(e) 対策の実施予定
(f) 対策試験の必要性
(g) 対策試験の方法
(h) 対策試験の実施予定

(10) 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。
(11) 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。
(12) サーバ装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処すること。なお、脆弱性対策の状況を確認する間隔は、可能な範囲で短くすること。

3.10.26. セキュリティ対策実装方針書の策定

次期システム請負事業者は、本システムの構築を行うにあたり、以下を実施することをセキュリティ対策実装方針書に記載のうえ、原子力規制庁に提出し、承認を得ること。

(1) 本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) 本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

3.10.27. 構築・改修における情報セキュリティ対策

次期システム請負事業者は、本システムの構築・改修等において、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、原子力規制庁に報告すること。

(1) 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。
(2) 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。
(3) 情報セキュリティの観点から実施した試験の実施記録を保存すること。

3.10.28. 開発工程における情報セキュリティ対策

開発工程における情報セキュリティ対策として、以下を実施すること。

(1) 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。
(a) ソースコードの変更管理
(b) ソースコードの閲覧制限のためのアクセス制御
(c) 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
(2) 本システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従うこと。

(3) 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。

3.10.29. 機器等の納入時又は本システムの受入れ時の情報セキュリティ対策

次期システム請負事業者は、機器等の納入時において、以下の要件が満たされていることを原子力規制庁へ報告し、承認を得ること。

(1) 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。
(2) 機器等に不正プログラムが混入していないこと。

3.10.30. 運用及び保守実施要領書の策定における情報セキュリティ対策

次期システム請負事業者は、以下を運用及び保守実施要領書に記載し、原子力規制庁へ提出し、承認を得ること。また、運用及び保守実施要領書に則り、本システムに実装されたセキュリティ機能を適切に運用すること。

(1) 本システムの運用環境に課せられるべき条件の整備
(2) 本システムのセキュリティ監視を行う場合の監視手順や連絡方法
(3) 本システムの保守における情報セキュリティ対策
(4) 運用中の本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

3.10.31. アプリケーション・コンテンツの不正プログラム対応

次期システム請負事業者は、提供するアプリケーション・コンテンツに不正プログラムが含まれていないことを確認し、原子力規制庁へ報告し、承認を得ること。

(1) アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。
(2) 当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認すること。
(3) 提供するアプリケーションが脆弱性を含まないこと。
(4) 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。
(5) 電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。改ざん等がなく真正なものであることを確認できる手段の提供として電子証明書を用いた署名を用いるとき、政府認証基盤（GPKI）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。また、電子証明書を利用する場合は、有効期限切れとならないように定期的に確認を行うこと。
(6) 提供するアプリケーション・コンテンツにおいて、本システム外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTML ソースを表示させるなどして確認すること。必要があって当該機能を含める場合は、原子力規制庁外へのアクセスが情報セキュリティ上安全なものであることを確認すること。

(7) 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンの OS やソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OS やソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。
(8) サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

3.10.32. 更改又は廃棄における情報セキュリティ対策

次期システム請負事業者は、本システムの更改又は廃棄を行う場合は、本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、原子力規制庁へ報告し、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、原子力規制庁へ提出すること。

(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

3.10.33. リモート環境の構築における情報セキュリティ対策

次期システム請負事業者は、保守回線や次期システム請負事業者側の環境を用意することで、原子力規制庁のリモート環境を利用した運用・保守体制を構築できる。

リモート環境の要件は以下の通りである。

(1) 保守回線の構築
  (a) 保守回線は、専用回線か、IPSec を用いてセキュリティを高めた VPN 接続の何れかで実現すること。
  (b) 保守回線の構築・維持は次期システム請負事業者が行うこと。
(2) 次期システム請負事業者側設備の構築
  (a) 次期システム請負事業者は、次期システム請負事業者側アクセスサーバを１台用意すること。
  (b) 次期システム請負事業者は、次期システム請負事業者側設備において、原子力規制庁側のアクセスサーバへ接続する機器は、この次期システム請負事業者側アクセスサーバのみとすること。
  (c) 次期システム請負事業者は、次期システム請負事業者側アクセスサーバにログインしなければ原子力規制庁側のアクセスサーバにログインできないように設備を構築すること。
  (d) 次期システム請負事業者は、次期システム請負事業者側アクセスサーバ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義し、設計書、セキュリティ対策実装方針書等に記載の上で原子力規制庁に提出し、承認を得ること。
(3) ログの保存と不正アクセスへの対応
  (a) 次期システム請負事業者は、原子力規制庁に導入するアクセスサーバにおいて、利用者のログイン／ログアウト情報を記録したアクセスログを自動生成し、保存するように設定すること。

(b) 次期システム請負事業者は、次期システム請負事業者側アクセスサーバから原子力規制庁側アクセスサーバへアクセスする際は、次期システム請負事業者側アクセスサーバのアクセスログ及び操作ログを必ず生成し、暗号化して保存すること。
(c) ログの保存は原則 5 年間とするが、システム上の問題等により 5 年の保存が難しい場合は別途原子力規制庁と協議の上、保存期間を決定するものとする。
(d) 原子力規制庁が要求した場合、次期システム請負事業者は次期システム請負事業者側アクセスサーバのアクセスログと操作ログを提出すること。
(e) 不正アクセス等が疑われる場合、次期システム請負事業者は、次期システム請負事業者側アクセスサーバのアクセスログと操作ログと原子力規制庁側アクセスサーバのアクセスログを合わせて不正アクセスの究明を行うこと。

(4) 次期システム請負事業者設備の撤去
(a) リモート環境の運用を終了、又は更新等で設備を撤去する場合には、次期システム請負事業者側設備の電磁的記録媒体に記録されている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

本システムの稼働環境に関する事項の要件を以下に示す。

3.11.1. ハードウェア構成

本システムのハードウェア構成を以下に示す。

3.11.1.1. ハードウェア構成図

本システムのハードウェア構成案を、「別紙 13　情報システム稼働環境に関する事項（ハードウェア構成（案））」に示す。なお、別紙 13 に示すハードウェア構成は次期システムの各要件及び現行システムのハードウェア構成を基に検討した案である。次期システムはこれに縛られるものではなく、次期システムの各要件を満たした上で性能や可用性が同等以上である、導入開発・運用コストの低減を図るなど、本システムの構築・運用するにあたり合理的なハードウェア構成とすること。

3.11.1.2. ハードウェア要件

本システムを構成するハードウェアの要件を以下に示す。

(1) ハードウェア要件

本システムを構成するハードウェア製品の要件案を「別紙 14　情報システム稼働環境に関する事項（ハードウェア要件（案））」に示す。ただし、別紙 14 のハードウェア要件は、次期システムに求める各要件及び現行システムのハードウェア要件を基に検討した案であり、本システムはこれに縛られるものではない。なお、提示した案と異なるハードウェア構成、ハードウェア製品を提案する場合は下記要件は必須とした上で提案すること。

(a) 機器性能については現行機器以上の性能とすること。

(b) 以下のハードウェア要件については、代替の構成は認めない。

(ｱ) プラントデータ収集サーバおよびデータベースサーバについては物理サーバとすること。

(ｲ) プラント情報表示 Web サーバ、XenApp サーバはハードウェア及びミドルウェアの単一障害で各データセンター内の機能停止とならない構成（ハードウェア構成・ミドルウェア構成）とすること。

(ｳ) プラント情報表示 Web サーバは、各データセンター4 台以上を基本とすること。

(ｴ) TDS 用に各データセンターと規制庁本庁舎内に NAS を配置すること。ディスクサイズは各 8TB 以上とすること。

- E ドライブ・・・現在、ERSS にて運用しているドライブ：2TB
- F ドライブ・・・構築当初の環境が格納されているドライブ：2TB
- G ドライブ・・・1 回／月のバックアップデータが格納されているドライブ：4TB

(ｵ) TDS 用に構築するサーバは XenApp サーバとし、各データセンター3 台以上を基本とすること。

(ｶ) XenApp サーバのメモリサイズは 32GB 以上とすること。

(2) ハードウェア要件に係る補足

本システムでは、現行システムから以下に示す変更が行われるため、それらを考慮してハードウェアの追加や、仕様・数量等の追加・変更を行うこと。

(a) プラントデータ収集システム

(ｷ) 以下のような観点で伝送データ項目の追加・変更を行う。

- 原子力災害発生時の各種判断に必要な情報
- 新規制基準への対応にともなう SA 設備等の追加

(ｸ) 障害時の切り分けを迅速にするため、プラントデータ収集サーバおよびデータベースサーバについては物理サーバとすること。

(b) プラント情報表示システム（ICS）

(ｱ) 伝送データの追加項目をユニット情報画面に追加する。

(ｲ) トレンドグラフのポップアップ表示は 1 度に 4 画面程度同時に表示可能とする。

(ｳ) 伝送データの追加項目について、ユニット情報画面への項目を追加する。

(ｴ) 現行システムで設けている 1 端末あたり 1 プロセスのみ起動可能とする制限を解除し、1 端末において複数プラント情報を同時に表示可能とする。

(オ) 現行プラント情報表示システムで使用している「Adobe Flash」は、2020 年に廃止されるため、他の方法（例：HTML5 の Canvas を使用する方法、等）に変更する。
(カ) 支援情報の追加・変更を容易に行える仕組みを導入する（例：所定フォルダに格納した支援情報ファイルを自動的にリスト化して画面上に表示可能とし、ファイルの追加・変更のみで容易に支援情報を追加・変更可能とする、等）。

3.11.1.3. その他の要件

その他のハードウェア要件は以下の通りとする。

(1) 第一データセンター、第二データセンター及び原子力規制庁本庁舎のサーバ室で、本システムを構築するに必要なラック及び電源設備は、原子力規制庁が提供するものとする。ただし、本システムの機器をラックにセットアップするために必要な資材、用具等はすべて次期システム請負事業者において用意すること。
(2) 本システムのハードウェア機器については、機器等の運搬、撤去、撤去時のデータ消去も実施すること。
(3) 経済産業省が定める「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、適切な製品を選定すること。

3.11.2. ソフトウェア構成

本システムのソフトウェア構成を以下に示す。

3.11.2.1. ソフトウェア構成図

本システムのソフトウェア構成案を、「別紙 11　情報システム稼動環境に関する事項（ソフトウェア構成（案））」に示す。なお、別紙 11 に示すソフトウェア構成は、次期システムに求める要件及び現行システムのソフトウェア構成を基に検討した案である。本システムはこれに縛られるものではなく、次期システムに求める各要件を満たした上で性能や可用性が現行システムと同等以上である、導入開発・運用コストの低減を図れるなど、本システムの構築・運用するにあたり合理的なソフトウェア構成とすること。

3.11.2.2. ソフトウェア製品の要件

本システムを構成するソフトウェア製品の要件を以下に示す。

(1) ソフトウェア要件

本システムを構成するソフトウェア製品の要件案を「別紙 12　情報システム稼働環境に関する事項（ソフトウェア要件（案））」に示す。ただし、別紙 12 のソフトウェア要件は、次期システムに求める各要件及び現行システムのソフトウェア構成を基に検討した案であり、本システムはこれに縛られるものではない。なお、提示した案と異なるソフトウェア構成、ソフトウェア製品及び要件を提案する場合は下記要件を必須とした上で提案すること。

- TDS として構築する XenApp サーバの仮想化ソフトウェアは、Citrix XenApp Enterprise を使用すること。

- ライセンス数はハードウェア要件および利用者数を参考に用意すること。
  - ウィルス対策ソフトウェアについては、統合原子力防災ネットワークで採用したウィルスバスターCorp XG SP1 と DeepSecurit のライセンスを原子力規制庁が必要数用意するので、各サーバに当該ソフトウェアを導入するものとし、設定方法及び運用については、統合原子力防災ネットワーク側と調整すること。当該ソフトウェアで対応できないサーバを採用する場合は、相応のセキュリティが確保できるよう別途対策を用意すること。

(2) ソフトウェア要件に係る補足

本システムでは現行システムから以下に示す変更が行われるため、それらを考慮してソフトウェアの追加や、仕様・数量等の追加・変更を行うこと。

(a) プラントデータ収集システム

(ｱ) 以下のような観点で伝送データ項目の追加・変更を行う。

- 原子力災害発生時の各種判断に必要な情報
- 新規制基準への対応にともなう SA 設備等の追加

(b) プラント情報表示システム（ICS）

(ｳ) 伝送データの追加項目をユニット情報画面に追加する。

(ｴ) トレンドグラフのポップアップ表示は 1 度に 4 画面程度同時に表示可能とする。

(ｵ) 現行システムで設けている 1 端末あたり 1 プロセスのみ起動可能とする制限を解除し、1 端末において複数プラント情報を同時に表示可能とする。

(ｶ) 現行プラント情報表示システムで使用している「Adobe Flash」は、2020 年に廃止されるため、他の方法（例：HTML5 の Canvas を使用する方法、等）に変更する。

(ｷ) 支援情報の追加・変更を容易に行える仕組みを導入する（例：所定フォルダに格納した支援情報ファイルを自動的にリスト化して画面上に表示可能とし、ファイルの追加・変更のみで容易に支援情報を追加・変更可能とする、等）。

3.11.2.3. その他の要件

その他のソフトウェア要件は以下の通りとする。

(1) 導入するソフトウェアにおいて、本システムでは不要な機能については可能な限り停止または制限を行うこと。

(2) 経済産業省が定める「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、適切な製品を選定すること。

(3) 調達するソフトウェアは、運用期間中（稼働後 4 年間）は製品サポートが受けられる製品を選択し、サポートサービスを含めて調達すること。

(4) 運用監視ソフトウェアは、第一データセンター、第二データセンター及び原子力規制庁本庁舎内の本システム設備を対象として構築すること。

3.11.3. ネットワーク構成

本システムのネットワーク構成の要件を以下に示す。

3.11.3.1. ネットワーク構成図

統合原子力防災ネットワークに接続することとする。本調達の範囲外のためネットワーク構成図の記載は省略する。ネットワーク構成の概要は「3.11.1.1 ハードウェア構成図」を参照のこと。

3.11.3.2. ネットワーク回線の要件

統合原子力防災ネットワークに接続することとする。VLAN 構成は、統合原子力防災ネットワークの規定に則ること。

3.11.4. 施設・設備要件

本システムの施設・設備要件を以下に示す。

表 3-7 施設・設備要件

No.	施設名	施設形態	施設・設備要件	補足
1	第一データセンター	民間データセンター	原子力規制庁が指定する、既存のデータセンターを使用すること。	現行システムが設置されているデータセンターである。
2	第二データセンター	民間データセンター	原子力規制庁が指定する、既存のデータセンターを使用すること。	現行システムが設置されているデータセンターである。
3	原子力規制庁本庁舎	原子力規制庁内 サーバ室	原子力規制庁の既存のサーバ室を使用すること。	現行システムが設置されているサーバ室である。

3.12. テストに関する事項

本システムのテスト要件を以下に示す。

(1) 業務、運用、基盤、移行、障害運用の観点でフェーズごとに品質を積み上げるテストを行うこと。
(2) 本番環境に接続してのテストを行う場合は、現行システムに影響のないテスト計画を策定すること。
(3) 基盤検証については、別途調達される訓練データ配信システム（TDS）の TDS 次期システム請負事業者と事前調整を行い計画的に検証を行うこと。
(4) クライアント環境は既存の端末を利用するため、OS、ブラウザの種類、バージョンを合せて検証を行うこと。クライアント環境は「3.2.1.4 システム基盤の方針」を参照。

図 3-2 フェーズ別テストの検証ポイント

検証の観点	単体テスト	結合テスト		総合テスト	受入テスト
業務	条件網羅検証	機能内結合検証 機能間結合検証	外部IF検証/Hookup （各電力,TDS）	機能検証(各拠点) 性能検証	受入検証
運用		機能内結合検証 機能間結合検証	外部接続Hookup （監視システム）	運用検証(各拠点)	
基盤		基盤検証 (TDS稼働検証含む)	外部接続Hookup （統原防NW※）	—	—
移行	—	—		移行検証(各拠点)	—
障害	—	基盤障害検証		システム障害検証 障害時運用検証	—

※ 統合原子力防災ネットワークとの接続確認について、衛星回線を利用した接続確認は対象外

3.12.1. 単体テスト

単体テストの要件を以下に示す。

表 3-8 単体テスト要件

No.	項目	内容	補足
1	目的・内容	(1) プログラム単位で品質を確認すること	
2	テスト環境	(1) 次期システム請負事業者で準備する開発環境とすること	
3	テストデータ	(1) プログラムの処理分岐を網羅できるデータを次期システム請負事業者にて準備すること	

3.12.2. 結合テスト

結合テストの要件を以下に示す。

表 3-9 結合テスト要件

No.	項目	内容	補足
1	目的・内容	(1) 機能単位でプログラムを結合し、設計書の要求事項を満たしていることを確認すること (2) 原子力施設から送付されてくる外部データについて取込確認を行い、インターフェース定義に問題がないことを確認すること (3) 基盤検証については、データベース接続検証、監視機能検証、バックアップ・リストア機能検証、その他管理機能検証を実施後、別途調達される訓練データ配信システム（TDS）との稼働検証を行い、基盤設計に問題がないことを確認すること、また、基盤のみの障害発生ポイントを想定した障害検証を行うこと (4) 外部システムと疎通確認を行い、総合テストの環境準備を行うこと	外部システムとの疎通確認は、原子力施設、TDS、運用機能、統合原子力防災ネットワークの確認を想定する。実施可否はテスト計画時に原子力規制庁と調整すること
2	テスト環境	(1) 次期システム請負事業者で準備する開発環境とすること	
3	テストデータ	(1) 現行システムの本番データを加工してテスト目的に合ったデータを次期システム請負事業者にて準備すること(原子力規制庁と事前確認を行うこと) (2) バリエーションの不足するデータについては、次期システム請負事業者にてデータを作成すること	

3.12.3. 総合テスト

総合テストの要件を以下に示す。

表 3-10 総合テスト要件

No.	項目	内容	補足
1	目的・内容	(1) システム全体を対象とし、業務処理の一連の流れにおいて、本要件定義書で示す各種要件を満たしていることを確認すること (2) 機能検証として、業務を想定したシナリオでの検証を行い、業務要件を満たしていることを確認すること (3) 性能検証として、オンライン、バッチのそれぞれで最大処理を想定した検証を行い、性能要件を満たしていることを確認すること (4) 運用検証として、本番稼働後の体制で監視機能が稼働している状況を想定し、運用手順、マニュアルの検証を行い、運用要件を満たしていることを確認すること (5) 障害検証として、ミドルウェア、ネットワークなど基盤環境の障害発生ポイント別に発生しうる障害を想定した障害復旧手順の検証を行い、障害対策要件を満たしていることを確認すること (6) 移行検証として、移行リハーサルを行い、本番移行と同等の体制、タイムチャートで移行手順、時間配分に問題がないことを確認すること、また、移行リハーサル後にシナリオ検証を行うことで移行データ、初期設定データの整合性を確認すること (7) 外部システムと接続し、外部インタフェースが仕様通り動作すること及び業務運用が支障なく行えることを確認すること (8) TDS との結合テストは、TDS 側と協議してテスト対象の原子力施設を限定して実施すること (9) TDS の全プラントを対象としたテストは TDS 側を主体として実施することとし、次期システム請負事業者は TDS 次期システム請負事業者に協力すること	外部システムとの疎通確認は、原子力施設、TDS、運用機能、統合原子力防災ネットワークの確認を想定する。実施可否はテスト計画時に原子力規制庁と調整すること
2	テスト環境	(1) 利用する機器は本番機器とし、ネットワークは、テスト用ネットワークの使用を基本とすること (2) 原子力規制庁本庁舎、第一データセンター、第二データセンターそれぞれの環境に対し、総合テストを実施すること	
3	テストデータ	(1) 総合テストで使用する各種テストデータについては、移行データ、初期設定データを本番同等に準備する、原子力規制庁と協議し、次期システム請負事業者にて準備すること (2) 外部システムのデータは、原子力規制庁と事前調整の上、現行本番システムのデータを利用すること	

3.12.4. 受入テスト

受入テストの要件を以下に示す。

表 3-11 受入テスト要件

No.	項目	内容	補足
1	目的・内容	(1) システムの機能・性能等が業務目的及び使用意図に合致しているのか、原子力規制庁による妥当性確認を行うこと (2) 確認対象となる機能は、プラントデータ収集システム、プラント情報表示システム（ICS）が提供するすべての機能とし、特に現行システムから変更された機能の確認を行うこと (3) 外部システムを利用した業務が支障なく行えることを確認すること (4) 次期システム請負事業者はテスト計画及びテスト項目の作成支援を実施すること	
2	テスト環境	(1) 利用する機器およびネットワークは本番環境とすること(検証用に第二データセンターを事前切替する)	
3	テストデータ	(1) 総合テスト環境のデータを使用すること	

3.13. 移行に関する事項

本システムの移行に関する事項の要件を以下に示す。

3.13.1. 移行手順

本システムの移行に必要な作業は以下の通りとする。

(1) 移行計画書・コンティンジェンシープランの策定
(2) 移行作業手順書の作成（実施体制、タイムチャートの設定）
(3) 移行判定項目と基準の設定
(4) 移行リハーサルの実施（手順、実施体制、タイムチャートの妥当性確認）
(5) 移行判定
(6) 移行実施、移行結果報告（稼動判定）
(7) 本番切替（初回稼動の支援）
(8) 機器の導入

3.13.1.1. 移行計画書・コンティンジェンシープランの策定

移行計画・コンティンジェンシープランの策定にあたり、以下の事項を考慮すること。

(1) システム移行の概要（スケジュール、実施体制、作業概要、移行範囲等）及び移行方針を検討し、移行計画書を策定すること。
(2) 技術、外部要因、組織又はプロジェクトマネジメント等の観点で、本件と類似する案件で発生した問題等から、移行計画策定時点から本番システム移行の実施までの間において、想定されるリスクを識別し、抽出すること。また、抽出されたリスクについて、定性的又は定量的な分析を行ったうえで、回避、転嫁、軽減及び受容等の対応計画を作成すること。
(3) リスクが顕在化した場合に備え、現行システムを継続して稼働させる等で業務・運用の継続を担保するためのコンティンジェンシープランを策定すること。
(4) 移行計画書、コンティンジェンシープランを策定後、原子力規制庁の承認を得ること。

3.13.1.2. 移行作業手順書の作成（実施体制、タイムチャートの設定）

移行作業手順書の作成にあたり、以下の事項を考慮すること。

(1) 移行の事前に実施する準備作業、移行中の作業及び事後に実施する検証作業等を対象とし、移行に係わるすべての関係者が利用できる移行手順書を作成すること。
(2) 移行作業期間中、特に利用者へ周知すべき事項については、わかりやすい資料を作成すること。
(3) 移行作業の手順に各作業が正しく行われていることの確認を含めること。
(4) 移行作業の手順にチェックポイントを設定し、チェックポイントまでの実施済み作業の結果確認、以降の作業の継続可否などを確認すること。
(5) コンティンジェンシープランに定義した、リスクが顕在化した場合の対応計画を実施するための作業手順を、移行手順書に含めること。
(6) バックアップ等の準備作業、移行作業及び事後作業等を対象とし、移行の関係者全体で情報共有できるタイムチャートを作成すること。
(7) 移行の関係者（原子力規制庁、次期システム請負事業者、TDS 次期システム請負事業者、システム運用支援業者、緊急時ネットワーク監視センター員、原子力事業者、ハードウェアベンダー、ソフトウェアベンダー、ネットワークベンダー等）を含む作業体制図、連絡先一覧を作成すること。
(8) ハードウェア、ソフトウェア、ネットワークに起因するトラブルが発生した場合に、迅速に問い合わせを行うための情報（製品名称、型番、問い合わせのための利用者 ID 等）を整理した構成管理一覧を作成すること。

3.13.1.3. 移行判定項目と基準の設定

移行判定項目と基準の設定にあたり、以下の事項を考慮すること。

(1) 移行作業の開始前の移行判定、本番切替前の稼動判定について、作業の実施可否を判定する確認項目と判定基準を設定すること。
(2) 判定で不可となった場合の対応計画をコンティンジェンシープランに含めること。
(3) 設定した内容について、原子力規制庁の承認を得ること。

3.13.1.4. 移行リハーサルの実施（手順、実施体制、タイムチャートの妥当性確認）

移行リハーサルの実施にあたり、以下の事項を考慮すること。

(1) 移行計画書及び移行手順書に問題がないことを検証するため、本番の各拠点（原子力規制庁本庁舎、第一データセンター、第二データセンター）での本番移行を想定し、1 回以上の移行リハーサルを実施すること。
(2) 外部システム連携（訓練データ配信システム（TDS）、原子力事業者の伝送サーバ）を含めた移行リハーサルを実施すること。ただし、外部システム連携の実施可否は移行計画時に原子力規制庁と調整すること。
(3) 移行リハーサルの実施結果について、結果分析を行い、必要に応じて移行手順書を修正すること。
(4) 移行手順書の最終版を作成後、原子力規制庁の承認を得ること。

3.13.1.5. 移行判定

移行判定にあたり、以下の事項を考慮すること。

(1) 総合テストの検証結果、移行作業の準備状況をもとに、原子力規制庁にて移行作業の開始の承認を得ること。

3.13.1.6. 移行実施、移行結果報告（稼動判定）

移行実施・移行結果報告にあたり、以下の事項を考慮すること。

(1) 移行計画や移行手順書に基づいて作業を実施すること。
(2) コンティンジェンシープラン発動の必要が生じた場合は直ちに原子力規制庁に報告するとともに、判定項目にしたがって判定を行うこと。
(3) 各拠点（原子力規制庁本庁舎、第一データセンター、第二データセンター）のシステム移行作業の完了ごとに、移行計画書に記載されたスケジュール、使用するドキュメント等に基づいた移行結果報告書を作成し、原子力規制庁に提出し本番システム稼動の承認を得ること。

3.13.1.7. 本番切替（初期稼働支援）

本番切替（初回稼動支援）にあたり、以下の事項を考慮すること。

(1) システム移行直後は通常時と比べて多くのトラブルや問い合わせが発生する可能性があることから、初期稼働期間として原子力規制庁に対する作業支援を行うこと。
(2) 初期稼働期間はシステム移行完了後から 1 か月を想定しているが、次期システムの稼働状況を踏まえ、原子力規制庁と協議の上、決定すること。

3.13.1.8. 機器の導入

機器の導入にあたり、以下の事項を考慮すること。

(1) 機器設置施設にサーバなど機器を搬入・設置するに当たり、機器導入計画書を作成し、原子力規制庁の承認を得ること。
(2) 搬入・設置する場所及び周辺環境について、事前に現地調査を実施すること。
(3) 搬入後に行うハードウェア単体での基本動作の確認を初期動作確認手順として取りまとめ、機器導入計画書に含めること。

(4) 機器の導入・設置後、作成した初期動作確認手順に基づき、初期動作確認を実施すること。
(5) 初期動作確認終了後、導入・設置の結果をとりまとめた機器導入結果報告書を作成し、原子力規制庁に提出し承認を得ること。
(6) 障害が発生した場合は直ちに原子力規制庁に報告するとともに、迅速な対応を行うこと。

3.13.2. 移行要件

移行要件は以下の通りとする。

3.13.2.1. 移行スケジュール

本システムの稼働日は、現行システムの保守期限、および現行機器の撤去作業の期限が 2020 年 3 月末となるため、その期限に間に合うように移行を完了すること。ただし、本システム開発スケジュールの都合上、間に合わない場合は、原子力規制庁と移行時期、本番稼働日を検討・調整すること。（現行システムの稼動期間の延長が必要となるため。）

3.13.2.2. 移行対象

本システムの移行作業の対象は以下の通り。

(1) サーバ基盤（第一データセンター、第二データセンター、原子力規制庁本庁舎）
(2) アプリケーションリソース（プラントデータ収集システム、プラント情報システム（ICS））
(3) 端末の起動用ショートカット（原子力規制庁本庁舎、OFC、官邸、原子力事業者本店等）
(4) システム運用
(5) 業務

3.13.2.3. 移行方法

本システムの移行作業の都合により、現行システム及び関連システムのシステム停止を要請することのないよう、業務継続性を確保した移行計画及び移行手順を策定し、作業を行うこと。なお、移行計画に際しての留意事項は以下の通り。

(1) 第一データセンターと第二データセンターのいずれか一方は本番業務が可能な状態を確保すること。
(2) 本システムの切替に際して、原子力施設側のシステム変更は発生しないように計画すること。そのため、各拠点のプラントデータ収集システムのプラントデータ受信サーバは現行システムのサーバと同 IP アドレスを設定して、原子力施設からのデータを受信可能とする。現行サーバをネットワークから切断後、新サーバを接続する手順で切替を行うこと。
(3) 現行システムの原子力規制庁本庁舎内設備は、第一データセンターのドメインコントローラー、NAS 環境を利用しているため、本番切替は同タイミングで実施すること。
(4) サイト URL は現新システムで変更すること。新システム起動用ショートカットは各端末に事前に配布し、現行システム起動用のショートカットは新システムのサービスイン後に各端末から削除すること。ショートカットの配布・削除は原子力規制庁にて実施することとする。

(5) 第二データセンターを受入テスト、教育、引継ぎの目的で事前移行し、問題なければそのまま本番業務の切替を行うこと。受入テスト、教育、引継ぎの期間は予備期間を含めて 5 週間程度を想定すること。原子力規制庁本庁舎、第一データセンターは、第二データセンターの本番稼働後にネットワークの切替を行い、検証を完了した後に本番業務に利用可能とすること。
(6) サーバ基盤は、可能な限り事前移行で待ち受け状態とし、移行日当日の作業は最小限とすること。
(7) 緊急時ネットワーク監視センターの運用監視業務は、第二データセンターが本番業務に切替えるタイミングで新システム運用に切替を行うこと。
(8) 現行システム運用事業者、他の開発事業者等への依頼事項が発生する場合は事前に調整を行うこと。
(9) TDS についても同様の移行方式とすること。

図 3-3 移行作業のスケジュール（案）

3.13.2.4. 移行体制

本システムの移行体制は以下の通り。

(1) 移行準備・移行実施
次期システム請負事業者が中心となって作業を実施する。策定した計画、手順書などの承認は原子力規制庁が行うこと。

(2) 移行判定・稼働判定・コンティンジェンシープランの発動
原子力規制庁が行うこと。

3.13.3. 移行対象データ

データ移行は行わない。

3.14. 引継ぎに関する事項

次期システム請負事業者は、本契約の終了後に他の運用事業者が本システムの運用・保守を受注した場合には、当該事業者に対し、作業経緯、残存課題等についての引継ぎを行うこと。

3.15. 教育に関する事項

本システムの教育対象者の範囲、教育の方法の要件を以下に示す。

3.15.1. 教育対象者の範囲、教育の方法

教育対象者の範囲、教育方法は以下の通りとする。

3.15.1.1. 運用開始前

本システムの運用開始前における教育対象者の範囲、教育の方法の要件は以下の通りとする。

表 3-12 教育に関する要件（運用開始前）

No.	教育対象者の範囲	教育の内容	教育の実施時期	教育の方法	使用教材	教育対象者数	補足
1	システム管理者（原子力規制庁職員）	ICS のロール、機能ごとの機能概要及び操作方法	次期システムへの移行期間中	現行システムからの変更点をまとめた資料及び操作マニュアルを作成し、原子力規制庁にて研修を	・変更点をまとめた資料 ・ICS 操作マニュアル	約 2 名	研修の実施内容、対象者、実施場所、スケジュールは別途調整の上、実施すること

No.	教育対象者の範囲	教育の内容	教育の実施時期	教育の方法	使用教材	教育対象者数	補足
				実施			
2	システム運用支援業者	同上	同上	同上	同上	約 15 名	同上
3	緊急時ネットワーク監視センター員	同上	同上	同上	同上	約 3 名	同上

3.15.1.2. 運用期間中

本システムの運用期間中における教育対象者の範囲、教育の方法の要件は以下の通りとする。

表 3-13 教育に関する要件（運用期間中）

No.	教育対象者の範囲	教育の内容	教育の実施時期	教育の方法	使用教材	教育対象者数	補足
1	システム管理者（原子力規制庁職員）	以下の内容について教育を実施 (1) 監視機能の概要 (2) 監視対象機器の範囲 (3) 監視項目 (4) 障害の判別方法 (5) 障害発生時のフロー等 (6) 障害例一覧	原子力規制庁が指定する実施日（毎年度上期に 1 回）	運用マニュアルを用い、原子力規制庁にて研修を実施	システム運用マニュアル	約 2 名	教育は運用監視マニュアルを用い、学習目的・学習到達目標を定めて初修者でも理解できるようにすること
2	システム運用支援業者	同上	同上	同上	同上	約 15 名	同上
3	緊急時ネットワーク監視センター員	同上	同上	同上	同上	約 3 名	同上

3.15.2. 教材の作成

教材の作成の要件は以下の通りとする。

表 3-14 教材一覧

No.	教材	教材の概要	対象者	補足
1	変更点をまとめた資料	現行システムからの変更点をまとめた資料	(1) システム管理者（原子力規制庁職員） (2) システム運用支援業者 (3) 緊急時ネットワーク監視センター員	
2	ICS 操作マニュアル	以下の項目について記載されていること (1) ICS のロール、機能ごとの機能概要及び操作方法	(1) システム管理者（原子力規制庁職員） (2) システム運用支援業者 (3) 緊急時ネットワーク監視センター員	(1) 担当者の実施する操作に対応した構成であること (2) 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 (3) 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	システム運用マニュアル	以下の項目について記載されていること (1) 監視機能の概要 (2) 監視対象機器の範囲 (3) 監視項目 (4) 障害の判別方法 (5) 障害発生時のフロー等 (6) 障害例一覧	(1) システム管理者（原子力規制庁職員） (2) システム運用支援業者 (3) 緊急時ネットワーク監視センター員	

3.16. 運用に関する事項

運用の全般的な要件を以下に示す。

(1) 「3.9.1 継続性に係る目標値」を達成できる運用体制を整えること。
(2) 運用期間中における本システムの開発環境及びテスト環境を次期システム請負事業者の責任と負担で準備すること。開発環境とテスト環境は同一環境を併用しても構わないこととする。外部接続が必要な場合は、スタブやドライバ等で代用すること。
(3) 運用範囲はアプリケーション、ハードウェア、ミドルウェア及びソフトウェアとする。
(4) ネットワーク機器や管理すべきサービスの構成情報（IP アドレス、ポート接続情報、回線情報等）を管理すること。
(5) 次期システム請負事業者は、システムの運用開始までにシステムで利用を認めるソフトウェア及びアプリケーション一覧を作成すること。運用開始後、一覧へのソフトウェアやアプリケーションの追加等を行う場合は、原子力規制庁の承認を得ること。
(6) 原子力規制庁の依頼内容に基づき、本システムの調査等を行うこと。
(7) 不正プログラム対策ソフトウェアの動作状況やパターンファイルの更新状況の確認を行うこと。
(8) ログを確認し、問題等があれば把握すること。
(9) 本システムを構成する各資産を管理すること。
(10) 運用・保守記録台帳及び障害記録台帳を作成し、インシデント管理、問題管理、変更管理、リリース管理を行うこと。
(11) 運用・保守業務等の作業内容を記録した報告書と共に月次報告書として毎月末毎に作成し、提出すること。また、月 1 回、原子力規制庁にて報告会を行うこと。
(12) 年 1 回、原子力規制庁が実施する現況確認を支援すること。
(13) 年 2 回、第一データセンター、第二データセンター及び原子力規制庁本庁舎内の本システム設備を対象として定期点検を行うこと。なお、第一データセンターと第二データセンターにおける点検は、原則別時間で行うものとし、必要によりシステムの計画停止を行う場合においても、いずれかでは業務継続が可能となるように行うこと。
(14) 定期点検は原子力規制庁との協議による年間運用計画に従い実施するものであるが、実施にあたっては、関係者への周知を行い、実施時間等を調整し、定期点検によって業務に支障が発生しないように行うこと。
(15) 運用に関して以下の法律を遵守すること。
  (a) 高度情報通信ネットワーク社会形成基本法（必須）
  (b) サイバーセキュリティ基本法（必須）
  (c) 国等による環境物品の調達の推進に関する法律・グリーン購入法（任意）
(15) 次期システム請負事業者は、保守回線や次期システム請負事業者側の環境を用意することで、原子力規制庁のリモート環境を利用した運用・保守体制を構築できる。リモート環境構築にあたり、「3.10.33 リモート環境の構築における情報セキュリティ対策」を実施のこと。

3.16.1. 運用管理・監視等要件

本システムの運用管理・監視等要件を以下に示す。

表 3-15 運用管理・監視等要件

No.	運用の分類	運用名	運用内容	補足
1	運転管理・監視	監視全般	(1) 監視範囲は本システム全体とする (2) 監視対象は本システムのアプリケーション、ハードウェア、ミドルウェア及びソフトウェアとする (3) 監視間隔はリアルタイム（分間隔）を基本とすること (4) 監視方法は 24 時間 365 日の自動監視を基本とすること (5) サーバは死活監視、SNMP トラップ監視、CPU、メモリ、ディスクなどのリソース監視、データベース及びアプリケーション稼動状況を確認するプロセス、ログ監視などシステム機能を維持するための監視を行うこと。必要に応じて、監視 Agent 導入を検討すること (6) その他機器についても、死活監視、SNMP トラップ監視、CPU、メモリ、ディスクなどのリソース監視の確認を行うこと (7) 監視対象となるログや SNMP トラップの時刻を統一するため、サーバおよび NW 機器は時刻同期を行うこと (8) アラート発生時は次期システム請負事業者、原子力規制庁、緊急時ネットワーク監視センターに自動で通知される仕組みを構築すること (9) 監視状況は月次報告書を作成し、提出すること (10) 月次の原子力規制庁の報告会にて、監視状況を報告すること	
2		死活監視	(1) 監視対象全般に対し、死活監視を行う	
3		性能監視	(1) 監視対象のハードウェアに対し、CPU、メモリ、ディスク等のリソース監視を行う	
4		稼働状況監視	(1) 監視対象全般に対し、SNMP トラップ監視やプロセス監視、ログ監視を行う	
5		セキュリティ監視	(1) 監視対象全般に対し、ウイルス対策ソフトやファイアウォールのログの監視を行う	
6		アプリケーション監視	(1) 業務ログの監視を行い、原子力施設からのプラントデータの不受信（10 分間）の監視を行う	
7		障害発生時対応	(1) 障害発生時には速やかに原子力規制庁に報告するとともに、その緊急度及び影響度を判断の上、障害検知、障害発生箇所の切り分け、関係事業者への連絡、復旧作業及び復旧後の動作確認、対応報告等を行うこと (2) 駆けつけ保守での対応は、監視上のアラート発報、もしくは障害の連絡から 2 日以内とする (3) 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、恒久的な対応案を作成すること	
8		障害の一次対応	(1) 障害発生後、速やかに障害原因を究明し、障害の切り分けを行うこと	

No.	運用の分類	運用名	運用内容	補足
			(2) 障害管理を行い、障害回復作業中の問い合わせ対応を行うこと	
9	システム操作	バックアップ管理	(1) バックアップ管理は次期システム請負事業者が実施すること (2) バックアップ運用範囲はシステムバックアップ及び業務で使用するデータの日次バックアップとする (3) 日次バックアップは第一データセンター及び第二データセンターそれぞれで取得し、取得タイミングは日次で夜間とし、データ保管は 14 世代以上とすること (4) システムバックアップの取得タイミングはソフトウェア等の更新時及び設定変更時とし、データの保管は 2 世代以上とすること (5) システムバックアップの処理は取得対象のサーバを停止した状態で手動で実施すること (6) 二次バックアップとして、一次バックアップを別物理筐体(バックアップストレージ等)にコピーすること (7) 拠点間でのシステムバックアップデータの複製、退避は行わない	
10		情報システムの設定変更	(1) 本システムの設定変更に係る作業は次期システム請負事業者が実施すること (2) 本システムの軽微な設定変更等を行うこと (3) ネットワーク機器のファームウェアなどの組込みソフトウェアの設定変更等を行うこと (4) 保守に必要となる本システムの設定変更等を行うこと	設定変更は、原子力規制庁からの依頼による
11	ログ管理	業務ログ	(1) 業務アプリケーションのログは、以下のログを出力して管理すること (a) プラントデータ収集システム受信ログ(ソケット通信の接続、受信、送信、切断を出力する) (b) プラント情報 DB 登録ログ(受信データの DB 登録、およびエラーを出力する)(※) (c) プラント情報表示システムアクセスログ（システムの起動、終了、エラー、運用管理操作を出力する） (2) 業務アプリケーションのログはファイルを月次でローテーションし、圧縮後 5 年間保管すること	※データが 10 分間不受信の場合のエラーログは監視機能で監視し、発生時は検知可能とすること
12		システムログ	(1) OS、ミドルウェアのログはファイルを日次でローテーションし、圧縮後 1 年間保持すること	
13	定期点検	システムの点検	(1) 定期点検に係る運用は次期システム請負事業者が実施すること (2) 点検の実施日時は、事前に原子力規制庁の承認を得ること (3) システム LED 確認、機器の清掃、目視確認、異臭確認、異音確認、架内ケーブル接続状態確認、ファン動作確認、システムログ確認、サーバ・ステータス確認等を行い、システムの機能を十分に発揮できる状態に保つこと (4) サーバ機器に対し、脆弱性診断を実施すること	

No.	運用の分類	運用名	運用内容	補足
			(5) ウェブアプリケーションの脆弱性の対策に漏れがないかを確認すること (6) システムに導入されているソフトウェア及びアプリケーションを確認し、利用が認められていないソフトウェア及びアプリケーションの存在確認を実施すること (7) 点検時、システム及びデータ（データベース、その他データ）のバックアップを取得すること	
14		ログ解析	(1) サーバ機器に対し、年 2 回 OS 及びミドルウェアのログ解析を実施すること (2) ログ解析の内容について、原子力規制庁と協議すること	
15		サーバ再起動	(1) サーバ機器に対し、年 1 回再起動を行うこと。その際、各サーバ機器の冗長構成を考慮し、原則機能停止を起こさないように計画的に行うこと (2) サーバ機器の再起動を行う際、システム領域を含めたフルバックアップをバックアップストレージに取得すること	
16		修正プログラム又はアップデートファイルの適用	(1) OS、ハードウェア、ミドルウェア及びソフトウェアについて、ベンダーから提供されるアップデートファイル等の適用を行うこと (2) 緊急でアップデートファイル等の適用が必要な場合は、別途契約とする	
17		点検結果報告	(1) 点検成績書を作成し、原子力規制庁に提出すること (2) 定期点検報告書を作成し、原子力規制庁にて報告会を実施すること	

3.16.2. 運用サポート業務

運用サポート業務の要件は以下の通りとする。

(1) 「3.9.1 継続性に係る目標値」を達成できるように受付窓口を設置し、ハードウェア障害、ミドルウェア障害、ソフトウェア障害、アプリケーション障害及びネットワーク障害の受付を行い、次期システム請負事業者がこれらの障害を切り分けること。
(2) 受付窓口は、24 時間 365 日電話にて対応すること。
(3) 障害を切り分けた結果、障害原因が本システム以外のアプリケーションと判明した場合は、該当アプリケーションの保守事業者と連携・協力し、障害復旧対応に努めること。

3.16.3. 業務運用支援

ERSS に係る業務の運用支援作業は、別途調達の業務で行うため、本書の対象外とする。

3.16.4. 運用実績の評価と改善

運用実績の評価と改善の要件は以下の通りとする。

(1) 次期システム請負事業者は、毎月本システムの運用に関する作業実績やサービスレベルの達成状況等をとりまとめ、評価すること。評価の結果、改善が必要と判断された事項は要因分析を行い、改善措置を検討すること。
(2) 月次報告書には、運用業務の評価結果、改善すべき事項及び改善措置（担当者、実施内容、実施期限）を記載すること。

上記内容を月次の報告会で原子力規制庁に報告すること。

3.17. 保守に関する事項

保守の全般的な要件を以下に示す。

(1) 「3.9.1 継続性に係る目標値」を達成できる保守体制を整えること。
(2) 保守範囲はすべてのアプリケーション、ハードウェア、ミドルウェア及びソフトウェアとする。
(3) メンテナンス等の作業はすべて次期システム請負事業者が行うこと。
(4) 重大障害とは、ハードウェア又はミドルウェアの機能障害により、第一データセンター及び第二データセンターの一方又は双方で、本システムの機能がシステム利用者に提供できない障害が発生した場合とし、重大障害の場合には、休日・夜間を問わず、迅速な障害復旧を行うこと。
(5) 運用・保守記録台帳及び障害記録台帳としてのインシデント管理台帳を作成し、運用・保守業務等の作業内容を記録した報告書と共に月次報告書として毎月末毎に作成し、提出すること。また、月 1 回、原子力規制庁にて報告会を行うこと。
(6) 次期システム請負事業者は、保守回線や次期システム請負事業者側の環境を用意することで、原子力規制庁のリモート環境を利用した運用・保守体制を構築できる。リモート環境構築にあたり、「3.10.33 リモート環境の構築における情報セキュリティ対策」を実施のこと。

3.17.1. アプリケーションプログラムの保守要件

アプリケーションプログラムの保守要件は以下の通りとする。

表 3-16 アプリケーションプログラムの保守要件

No.	分類	項目	内容	補足
1	前提	保守対象	(1) 本システムを構成するサブシステムのうち、プラントデータ収集システム、プラント情報表示システム（ICS）を対象とすること	
2		保守時間	(1) 保守受付窓口は 24 時間 365 日、電話又はメールによる連絡に速やかに対応すること (2) 保守対応は原則翌営業日の定時（17 時）までに対応すること	保守時間内に対応が完了しない場合、直ちに原子力規制庁の連絡し、指示を仰ぐこと
3		対応方法	(1) 「3.5.1 可用性要件」を満たす対応ができる体制を構築すること	
4	作業要件	維持・更新	(1) システムの構成及び各種設定情報に係る維持・管理を行うこと	

No.	分類	項目	内容	補足
5		問い合わせ	(1) システムに関する動作仕様や操作方法等の技術的問い合わせに対し、調査及び回答を行うこと	
6		障害対応	(1) 障害が発生した場合は、原子力規制庁と連携し、障害の原因を調査し、特定すること (2) 次期システム請負事業者の責任と負担においてプログラムの修正を行うこと (3) 障害原因が本システム以外のアプリケーションと判明した場合は、該当アプリケーションの保守事業者と連携・協力し、障害復旧対応に努めること (4) 障害対応時、施設及び他の機械等に損壊を生じさせた場合は、次期システム請負事業者の責任において補償すること	

3.17.2. ハードウェアの保守要件

ハードウェア保守の保守要件は以下の通りとする。

表 3-17 ハードウェアの保守要件

No.	分類	項目	内容	補足
1	前提	保守対象	(1) 第一データセンター、第二データセンター及び原子力規制庁本庁舎内に設置された本システムを構成するハードウェアを対象とすること	
2		保守時間	(1) 保守受付窓口は 24 時間 365 日、電話又はメールによる連絡に速やかに対応すること (2) 保守対応は 24 時間 365 日対応すること	
3		対応方法	(1) 「3.5.1 可用性要件」を満たす対応ができる体制を構築すること	
4	作業要件	維持・更新	(1) ファームウェアなどの組込みソフトウェアの設定変更やアップデートの情報を収集すること (2) ファームウェアなどの組込みソフトウェアの設定変更やアップデートを提供すること (3) 本システムにおけるサーバやディスク等の不具合を受け付けること (4) ハードウェアの修理又は交換対応をすること	
5		問い合わせ	(1) ハードウェアに関する動作仕様や操作方法等の技術的問い合わせに対し、調査及び回答を行うこと	
6		障害対応	(1) 障害が発生した場合は、原子力規制庁と連携し、障害の原因を調査し、特定すること	

3.17.3. ミドルウェアの保守要件

ミドルウェアの保守要件は以下の通りとする。

表 3-18 ミドルウェアの保守要件

No.	分類	項目	内容	補足
1	前提	保守対象	(1) 第一データセンター、第二データセンター及び原子力規制庁本庁舎内に設置された本システムを構成するハードウェアに導入されたミドルウェアを対象とすること	
2		保守時間	(1) 保守受付窓口は 24 時間 365 日、電話又はメールによる連絡に速やかに対応すること (2) 保守対応は 24 時間 365 日対応すること	
3		対応方法	(2) 「3.5.1 可用性要件」を満たす対応ができる体制を構築すること	
4	作業要件	維持・更新	(1) アップデートファイル（セキュリティパッチ等）の情報を収集すること (2) アップデートファイル（セキュリティパッチ等）を提供すること (3) ミドルウェアの不具合を受け付けること	
5		問い合わせ	(1) ミドルウェアに関する動作仕様や操作方法等の技術的問い合わせに対し、調査及び回答を行うこと	
6		障害対応	(1) 障害が発生した場合は、原子力規制庁と連携し、障害の原因を調査し、特定すること	

3.17.4. ソフトウェア製品の保守要件

ソフトウェアの保守要件は以下の通りとする。

表 3-19 ソフトウェアの保守要件

No.	分類	項目	内容	補足
1	前提	保守対象	(1) 第一データセンター、第二データセンター及び原子力規制庁本庁舎内に設置された本システムを構成するハードウェアに導入されたソフトウェアを対象とすること	
2		保守時間	(1) 保守受付窓口は 24 時間 365 日、電話又はメールによる連絡に速やかに対応すること (2) 保守対応は原則翌営業日に対応するものとする	
3		対応方法	(1) 「3.5.1 可用性要件」を満たす対応ができる体制を構築すること	
4	作業要件	維持・更新	(1) アップデートファイル（セキュリティパッチ等）の情報を収集すること (2) アップデートファイル（セキュリティパッチ等）を提供すること (3) ソフトウェア製品の不具合を受け付けること	
5		問い合わせ	(1) ソフトウェアに関する動作仕様や操作方法等の技術的問い合わせに対し、調査及び回答を行うこと	
6		障害対応	(1) 障害が発生した場合は、原子力規制庁と連携し、障害の原因を調査し、特定すること	

3.17.5. データの保守要件

データの保守要件は以下の通りとする。

表 3-20 データの保守要件

No.	分類	項目	内容	補足
1	前提	保守対象	(1) 本システムを構成するサブシステムのうち、プラントデータ収集システム、プラント情報表示システム（ICS）が扱うデータを対象とすること	
2		保守時間	(1) 保守受付窓口は 24 時間 365 日、電話又はメールによる連絡に速やかに対応すること (2) 保守対応は原則翌営業日に対応すること	
3		対応方法	(1) 「3.5.1 可用性要件」を満たす対応ができる体制を構築すること	
4	作業要件	伝送データ異常	(1) 原子力事業者より伝送されるプラントデータに異常・不整合が発生した場合、それを検出し、原因を調査して復旧作業を行うこと。 (2) データ異常の原因が本システムの場合、再発防止策を策定し、原子力規制庁の承認を得ること	
5		設定データ異常	(1) システムの設定データ又はマスタデータに異常が発生した場合、復旧対応を行うこと	

3.17.6. 保守実績の評価と改善

保守実績の評価と改善の要件は以下の通りとする。

(1) 次期システム請負事業者は、毎月本システムの保守に関する作業実績やサービスレベルの達成状況等をとりまとめ、評価すること。評価の結果、改善が必要と判断された事項は要因分析を行い、改善措置を検討すること。
(2) 月次報告書には、保守業務の評価結果、改善すべき事項及び改善措置（担当者、実施内容、実施期限）を記載すること。
(3) 上記内容を月次の報告会で原子力規制庁に報告すること。

3.18. 機器の撤去

(1) 次期システムの請負事業者は、本契約の終了時に機器を撤去すること。
(2) 撤去時期、移行データの有無等に関しては原子力規制庁の指示に従うこと。
(3) データの抹消及び移行は「3.10.32. 更改又は廃棄における情報セキュリティ対策」に従うこと。