公開系 Web サイト用サーバ基盤の利用

仕様書

Ⅰ. 一般仕様

1. 件名

公開系 Web サイト用サーバ基盤の利用

2. 目的

本調達は、日本原子力研究開発機構（以下、「当機構」という。）の外部に向けた公開 Web サイトをクラウドサービスで運用することを目的とする。

3. 調達物品及び構成内容

公開系 Web サイト用サーバ基盤　　一式
当機構と受注者環境を接続するネットワーク　　一式

4. 調達方法

サービスの利用契約とする。

5. 納期

令和 8 年 1 月 1 日から令和 8 年 3 月 31 日までに設定を完了し、
令和 8 年 4 月 1 日からサービスを利用できる環境を提供すること。
「8.提出図書」を令和 8 年 4 月 30 日までに提出すること。

6. サービス利用期間

令和 8 年 4 月 1 日～令和 9 年 9 月 30 日（18 ヶ月間）
※令和 8 年 1 月 1 日～令和 8 年 3 月 31 日を環境構築期間とする。

7. 納入場所

茨城県那珂郡東海村白方 2-4
日本原子力研究開発機構　原子力科学研究所　情報交流棟南ウィング
システム計算科学センター サイバーセキュリティ統括室

8. 提出図書

本調達において、落札後に必要な提出書類は、以下のとおりである。なお、下記指定の部数に加え、電磁的記録媒体（CD-R または DVD-R）1 部を提出すること。

① サービス利用許諾書　　1 部
② 基本・詳細設計書　　1 部
③ 機器構成表　　1 部

④ ネットワーク構成図　1 部
⑤ マニュアル　1 部
⑥ サポート体制表　1 部
⑦ 検査要領書（検査実施の 2 週間前）（要確認）　1 部
⑧ 検査成績書　1 部
⑨ 従量課金分試算表　1 部

9. その他

9.1. 検収条件

(1) 令和 8 年 3 月 31 日までにサービスを利用できる環境を構築し、検査要領書記載の検査に合格すること。なお、検査に用いる検査要領書は受注者が作成し、事前に当機構に提出して確認を得ること。

(2) 令和 8 年 4 月 30 日までに「8.提出図書」が「7.納入場所」にすべて提出されていること。

9.2. サービス料金の支払いについて

(1) サービス利用料の内、バックアップを除く部分を月額固定の料金(以下この料金を「月額固定料金」という)として算出し請求すること。

(2) バックアップの利用料金に関しては月内に利用した利用実績に応じた料金(以下この料金を「バックアップ従量課金分料金」という)を請求すること。なお、入札は総価で行うため、仕様上の最大利用容量(40TB)を想定し入札すること。

(3) バックアップ従量課金分料金はその月に利用した容量(GB)に応じて精算するため、1GB あたりの単価を示すこと。

(4) 各月のサービス利用料は月額固定料金とバックアップ従量課金分料金を合算し請求すること。

(5) 「6.サービス利用期間」に記載の環境構築期間(令和 8 年 1 月 1 日～令和 8 年 3 月 31 日)に設計費･構築費･工事費･通信費･作業費等の環境整備に料金が発生する場合は、その対価をサービス利用期間(月数)で均し、各月の利用料金に含めて請求すること。

9.3. 秘密保持義務に関する留意事項

(1) 供給者は、本調達により知り得た秘密（当機構が公開していない情報等）を第三者に漏らしてはならない。但し、あらかじめ書面により当機構の承認を得た場合は、この限りではない。本調達終了後においても、同様とする。

(2) 供給者は、上記(1)の義務に加えて、当機構の秘密文書取扱規程及び秘密文書の安全管理に関する当機構の規則等、当機構が定める秘密文書の安全確保のための義

務を遵守しなければならない。

9.4. 協議事項に関する留意事項

本仕様書に記載されている事項及び本仕様書に記載のない事項について疑義が生じた場合は、当機構と協議のうえ、その決定に従うものとする。

9.5. グリーン購入法の推進

(1) 本契約において、グリーン購入法（国等による環境物品等の調達の推進等に関する法律）に適用する環境物品（事務用品、OA 機器等）の採用が可能な場合は、これを採用するものとする。

(2) 本仕様に定める提出図書（納入印刷物）については、グリーン購入法の基本方針に定める「紙類」の基準を満たしたものであること。

9.6. 特記事項

(1) 受注者は当機構が原子力の研究・開発を行う機関であるため、高い技術力及び高い信頼性を社会的にもとめられていることを認識し、当機構の規程等を遵守し安全性に配慮し業務を遂行しうる能力を有する者を従事させること。

(2) 受注者は業務を実施することにより取得した当該業務及び作業に関する各データ、技術情報、成果その他のすべての資料及び情報を当機構の施設外に持ち出して発表もしくは公開し、または特定の第三者に対価をうけ、もしくは無償で提供することはできない。ただし、あらかじめ書面により当機構の承認を受けた場合はこの限りではない。

(3) 受注者は異常事態等が発生した場合、当機構の指示に従い行動するものとする。

(4) 本契約の終了時、仮想マシン及びデータを別環境に移行する可能性がある。受注者は、機構からの相談に対し、真摯に対応すること。

(5) 本業務の履行に支障が生じる可能性があると当機構と受注者が認めた場合は、その対策について緊急に協議すること。

II. 技術仕様

1. 仕様

1.1. 受注者サービス環境・設備全般等に関する要件

(1) 本サービスは受注者環境に構築された仮想化基盤及び当機構とその仮想化基盤を接続する回線で構成される。システムの構成概要を以下の図に示す。

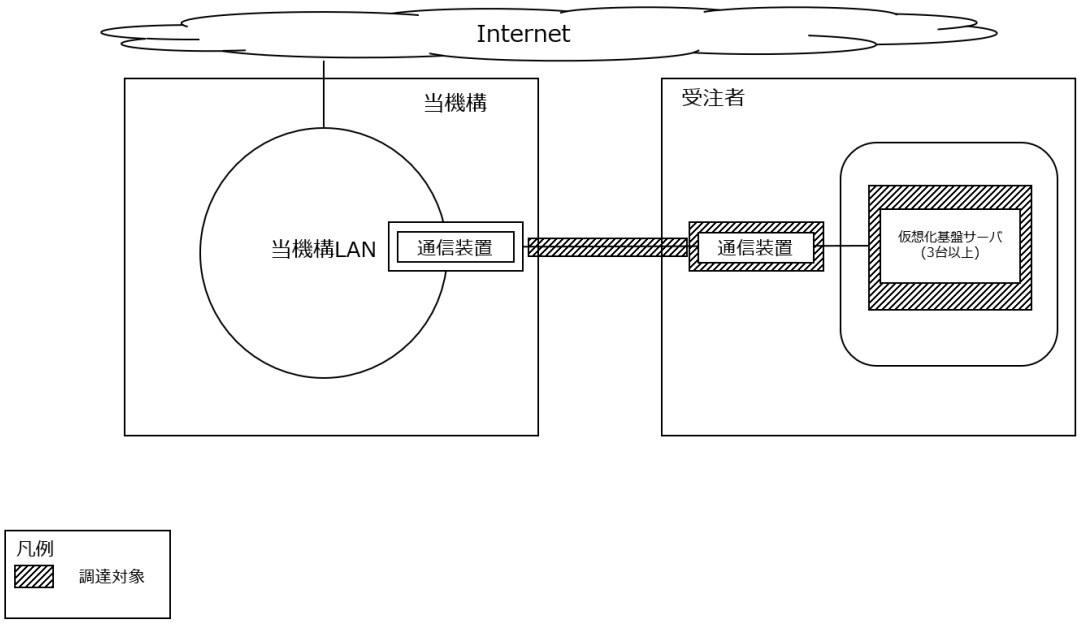

図.構成概要

(2) 受注者サービス環境設備が設置されている建築物（以下、「データセンター」という。）は、耐震・免震・制震いずれかの構造で且つ消火設備を備えていること。

(3) データセンターは、厳重な入退室管理システム等の物理的セキュリティにより防御されていること。

(4) データセンターは、非常用電源設備及び無停電電源装置により、商用電源による給電が停止した場合においても、24 時間以上の動作継続が可能なこと。

(5) 緊急対処が必要な場合を除き、サービス停止等を伴うメンテナンス作業を実施する際は、少なくとも 14 日前までに、日時及び作業の影響範囲を当機構へ通知すること。

(6) 本サービスの廃止、サービス内容の変更等に伴い契約を終了する場合は、十分な期間をもって事前（サービス廃止等の 1 年以上前が望ましい。）に当機構へ通知すること。

(7) 本サービスに関する問い合わせを受ける窓口(電話及び電子メール、平日 9:00 から 17:30)を設けること。
(8) ISMAP（Information system Security Management and Assessment Program）サービスリストに登録しているサービスであること。
(9) 現状の仮想環境上で動作している当機構の仮想サーバ構成※と同等の環境を構築し、現データの移行と動作確認を行い、当機構の確認を得ること。
移行時に当機構側のネットワーク・サーバ等の設定変更が必要な場合は申し出ること。
※仮想サーバ数 : 約 200、現使用ディスク容量 : 約 25TB
(10)「技術仕様」内の「1.7.6(3)」を除く要件に記載の内容が設定されていることを確認する表として検査要領書を受注者にて作成し、当機構の許可を得ること。
(11)検査要領書に記載の設定がなされていることの証跡をまとめた検査成績書を受注者にて作成し、当機構の許可を得ること。

1.2. サービスに係る情報セキュリティに関する要件
(1) 本サービスに対するアクセスログやエラーログの保存（保存期間は 1 年間以上が望ましい。）が実施され、保存した証跡を常時当機構の必要に応じて、提供すること。
(2) 本サービスの監視を 24 時間 365 日体制で行い、サービス停止やセキュリティインシデントが発生した場合は、速やかに当機構へ連絡すること。また、その場合には復旧時点目標（RPO）等の指標を提示すること。
(3) 本サービスで発生したセキュリティインシデントへの対応に関する当機構の調査及び復旧活動に協力すること。
(4) 本サービスで運用する仮想マシンの管理者が、自らの意思により当サービス上で取り扱う情報を確実に抹消できること。
(5) 本サービスの利用終了時は当機構に関する一切の情報を消去し、データ消去が完了したことを示す証明書を提出すること。

1.3. 管轄裁判所及び準拠法に関する要件
(1) 当機構と受注者間で訴訟の必要性が生じた場合は、管轄とする裁判所を日本国内の裁判所とすること。
(2) 本サービスで取り扱う情報について、日本国内法以外の法令が適用され、強制的な情報開示やデータ没収等のカントリーリスクを防止する観点から、日本国内のデータセンターにてサービスを提供すること。

1.4. 仮想化基盤に関する要件

(1) VMware vSphere サーバ上で稼働させている仮想サーバを、フォーマット変換することなく稼働させられる仮想化基盤環境を提供すること。

(2) 仮想化基盤サーバのリソースは以下を満たすこと。

① ハイパーバイザ：3 台以上によるクラスタ構成

ハイパーバイザ 1 台当たりのリソース

ハイパーバイザ：VMware　ESXi 8.0 以降のバージョン

メモリ　　：320GB 以上

CPU　　：2CPU 以上

：24 コア以上(物理コアとして、1CPU 当り 12 コア以上)

：2.2GHz 以上

② 共有ストレージ：40TB 以上

(3) サービス品質保証制度（Service Level Agreement。以下「SLA」という。）により、仮想化基盤の稼働率 99.9%以上を保証していること。

(4) 仮想化基盤サーバのハイパーバイザ OS としては ESXi 8.0 以降のバージョンを選定すること。VMware vCenter Server Appliance は最新バージョンを選定すること。上記バージョンでの導入が困難な場合は当機構と協議の上、バージョンを選定すること。

(5) RedHat Enterprise Linux の無制限ライセンスを月額型サブスクリプションとして提供すること。RedHat Enterprise Linux7 の ELS ライセンスを含めること。

(6) 利用期間内に RedHat Enterprise Linux のメジャーバージョンが新たにリリースされた場合、その OS が仮想化基盤上で利用できるよう設定を実施すること。

メジャーバージョンが利用期間内に 2 つ以上リリースされた場合、少なくとも 1 つ

めのメジャーバージョン OS については仮想化基盤上で利用できるよう設定を実施

すること。

(7) RedHat Enterprise Linux のリポジトリサーバを提供すること。

(8) 仮想化基盤の統合管理機能を提供すること。また、統合管理機能の管理者権限を提供すること。統合管理機能へのアクセスに関しては、アクセス元の IP アドレスを限定及び通信の暗号化を実施するとともに、管理者の認証を行うこと。

(9) 仮想サーバを停止することなく、クラスタを構成する別ノードに移動できること。

(10) 仮想化基盤ネットワークにおいて当機構所有のグローバル IP アドレス空間の複数のサブネットを持ち込み利用できる環境を提供すること。

必要であればルーティングを行う機能・製品を提供し設計・構築し、提供すること。

ルーティングを行う装置は冗長構成であることが望ましい。

(11)サービス提供開始より 3 か月以上、受注者側で本サービスに関するサポート窓口を提供すること。

1.5. 仮想マシンの移行に関する要件

(1) VMware vSphere サーバ上で稼働させている仮想サーバを、フォーマット変換することなく移行できること。

(2) 移行日時は当機構と協議の上で決定し、移行を行う 1 週間前までに当機構に対象の仮想マシンと移行日時を知らせること。

(3) 仮想マシンへのアクセスが可能な状態で移行できる機能を有することが望ましい。

(4) 移行に伴い「3.調達物品及び構成内容」に記載以外のリソースが必要な場合は受注者が用意すること。

＜既存環境＞

IIJ GIO インフラストラクチャーP2

IIJ プライベートバックボーン

IIJ プライベートアクセス

IIJ シンプルバックアップ

IIJ サブスクリプションライセンス

1.6. 当機構と受注者環境間の回線に関する要件

(1) 当機構と受注者環境間において、1.6.1、1.6.2、1.6.3 のいずれかの要件を満たした通信環境を提供すること。それぞれにおいて要件を満たせない事項がある場合には、機構と協議して決定すること。なお、当機構と受注者環境を接続する通信機器の設置場所は別途受注者のみに開示する。

(2) 当機構と受注者環境間において、レイヤ 2 又はレイヤ 3 による接続が可能な通信サービスを提供すること。

(3) 当機構と受注者環境間における通信は全て暗号化すること。

(4) IPsec で利用する受注者環境と SINET 間及び閉域網で利用する通信網の通信速度については、100Mbps 以上とし、帯域保証型であること。また、年間稼働率は 99.9%以上を目標とすること。

(5) 当機構側の既存ネットワークシステムでの設定変更が必要場合はその申し出を行い、設定変更の支援を行うこと。

1.6.1. IPsec を利用した接続に関する要件

当機構と受注者環境間を IPsec で接続する場合、本項に示す要件を満たすこと。

(1) 当機構と受注者環境間を接続する回線の境界において、ファイアウォール機能を持つネットワーク機器を当機構と受注者環境それぞれに 1 台ずつ設置し、機器間の IPsec を設定すること。なお、当機構と受注者環境は SINET を経由した IPsec

を利用し接続すること。

(2) ファイアウォール機能を持つネットワーク機器は以下の要件を満たすこと。

① IPsec のスループットは、200Mbps 以上の性能を有すること。

② 他の機器へ接続するインタフェースとして、100BASE-TX 又は 1000BASE-T のポートを 4 ポート以上提供すること。

③ ファイアウォールスループットは、3Gbps 以上の性能を有すること。

(3) 受注者環境と SINET 間を占有回線で接続すること。

(4) IPsec で利用するネットワークが、受注者が通常業務を行うネットワークと分離されていること。

(5) ファイアウォールは、当機構の既存ポリシーと同等の設定をすること。ファイアウォールの OS は最新バージョンを検討すること。最新バージョンが困難な場合は当機構と協議の上、バージョンを選定すること。

1.6.2. 閉域網を利用した通信に関する要件

当機構と受注者環境間を閉域網で接続する場合、本項に示す要件を満たすこと。

(1) 当機構と受注者環境間を接続する回線の境界において、閉域回線集約用のルータを当機構と受注者環境それぞれに 1 台ずつ設置すること。
当機構側の既存ネットワークシステムで設定変更が必要な場合は申し出ること。

(2) 閉域網で要求するサービスレベルは以下のとおりとする。

① 広域通信サービスが利用不可となる状態が目標として 1 時間以上継続して発生しないこと。
発生した場合は当該停止期間の利用料を返金する処理を速やかに行えること。

② 受注者のバックボーンにおける平均遅延時間が目標として35ミリ秒を超えないこと。

③ 100Mbps以上の帯域で提供すること。

④ 閉域通信を傍受される可能性がある場合は通信の暗号化を行うこと。

1.6.3. SINET のクラウド接続サービスを利用した接続に関する要件

当機構と受注者環境を SINET のクラウド接続サービスを利用して接続する場合、本項に示す要件を満たすこと。

(1) 受注者環境と SINET 間は 100Mbps 以上の専用回線で接続されており、冗長化されていること。
(2) クラウド接続サービスを利用するために、当機構で既存ルータへの追加設定（VLAN等）を実施するが、必要となる情報提供ならびに、本サービス利用のためのSINETへの各種申請手続きを受注者で支援すること。
(3) 仮想化基盤上にファイアウォールを提供し、IPSec を設定して当機構の既存のポリシーと同等の設定をすること。ファイアウォールの OS は最新バージョンを検討すること。最新バージョンが困難な場合は当機構と協議の上、バージョンを選定すること。

1.7. バックアップに関する要件

1.7.1. バックアップの基本要件

(1) 仮想基盤上の全仮想マシンのフルバックアップが行えること。
(2) フルバックアップ、差分バックアップ、増分バックアップに準ずるバックアップ方式を選択し実行する機能を有すること。
(3) 仮想マシンにエージェントをインストールせずにバックアップが行えること。

1.7.2. バックアップの管理と運用要件

(1) 仮想マシンごとにバックアップの頻度、方式を設定できること。
(2) バックアップのスケジュールに基づき自動でバックアップが行えること。
(3) バックアップが成功･失敗したことを通知する機能を有すること。

1.7.3. 復旧要件

(1) 最低でも 30 日前のリカバリポイントに戻す機能を有すること。
(2) 6 時間以内にバックアップを利用した復旧が可能であること。
(3) バックアップから仮想マシンを復旧する手順を提供すること。また、復旧に関する問い合わせを受け付け、復旧を支援すること。

1.7.4. セキュリティと通信要件

(1) バックアップデータを暗号化し保管すること。
(2) バックアップデータは当機構と受注業者からのみアクセスが可能な状態であること。
(3) バックアップを行う回線は Web サービスを公開する経路とは別に用意すること。バックアップから復旧する際も Web サービスを外部に公開する経路と別の経路で行えること。
(4) バックアップ用回線は 100Mbps 以上の帯域を確保できること。

1.7.5. インフラ運用要件

(1) バックアップを管理するサーバが必要な場合はそのサーバの設計･構築も行うこと。この場合においてOSは本契約内でサポートされるRHELで検討すること。管理サーバに別OSを用いる必要がある場合は当機構側と協議し方針を決定すること。

(2) サービス利用期間中、バックアップの対象と方式を当機構側で変更できること。

(3) バックアップデータを重複排除等で圧縮する機能を有すること。

1.7.6. その他

(1) バックアップ容量として40TB以上利用できる環境を提供し、月内のバックアップ容量の利用実績をもとに精算し請求すること。
※バックアップ元の実容量は25TBほどを想定している。

(2) バックアップについて1.7.1～1.7.6要件を満たせない場合や選択肢が複数ある場合は当機構側と協議の上、方針を決定すること。

(3) サービス利用初月(2026/4/1～2026/4/30)の期間にバックアップの実容量を計測し、利用期間内の従量課金額の試算を表す「従量課金分試算表」を作成し提出すること。

以上

情報セキュリティ強化に係る特約条項

受注者（以下「乙」という。）は、本契約の履行に当たり、情報セキュリティの強化のため、契約条項記載の情報セキュリティに係る遵守事項に加え、以下に特約する内容を遵守するものとする。

（情報セキュリティインシデント発生時の対処方法及び報告手順）

第１条 乙は、情報セキュリティインシデントが発生した際の対処方法（受注業務を一時中断することを含む。）及び発注者（以下「甲」という。）に報告する手順について整備しておかなければならない。

（情報セキュリティ強化のための遵守事項）

第２条 乙は、次の各号に掲げる事項を遵守するほか、甲の情報セキュリティ強化のために、甲が必要な指示を行ったときは、その指示に従わなければならない。

(1) この契約の業務を実施する場所を、情報セキュリティを確保できる場所に限定し、それ以外の場所で作業をさせないこと。

(2) 業務担当者に遵守すべき情報セキュリティ対策について教育・訓練等を受講させるとともに、業務担当者には甲の情報セキュリティ確保に不断に取り組み、甲の情報及び情報システムの保護に危険を及ぼす行為をしないよう誓約させること。また、業務担当者の異動・退職等の際には異動・退職後も守秘義務を負うことを誓約させ、これを遵守させること。

(3) 暗号化を要する場合は、「電子政府推奨暗号リスト」に記載された暗号化方式を実装し、暗号鍵を適切に管理すること。

(4) 甲の承諾のない限り、この契約に関して知り得た情報を受注した業務の遂行以外の目的で利用しないこと。

(5) 甲が提供する情報を取り扱う情報システムへの不正アクセスを検知・抑止するために、ログを取得・監視し全ての業務担当者についてシステム操作履歴を取得すること。

(6) 甲が提供する情報を格納する装置、機器、記録媒体及び紙媒体について、業務担当者のみがアクセスできるよう施錠管理や入退室管理を行い、セキュアな記録媒体の使用や使用を想定しないUSBポートの無効化、機器等の廃棄時・再利用時のデータ抹消など想定外の情報利用を防止すること。

(7) 情報システムの変更に係る検知機能やログ解析機能を実装し、外部ネットワークへの接続を伴う非ローカルの運用管理セッションの確立時には、多要素主体認証を要求するとともに定期的及び重大な脆弱性の公表時に脆弱性スキャンを実施し、適時の脆弱性対策を行うこと。

(8) システムの欠陥の是正及び脆弱性対策について、対策計画を策定し実施するとともに、システムの欠陥の是正及び脆弱性対策等の情報セキュリティ対策が有効に機能していることの継続的な監視と確認を行うこと。

(9) 委任をし、又は下請負をさせた場合は、当該委任又は下請負を受けた者に対して、業務担当者が遵守すべき情報セキュリティ対策についての教育・訓練等を行うこと。

(10) 契約条項に基づき甲が乙に対して行う情報セキュリティ対策の実施状況についての監査の結果、情報セキュリティ対策の履行が不十分である場合には、甲と協議の上改善を行い、甲の承諾を得ること。

(11) 契約の履行期間を通じて前各号に示す情報セキュリティ対策が適切に実施されたことの報告を含む検収を受けること。また、本契約の履行に関し、甲から提供を受けた情報を含め、本契約において取り扱った情報の返却、廃棄又は抹消を行うこと。