第４号議案

２０２６年１月２８日
第５５０回理事会

OA システムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託の実施について（案）

１．本委託の概要

2024 年 11 月 6 日第 484 回理事会第 1 号議案の承認を得て、2026 年度に向けて進めている OA システムリプレースの一環の最終段階として、ネットワークならびに認証機能等の設計・構築及び運用保守の業務委託について入札を実施する。

２．調達方法

一般競争入札（総合評価落札方式）とし、技術点、価格点の内訳は以下のとおり
「総合評価点（200 点）＝技術点（100 点）＋価格点（100 点）」

３．入札スケジュール（予定）

2026 年　1 月 28 日（水）	公告（本理事会後速やかに実施）
2026 年　2 月　6 日（金）	入札説明会
2026 年　2 月　9 日（月）	問合せ締切
2026 年　2 月 16 日（月）	問合せに対する回答
2026 年　3 月　2 日（月）	入札締切
2026 年　3 月　5 日（木）	技術審査、開札
2026 年　3 月 18 日（水）	落札者決定（理事会）
2026 年　3 月 19 日（木）	落札通知

４．落札者の決定および契約の締結

開札については、総務部長が実施することとし、落札者の決定および契約の締結については、別途理事会で議決する。

５．入札説明書（仕様書含む）

入札説明書は、別紙入札資料一式のとおり。なお、公告時にウェブサイト上で開示する。

以　上

【添付資料】
別紙_入札資料一式
（内訳：入札説明書、入札仕様書、OAシステムサービス要求仕様書、非機能要求グレード、応札資料作成要領、適合証明書、質問票、評価項目一覧、評価手順書）

別紙

OA システムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託

入札説明書

電力広域的運営推進機関

２０２６年１月

入札説明書

電力広域的運営推進機関

電力広域的運営推進機関（以下、「本機関」という。）の「OA システムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託」に係る入札公告（2026 年 1 月 28 日付け公示）に基づく入札については、下記に定めるところによる。

記

1. 競争入札を実施する事項

（１） 件名　　OA システムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託

（２） 委託内容　　別紙仕様書のとおり

（３） 調達方式　　一般競争入札（総合評価落札方式）

（４） 履行期限　　別紙仕様書のとおり

（５） 納入場所　　別紙仕様書のとおり

（６） 入札金額　　入札金額は、「OA システムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託」に関する総価で行う。
なお、本件については入札の際に提案書を提出し、技術審査を受けなければならない。
落札決定に当たっては、入札書に記載された金額に当該金額１０パーセントに相当する額を加算した金額（当該金額に１円未満の端数が生じたときは、その端数金額を切捨てるものとする。）をもって落札価格とするので、入札者は消費税及び地方消費税に係る課税事業者であるか免税事業者であるかを問わず、見積もった契約金額の１１０分の１００に相当する金額を入札書に記載すること。

2. 競争参加資格

（１） 令和０７・０８・０９年度の競争参加資格（全省庁統一資格）、「物品の販売」及び「役務の提供等」において、「A」以上の等級に格付けされていること。

（２） 各省各庁から指名停止又は一般競争入札資格停止若しくは営業停止をうけていない者であること。

（３） 入札説明会に参加した者であること。

（４） 予算決算及び会計令（昭和２２年勅礼第１６５号）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。

（５） 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。

（６） 会社更生法（平成１４年法律第１５４号）に基づく更生手続開始の申立て又は民事再生法（平成１１年法律第２２５号）に基づく再生手続開始の申立てがなされている者ではないこと。（但し、会社更生法に基づく更生手続開始の申立て又は民事再生法に基づく再生手続開始　の申立てがなされている者で、手続開始の決定後、競争参加資格の再認定を受けている者を除く。）

（７） 自己、自社若しくはその役員等（注１）が、暴力団員による不当な行為の防止等に関する法律第２条に定める暴力団、暴力団員又はその他反社会勢力（注２）でない者であること。

（注１）取締役、監査役、執行役、支店長、理事等、その他経営に実質的に関与している者。

（注２）暴力団準構成員、総会屋等、社会運動等標ぼうゴロ又は特殊知能暴力集団、暴力団又は暴力団員と社会的に非難されるべき関係を有する者、暴力団員でなくなった時から５年を経過しな

い者等、その他これに準じる者。

（８） 破壊活動防止法（昭和 27 年法律第 240 号）に定めるところの破壊的団体およびその構成員でない者であること。

3. 入札説明会の実施

下記日時で入札説明会（Web 開催）を実施する。入札を希望する者は、必ず参加すること。
（不参加の場合は入札できないものとする）

日　時　：2026 年 2 月 6 日（金）15 時 00 分～（３０分程度）
参加資格　：「２．競争参加資格」を満たす者
そ の 他　：参加を希望する事業者は 2026 年 2 月 4 日（水）１２時までに「電力広域的運営推進機関契約担当」まで事業者名及び連絡先を記載のうえ、メールにて申入れること。なお、入札説明会までに通信状態の事前確認を実施する（別途連絡）。

4. 入札者の義務

この一般競争入札に参加を希望する者は、本機関が交付する仕様書に基づいて提案書を作成し、これを入札書に添付して入札書の提出期限内に提出しなければならない。

また、落札者決定までの間において本機関の職員から当該書類に関して説明を求められた場合は、これに応じなければならない。なお、入札者の作成した提案書は本機関において審査するものとし、採用し得ると判断した提案書を添付した入札書のみを落札決定の対象とする。

5. 入札書・提案書・入札資格確認書類の提出期限、提出書類及び提出先

提出期限：2026 年 3 月 2 日（月）15 時必着で必要書類を郵送または持参すること。
提出書類：①入札書（別途封入すること）
②評価項目一覧（提案書頁番号欄に必要事項を記入したもの）
③提案書（別途電子媒体でも提出すること）
④契約書（案）
⑤適合証明書
⑥全省庁統一資格審査結果通知書（写）
提出先：〒135-0061　東京都江東区豊洲６－２－１５
電力広域的運営推進機関総務部会計室
OA システムリプレースに係るネットワークならびに認証機能等の設計・構築
及び運用保守の業務委託　入札係

6. 競争参加者は、提出した入札書の変更及び取り消しをすることができない。

7. 技術審査のプレゼンテーションの日時

2026 年 3 月 5 日（木）
時間については、本機関より入札者に別途連絡の上調整

8. 入札の無効

次の各号の一に該当する入札は、無効とする。
①「２．競争参加資格」に示した競争参加資格のない者による入札

② 記名押印（外国人又は外国法人にあっては、本人又は代表者の署名をもってかえることができる。）を欠く入札
③ 金額を訂正した入札
④ 誤字、脱字等により意思表示が不明瞭である入札
⑤ 明らかに連合によると認められる入札
⑥ 提案書が本機関の審査の結果採用されなかった入札
⑦ 入札書提出期限までに到着しない入札
⑧ 虚偽の提案を入札
⑨ その他入札に関する条件に違反した入札

9. 落札者の決定方法

本機関が設定する予定価格の制限の範囲内で、本機関が入札説明書で指定する要求事項のうち、必須とした項目の最低限の要求をすべて満たしている提案をした入札者の中から、本機関が定める総合評価の方法をもって落札者を定めるものとする。ただし、落札者となるべき者の入札価格によっては、その者より当該契約の内容に適合した履行がなされないおそれがあると認められるとき、又はその者と契約することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、予定価格の範囲内の価格をもって入札をした他の者のうち、評価の最も高い者を落札者とすることがある。

なお、開札をした場合において、各人の入札のうち予定価格の制限に達した価格の入札がない場合は、各人の連絡の上、後日、再度入札を行う。

また、落札となるべき同総合評価点の入札をした者が２者以上あるときは、各人に連絡の上、当該入札をしたものにくじを引かせて落札者を決定する。

10. 落札結果の通知

2026 年 3 月 19 日（木）までに、入札者に対して落札結果を通知する。

11. 入札保証金及び契約保証金

免除

12. 契約書作成の要否

要

13. 支払条件

本委託にかかる支払は、契約書記載の条件により、支払請求書の受領日の翌月末までに支払うものとする。

14. 見積条件

- 支出計画書を作成すること。
- 見積総額及び内訳について可能な限り詳細に明記すること。見積金額には、本契約の履行に関して必要な一切の費用を含めること。

15. 契約書の記載内容

契約書は仕様書に定める環境構築および保守、サービスの内容全てを包含するものとする。なお、環境構築および保守、サービスについては、それぞれ個別の契約書を締結するものとする。

また、保守、サービスについては、年度更新（自動更新を含む）とする。

16. 入札書等に使用する言語及び通貨

入札書、提案書、技術審査のプレゼンテーションに使用する言語は日本語とし、通貨は日本国通貨に限る。

17. 落札決定の取消し

落札決定後であっても、この入札に関して連合その他の事由により正当な入札でないことが判明した時は、本機関は落札決定を取り消すことができる。

18. その他

（１） 競争参加者は、提出した証明書等について説明を求められた場合は、自己の責任において速やかに書面をもって説明しなければならない。

（２） 本入札結果については、落札者との契約締結後、原則として、契約件名、契約相手方、契約締結日及び契約金額等の契約概要を公表する。

（３） 本業務の実施にあたり参考となるシステムの設計書等に関する資料については、入札説明会に参加したうえで、下記問い合わせ先へ機密保持に関する誓約書を提出した場合に限り、閲覧を可能とする。

（４） この入札に関して明な点は、2026 年 2 月 9 日（月） １７時までに下記問い合わせ先へ、電子メールで問い合わせることができる。問い合わせへの回答は、2026 年 2 月 16 日（月）までに本機関ウェブサイトの本入札公告上に開示する。

（５） 本仕様書に記載のない事項及び疑義については、本機関と協議のうえ決定することとする

【 問い合わせ先 】

本件に関するお問い合わせ先

- 電力広域的運営推進機関総務部会計室（契約担当）
- メールアドレス：keiyaku@occto.or.jp

以上

（様　式）

年　　月　　日

電力広域的運営推進機関　御中

住　　所

商号又は名称

代表者 氏 名　　印

入　札　書

入札金額　　¥＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

※消費税及び地方消費税を含まない金額

内訳　　別添支出計画書のとおり。

入札事項　　OA システムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託

貴機関「入札説明書」の内容を承知の上入札いたします。

（別 添）

支出計画書

【参考例】

区分	内訳	金額（円）	積算内訳
１．設計構築業務に係る費用	・物品費用 ・設計構築費用 ・機器設置及び配線工事費用 等	000,000,000	・物品費用・・・z,zzz,zzz ・設計構築費用・・・z,zzz,zzz ・機器設置及び配線工事費用・・・z,zzz,zzz 等
２．運用保守業務に係る費用 【年額】	・運用保守費用 ・クラウドサービス利用料 ・回線利用料　等	000,000,000	・運用支援費用・・・z,zzz,zzz ・HW,SW の保守費用・・・z,zzz,zzz ・クラウドサービス利用料・・・z,zzz,zzz ・回線利用料・・・z,zzz,zzz 等
3．運用保守業務に係る費用計【5 年分】		000,000,000	２．運用保守業務に係る費用【年額】×5 年分 （※年度毎に金額の差がある場合には、年度毎の費用が分かるように記載）
4．小計		000,000,000	１．設計構築業務に係る費用＋ 3．運運用保守業務に係る費用計【5 年分】(注１：入札金額と一致)
5．消費税及び地方消費税		000,000,000	
6．合計		000,000,000	１．設計構築業務に係る費用＋ 3．運運用保守業務に係る費用計【5 年分】＋ 5．消費税及び地方消費税

（別　添）

機密保持に関する誓約書

電力広域的運営推進機関
理事長　　大山　力　殿

2026 年　　月　　日

会社名
住所
氏名　　印

当社は、「OA システムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託」の入札（以下、「本入札」という。）に関して、以下の各事項を遵守することを誓約します。

1. 本誓約における機密情報とは、電力広域的運営推進機関（以下、「広域機関」という。）が開示する次の情報とする。
   開示予定資料
   「OA システム　基本設計書一式」
   「OA システム　構成図一式」
   「OA システム　詳細設計書一式」
   「OA システム　運用実施要領一式」
2. 当社は、広域機関から開示された機密情報を本入札の提案の目的にのみ使用するものとし、 その他の目的には使用しないものとする。
3. 当社は、広域機関から開示された機密情報を本入札の提案のために知る必要のある自己の役員、従業員以外に開示、閲覧等させないものとする。
4. 当社は、広域機関から開示された機密情報を第三者に開示または漏えいしないものとする。
5. 当社は、本入札の提案に当たって第三者に機密情報を開示、閲覧等させる場合には、広域機関の事前承諾を得た上で、当該第三者に開示するものとする。
6. 当社は、前項により、機密情報を開示する第三者に対し、本誓約と同様の機密保持誓約をさせるものとする。
7. 当社は、本入札の提案に当たって機密情報を知る必要のある自己の役員、従業員に本誓約の内容を遵守させるものとする。
8. 当社又は５.で定める第三者が、本誓約のいずれかの事項に違反した場合、又は漏えい等の事故により広域機関に損害を与えた場合には、当社は、広域機関が被った損害の賠償をするものとする。

以上

OA システムリプレースに係るネットワーク
ならびに認証機能等の設計・構築及び
運用保守の業務委託
入札仕様書

電力広域的運営推進機関

２０２６年１月

目次

仕様書

1. 調達案件の概要に関する事項

(1) 調達件名

OA システムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託

(2) 調達の背景

電力広域的運営推進機関（以下「本機関」という。）において、OA システムは 2015 年 4 月に運用を開始し、その後リプレースを経て現在に至っている。現行システムは 2026 年 9 月で稼働開始後 5 年が経過し、メーカーが定める標準保守期間が満了する。このため、2026 年 10 月から 2027 年 3 月までの期間については保守延長により対応しているが、当該延長保守は暫定的な措置であり、2027 年 4 月以降の保守契約の継続は困難である。

以上の理由から、安定稼働を継続的に確保するため、OA システムのリプレースを実施する。

(3) 目的及び期待する効果

本調達は、24 時間 365 日の稼働することを前提に、以下の効果を実現する。

- ＰＣを活用した事務処理の安定した利用
- インターネット、メール、SaaS 型クラウドサービス等の安定した利用
- 有線、WiFi 環境（無線）を利用しての安定した利用
- 業務システムに必要な環境の維持（広域機関システム、スイッチング支援システムの共通機能の維持）
- ハードウェア、ソフトウェア、ネットワーク機器等の一元管理

※ＯＡシステムとは、業務に依存しない共通的な機能を対象とする。分類として「ネットワーク」、「共通基盤」、「セキュリティ」に必要な機能から成る。

(4) 契約期間・作業スケジュール

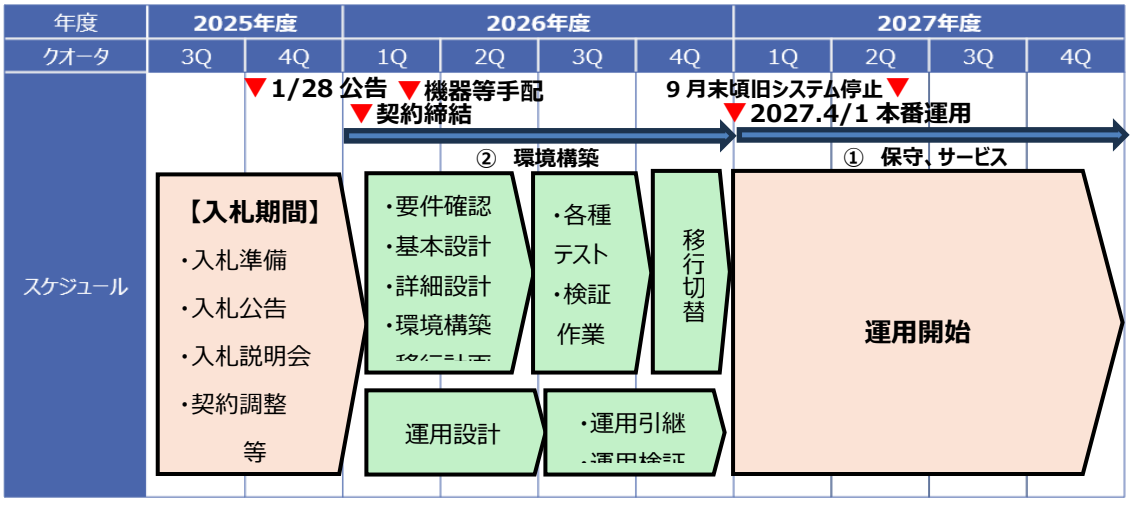
本業務委託に関しては、下記のスケジュールにて行うものとする。

① 環境構築については、契約締結日から 2027 年 3 月末まで

② 保守、サービスについては、2027 年 4 月から 2032 年 3 月末まで（5 年間運用）

※ 機器設置から 2027 年 3 月末までの保守について、①環境構築費用に含めることとする。

※ 環境構築等のスケジュール短縮および段階的にリリースできる場合は、必ず提案書に取り入れること。



2. 作業の実施内容に関する事項

(1) 作業の内容

作業の実施内容は以下を想定している。

なお、詳細は別紙 1_「OA システムサービス要求仕様書」を参照のこと。

Ａ．環境構築

① プロジェクト計画／管理

本作業の実施にあたり、目的、実施体制、役割、作業内容と作業方法、作業スケジュール、リスク管理、情報セキュリティ管理、課題管理、品質管理、人的資源管理、コミュニケーション管理、構成・変更管理等を明確にしたプロジェクト計画書を作成すること。

② 要件確認

本機関における要件（別紙 1_「OA システムサービス要求仕様書」と現行システムの設計書等）については、受託者との認識のずれや齟齬がないことを確認すること。

③ 設計

確認した要件に基づき、基本設計、詳細設計、運用設計、試験設計、移行設計を行うこと。

④ 構築

設計に基づき、システムをセットアップすること。

⑤ 設置・工事

サーバ、無線アクセスポイント、LAN 敷設、インターネット回線等の設置・工事を行うこと。

⑥ 移行・切替

移行設計に基づき、既存環境から新環境へのデータ移行およびシステム切替を実施すること。切替にあたっては、業務への影響を最小限に抑えるため、事前に切替手順および切替計画を策定すること。

⑦ 運用引継

新環境の運用に支障が生じないよう、運用手順書等の作成を行うとともに、本機関担当者への説明、教育および運用引継を実施すること。

⑧ 試験およびチューニング

試験設計に基づき、システムの試験を実施すること。また、広域機関システム、スイッチング支援システムの共通機能については、必ずシナリオ試験（実際の業務手順を想定した一連の処理を通じて、複数機能および関連システム間の連携が正しく行われることを確認）を実施すること。試験結果を踏まえ、性能・安定性・信頼性の向上を目的として、必要なチューニングを実施すること。

Ｂ．保守

① プロジェクト計画／管理

本作業の実施にあたり、リスク管理、情報セキュリティ管理、課題管理、品質管理、人的資源管理、コミュニケーション管理、構成・変更管理等を明確にしたプロジェクト計画書を作成すること。

② 保守

運用細則及び運用設計書に基づき、導入した機器およびシステムの稼働監視、バックアップ管理、定期メンテナンス等を行い、システムの安定稼働を確保すること。

Ｃ．サービス

① プロジェクト計画／管理

本作業の実施にあたり、リスク管理、情報セキュリティ管理、課題管理、品質管理、人的資源管理、コミュニケーション管理、構成・変更管理等を明確にしたプロジェクト計画書を作成すること。

② サービス

運用細則及び運用設計書に基づき、インシデントの監視、検知、通知および問い合わせ対応等を行い、利用者や業務の円滑な運用を支援すること。

(2) 成果物の範囲、納品期日等

A．環境構築

本調達における想定している調達機器（設備）については、受託者は作業の詳細スケジュールと併せて、納品予定日をプロジェクト計画書等に記載すること。

なお、設置場所については、メインサイト及びバックアップサイトの本機関が指定する場所とする。

B．保守

本調達における想定している保守期間は、機器導入時から 2032 年 3 月末までである。

また、追加の保守などがあれば支出計画書に記載すること。

C．サービス

本調達におけるサービスは、2027 年 4 月から 2032 年 3 月末まで（5 年間運用）である。

D．本調達に係る付帯業務

① 成果物・提出物

付帯業務において想定している成果物は以下のとおりとする。受託者は、各成果物について作業の詳細スケジュールと併せて納品予定日をプロジェクト計画書等に記載すること。

また、業務遂行上、追加で必要となる成果物がある場合は、その内容および納品予定日をプロジェクト計画書等に記載すること。

作業の内容	作業の内容	成果物
A．環境構築	プロジェクト計画／管理	プロジェクト計画書
		進捗管理表
		課題管理表
		リスク管理表
		会議議事録
	設計	基本設計書
		詳細設計書
		運用設計書
		試験設計書
		移行設計書
	試験	試験結果報告書
	移行・切替	移行・切替結果報告書
	チューニング	チューニング結果報告書
B．保守	プロジェクト計画／管理	プロジェクト計画書
	保守	作業計画書
		月次報告書、年次報告書
C．サービス	プロジェクト計画／管理	プロジェクト計画書
	サービス	運用マニュアル
		インシデント報告書
		月次報告書、年次報告書

② 納品方法

項番	分類	要件
1	言語	・成果物は、全て日本語で作成すること。ただし、日本国においても、英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。
2	準拠すべき規格	・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）」に準拠すること。 ・情報処理に関する用語の表記については、原則、日本工業規格（ＪＩＳ）の規定に準拠すること。
3	納品形態	・成果物は電磁的記録媒体（ＣＤ-Ｒ等）により作成し、本機関から特別に示す場合を除き、原則電磁的記録媒体は 1 部を納品すること。なお、保守及びサービスの成果物については、メールでの納品も可能とする。 ・紙媒体による納品について、用紙のサイズは、原則として日本産業規格 A 列 4 番とするが、必要に応じて日本産業規格 A 列 3 番を使用すること。また、バージョンアップ時等に差し替えが可能なようにバインダ方式とすること。 ・電磁的記録媒体による納品について、Microsoft Word、Excel 又は同 PowerPoint で読み込み可能な形式、及びＰＤＦ 形式で作成し、納品すること。なお。これらは原則として文字列検索機能を活用して文字列が検索可能な状態のものを納品すること。ただし、本機関が他の形式による提出を求める場合は、協議の上、これに応じること。なお、受託者側で他の形式を用いて提出したいファイルがある場合は、協議に応じるものとする。
4	セキュリティ対策	・成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。 ・電磁的記録媒体に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等して、成果物に不正プログラムが混入することのないよう、適切に対処すること。
5	留意事項	• 納品後、本機関において改変が可能となるよう、図表等の元データも併せて納品すること。 • 成果物の作成にあたって、特別なツールを使用する場合は、本機関の承認を得ること。

③ 納品場所

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

〒135-0061
東京都江東区豊洲 6-2-15
電力広域的運営推進機関　総務部 情報システム室

3. 満たすべき要件に関する事項

本調達の実施に当たっては、別紙 1_「OA システムサービス要求仕様書」の各要件を満たすこと。

4. 作業の実施体制・方法に関する事項

(1) 作業実施体制

本プロジェクト実施に当たり、体制図及びその従事する人数について記載すること

(2) 作業場所

別紙 1_「OA システムサービス要求仕様書」に従うものとする。

(3) 作業の管理に関する要領

別紙 1_「OA システムサービス要求仕様書」に従うものとする。

5. 作業の実施に関する事項

(1) 機密保持、資料の取扱い

本機関から受託者に提供する秘密情報及び秘密情報を記録した資料等は、本契約期間中の如何を問わず、第三者に開示、漏えい又は他の目的に使用しないこと。ただし第三者に開示の必要性がある場合は、開示方針や漏えいの防止策を明示し本機関の承認を得ること。

(2) 遵守する法令等

① 本仕様書に示す業務の実施に当たっては、次の文書に記載された事項を遵守すること。

(ア) 政府情報システムの整備及び管理に関する標準ガイドライン

(イ) 政府機関の情報セキュリティ対策のための統一基準

(ウ) 本機関の情報管理セキュリティ関連規程

② 受託者は、現行情報システムの設計書等を参照する必要がある場合は、作業方法等について本機関の指示に従い、秘密保持契約を締結する等した上で、作業すること。

③ 受託者は、受託業務の実施において、民法、刑法、著作権法、不正アクセス行為の禁止等に関する法律、個人情報の保護に関する法律等の関連する法令等を遵守すること。

6. 成果物の取扱いに関する事項

(1) 検収

① 本仕様書に則って成果物を提出すること。

② 検査の結果、成果物の全部又は一部に不合格品を生じた場合には、受託者は直ちに引き取り、必要な修復を行った後、指定した日時までに修正が反映された全ての成果物を納入すること。

③ 本仕様書以外にも、必要に応じて成果物の提出を求める場合があるので、作成資料は常に管理し、最新状態に保っておくこと。

7. 再委託に関する事項

(1) 再委託の制限及び再委託を認める場合の条件

① 受託者は本仕様書に示す業務の全部又は総合的な企画及び判断並びに業務遂行管理部分を第三者に再

委託することは不可とする。また、本業務の契約金額に占める再委託契約金額は、原則２分の１未満とする。

② 受託者は、知的財産権、情報セキュリティ（機密保持及び遵守事項）、ガバナンス等に関して本仕様書が定める受託者の債務を、再委託先事業者も負うような必要な処置を実施すること。

③ 再委託者、再委託者が業務を委託する第三者（以下「再々委託者」という。）及び再々委託者が業務を第三者へ委託する場合の責任は受託者が負うこと。

④ 以下に示すものについても本仕様書「6 作業の実施に当たっての遵守事項」に示した事項を遵守させること。

(ア) 再委託者

(イ) 再々委託者

(ウ) 再々委託者が業務を委託する第三者

(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、契約予定金額について本機関に提出し、承認を受けること。

② 再委託の相手方からさらに第三者に委託が行われる場合には、当該第三者の商号又は名称及び住所並びに委託を行う業務の範囲について本機関に提出すること。

8. その他特記事項

(1) 前提条件及び制約条件

- 本仕様書は、受託者に業務遂行を求める最低限の基準を示したものである。したがって、本仕様書に記載していない事項であっても、本調達に必要と認められる事項は、本機関と追加負担を含め協議の上、これを行うこと。
- 本件受託後に本仕様書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、本機関に申し入れを行うこと。
- 本機関の要件と受託者の提案内容に齟齬がある場合には、本機関の要件を優先し、当該要件に従い対応すること。
- 受託者は、業務の遂行に当たり、本機関の作業負荷等を十分考慮すること。
- 受託者のプロジェクトマネージャーは、業務の円滑な運営を図るため、本機関との連絡を密にして業務を遂行すること。
- 本機関から貸し出された資料又は支給を受けた物品等については、善良なる管理者の注意をもって保管及び管理するものとし、紛失又は破損の場合直ちに本機関に報告し、本機関の指示に従って措置を講ずること。
- 受託者は、常に作業場所を整理・整頓し、安全に留意して事故の防止に努めるとともに、労働基準法、労働安全衛生法等を遵守して安全の徹底を図り、作業を行うこと。
- 受託者が行う提案や報告及び相談等は全て書面を持って実施し、内容については、本機関の承認を得ること。
- 本仕様書に記載したスケジュールは現時点での想定である。スケジュール変更があった場合の対応については、本機関と協議の上、決定すること。
- 本業務委託に係り作成、変更及び更新されるドキュメント類の著作権は本機関に帰属するものとする。
- 本機関に帰属する著作権のうち、著作者人格権について、受託者はこれを行使しないこととする。
- 本仕様書に記載のない事項及び疑義については、広域機関と協議のうえ決定することとする。

9. 関連資料

別紙 1_「OA システムサービス要求仕様書」

別紙 2_「非機能要求グレード」

以上

OA システムリプレースに係るネットワーク
ならびに認証機能等の設計・構築及び
運用保守の業務委託
応札資料作成要領

電力広域的運営推進機関

２０２６年１月

目次

本書は、「OA システムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託」に係る応札資料(評価項目一覧及び提案書)の作成要領を取りまとめたものである。

第 1 章　電力広域的運営推進機関が応札者に提示する資料及び応札者が提出すべき資料

電力広域的運営推進機関は応札者に以下の表 1 に示す資料を提示する。応札者は、それを受け、以下の表 2 に示す資料を作成し、電力広域的運営推進機関へ提出する。

[表 1 電力広域的運営推進機関が応札者に提示する資料]

資料名称	資料内容
① 仕様書	OAシステムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託の仕様を記述
② 応札資料作成要領	応札者が評価項目一覧及び提案書の作成する上での留意点等を記述
③ 評価項目一覧	提案書に記載すべき必須項目及び任意項目の区分、得点配分等を記述
④ 評価手順書	電力広域的運営推進機関が応札者の提案を評価する場合に用いる評価方式、総合評価点の算出方法及び評価基準等を記述

[表 2 応札者が電力広域的運営推進機関に提示する資料]

資料名称	資料内容
① 入札書	別添支出計画書とともに、入札金額を記載したもの。別途封入すること。
② 評価項目一覧の提案書頁番号欄に必要事項を記載したもの	仕様書に記述された要件一覧を達成するか否かに関し、提案書頁番号欄に、該当する提案書の頁番号を記入したもの。
③ 全省庁統一資格　資格審査結果通知書（写）	令和０７・０８・０９年度の競争参加資格（全省庁統一資格）の「役務の提供等」において、等級「A」以上に格付けされていること。
④ 提案書	仕様書に記述された要求仕様をどのように実現するかを説明したもの。
⑤ 契約書（案）	本業務を受託した際の契約書（案）
⑥ 適合証明書	入札資格を満たしていることを証する書面。

第 2 章　評価項目一覧に係る内容の作成要領

2.1　評価項目一覧の構成

評価項目一覧の構成及び概要説明を以下に記す。

[表 3　評価項目一覧の構成の説明]

評価項目一覧における	事項	概要説明
1 ～5	提案要求事項	提案を要求する事項。これら事項については、応札者が提出した提案書について、各提案要求項目の必須項目および任意項目の区分け、得点配分の定義に従いその内容を評価する。

2.2 提案要求事項

評価項目一覧中の提案要求事項における各項目の説明を以下に示す。応札者は、別紙 5_「評価項目一覧」の案要求事項における「提案書頁番号」欄に必要事項を記載すること。提案要求事項の各項目の説明に関しては、表４を参照すること。

[表 4 提案要求事項上の各項目の説明]

項目名	項目説明・記入要領	記入者
大項目～細項目	提案書の目次（提案要求事項の分類）。	広域機関
提案要求事項	応札者に提案を要求する内容	広域機関
仕様書の該当項目	評価項目に対する本機関からの要求事項を記載した仕様書の該当箇所	広域機関
評価区分	必ず提案すべき項目（必須）又は必ずしも提案する必要は無い項目（任意）の区分を設定している。各項目について、記述があった場合、その内容に応じて配点を行う。	広域機関
得点配分	各項目に対する最大加点	広域機関
評価基準	必須となる事項に対する評価基準、及び加点する際の評価基準を示している。	広域機関
提案書頁番号	作成した提案書における該当頁番号を記載する。	応札者

第 3 章　提案書に係る内容の作成要領及び説明

3.1　提案書の構成及び記載事項

以下に、別紙 5_「評価項目一覧」から[提案書の目次]の大項目を抜粋したものおよび求められる提案要求事項の概要を示す（表 5）。

提案書は、表 5 の項番、項目内容に従い、提案要求内容を十分に咀嚼した上で記述すること。なお、目次および要求事項の詳細は、別紙 5_「評価項目一覧」を参照すること。

[表 5 提案書目次]

提案書	大項目	提案要求事項の概要説明
1	業務委託の背景・目的	本業務に至った背景および目的を十分に理解した上で、現行システムの課題や将来像を踏まえ、業務効率化・安定運用・セキュリティ向上を実現するための適切な対応方針および提案内容。
2	プロジェクト計画・構成	本業務を円滑かつ確実に遂行するため、体制、役割分担、スケジュール、進捗・品質・課題管理方法等を明確にし、実現性および妥当性の高いプロジェクト計画等。
3	機能要件の理解と実現	提示された機能要件を正確に理解した上で、要件を満たす具体的な実現方法、構成、設定方針等を示し、現行機能の継続性および利便性向上が図られる等。
4	非機能要件の理解と実現	性能、可用性、信頼性、セキュリティ、拡張性等の非機能要件について十分に理解し、要件を満たすための設計方針、対策および根拠等。
5	運用・保守要件の実現	運用・保守要件を踏まえ、稼働監視、障害対応、バックアップ、問い合わせ対応等について、安定的かつ継続的なサービス提供が可能となる具体的な運用・保守体制および方法等。

3.2 提案書および契約書（案）様式

① 提案書の様式は自由とする。なお、最低限、別紙 5_「評価項目一覧」に記載の項目（詳細は評価項目一覧を参照）を提案書に含めなければならない。

② 提出物は、電子媒体により提出するものとする。提出時のファイル形式は、原則として、MS-Word、MS-PowerPoint、MS-Excel 又は PDF 形式とする（これによることが困難な場合は、事前に広域機関へ申し出ること）。なお、契約書（案）については、MS-Word 形式とする。

3.3 応札者による提案書の説明（プレゼンテーション）

① 応札者は、広域機関に対し自らの提案内容の説明を行う。

② 当該説明に当たっては、広域機関が指定する場所（Web 会議を含む）にてプレゼンテーションを行うこととし、その際には、原則としてプロジェクト・リーダーに該当する者が実施する。

③ 当該プレゼンテーションの日時等については、入札締切（提案書提出期限）後に広域機関と応札者とで別途調整する。また、プレゼンテーションの時間は、現時点では 1 社あたり 45 分程度（発表 30 分、質疑応答 15 分程度）を想定している。

④ プレゼンテーションにあたっては、与えられた時間を踏まえ、必要に応じて提案書とは別に要約版資料を用意するなど、効率的な実施のために工夫する。

3.4 留意事項

① 提案書を評価する者が特段の専門的な知識や商品に関する一切の知識を有しなくても評価が可能な提案書を作成する。なお、必要に応じて、用語解説などを添付する。

② 提案に当たって、特定の製品を採用する場合は、当該製品を採用する理由を提案書中に記載するとともに、記載内容を証明および補足するもの(製品紹介、パンフレット、比較表等)を添付する。

③ 応札者は提案の際、提案内容についてより具体的・客観的な詳細説明を行うための資料を、添付資料として提案書に含めることができる(その際、提案書本文と添付資料の対応が取れるようにする)。

④ 広域機関から連絡が取れるよう、提案書には連絡先(電話番号、FAX 番号、およびメールアドレス）を明記する。

⑤ 提出物を作成するに際しての質問等を行う必要がある場合には、別紙 3_「質問状」に必要事項を記載の上、2026 年 2 月 9 日（月） １７時までに下記問い合わせ先へ、電子メールで問い合わせる。

【問い合わせ先】

電力広域的運営推進機関　総務部会計室（契約担当）

メールアドレス：keiyaku@occto.or.jp

⑥ 上記の提案書構成、様式及び留意事項に従った提案書ではないと電力広域的運営推進機関が判断した場合は、提案書の評価を行わないことがある。また、補足資料の提出や補足説明等を求める場合がある。

第４章　別紙

4.1　別紙 3_「質問票」

4.1　別紙 4_「適合証明書」

OA システムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託
評価手順書（加算方式）

電力広域的運営推進機関

２０２６年１月

本書は、「OA システムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託」に係る評価手順を取りまとめたものである。落札方式、評価の手続き及び提案の配点基準を以下に記す。

第1章　落札方式及び得点配分

１．１　落札方式

次の要件をともに満たしている者のうち、「１．　２総合評価点の計算」によって得られた数値の最も高い者を落札者とする。

① 入札価格が予定価格の範囲内であること。

②「別紙 5_評価項目一覧」に記載される評価項目のうち評価区分が必須とされた項目を、全て満たしていること。

１．２　総合評価点の計算

総合評価点 ＝ 技術点 ＋ 価格点

技術点＝基礎点 ＋ 加点

価格点＝価格点の配分(※1) × （ 1.0 － 入札価格 ÷ 予定価格)

※1 なお、技術点の配分と価格点の配分は、１ ： １とする。

１．３　得点配分

技術点に関し、**必須及び任意項目の配分を 100 点、価格点の配分を 100 点とする。**

技術点	100 点
価格点	100 点

第2章　評価の手続き

２．１　一次評価

まず、別添「評価項目一覧」の「評価項目」の評価区分が必須の項目について、以下の基準により一次判定を行う。一次評価で合格した提案書について、「２．　２　二次評価」を行う。

・「提案書頁番号」に提案書の頁番号が記入されていること。

２．２　二次評価

「２．　１　一次評価」にて合格した提案書に対し、「３　評価項目の加点方法」にて記す評価基準に基づき採点を行う。その際、別添「評価項目一覧」に記載される「評価項目」のうち必須とされた項目について基礎点の得点が 0 となった場合、その応札者を不合格とする。複数の評価者が評価を行うため、各評価者の評価結果（点数）を合計し、それを平均して技術点を算出する。

２．３ 総合評価点の算出

以下を合計し、総合評価点を算出する。

①「２． ２ 二次評価」により与えられる技術点

② 入札価格から、「１． ２ 総合評価点の計算」に記した式より算出した価格点

③ 技術点及び価格点に小数点第２位以下の端数を生じた場合は切り捨てとする。

第3章 評価項目の加点方法

３．１ 評価項目得点構成

評価項目の得点は基礎点と加点の二種類に分かれており、その合計にて評価項目毎の得点が決定される。（評価項目毎の基礎点、加点の得点配分は「評価項目一覧」の「得点配分」欄を参照）

３．２ 基礎点評価

基礎点は、評価項目の評価区分が必須である事項にのみ設定されている。評価の際には評価基準の基礎点の基準を充足している場合には配分された点数が与えられ、充足していない場合は 0 点となる。応札者は、提案書にて基礎点の対象となる要件を全て充足することを示さなければならない。一つでも要件が充足できないとみなされた場合は、その応札者は不合格となる。各提案要求事項の基礎点を評価する際の観点は、「別紙 5_評価項目一覧」にて「評価基準」として示している。

３．３ 加点評価

加点は、各提案要求事項の加点を評価する際の観点に沿って評価を行う。各提案要求事項の加点を評価する際の観点は、「別紙 5_評価項目一覧」にて「評価基準」として示している。

別紙１

OA システムサービス要求仕様書

電力広域的運営推進機関

２０２６年１月

目次

要求仕様書

1. 調達要件

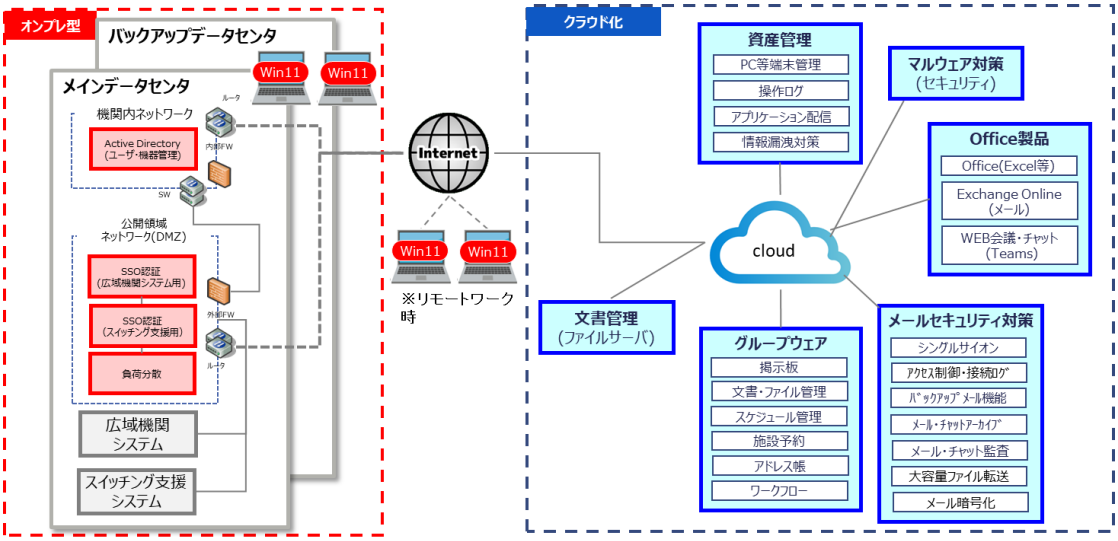
(1) 調達対象

今回の調達対象を次に記載する。

カテゴリ	調達対象	数量
1）設備	ハードウェア、ソフトウェア	一式
	ネットワーク機器	一式
2）役務	要件確認	一式
	設計	一式
	構築	一式
	設置・工事	一式
	試験・チューニング	一式
	移行・切替	一式
3）保守	稼働監視	5年分
	障害対応	5年分
	運用支援	5年分
	ハードウェア、ソフトウェア保守	5年分
4）サービス	外部サービス（※1）	5年分

※1）外部 DNS,NTP 等は外部サービスを利用することを想定しているため今回の提案に含めること。

赤枠（オンプレ型）が今回の調達対象になります。（図はイメージ図です。）



注意）広域機関システム、スイッチング支援システムは、本調達の対象外です。

【 参考 】

※広域機関システムとは

電力の需給状況および系統運用情報等を集約・管理し、広域的な電力需給調整および安定供給を支援するための基幹システムで。

※スイッチング支援システムとは

需要家の電力会社切替（スイッチング）に関する手続きを、小売電気事業者および一般送配電事業者間で円滑に実施するための共通基盤システム。

(2) サービス継続性の考え方

本機関における事業及びシステムは、メインサイトとバックアップサイトを構築するなどサービス継続性をより重要視している。

今回調達する OA システムについても、サービス継続性の考え方継承し、可能な限り地震、災害などの発生時にも継続できるよう関連設備や業務実施拠点などの DR 対応を希望している。

上記背景を理解のうえ、OA システムの継続性について入札者の対策状況を提案書に記述いただきたい。

2. 設備に関する要件

(1) 機能要件

本書で調達する設備に関する機能要件は次のとおりとする。

項目	内容
共通基盤に関する機能要件	
共通基盤 仮想化基盤	• 最新の OS を導入すること。 • 仮想化基盤の場合は、仮想マシンを動作させる機能をもつミドルウェアを導入すること。また、複数の仮想サーバの場合は、一元管理のためのミドルウェア及び信頼性確保のため、クラスター機能を導入すること。 • メインサイト災害時、バックアップサイトに切り替え、業務の復旧が行えるソフトウェアを導入すること。 • メインサイト災害時、以下の作業を自動化すること。（開始作業は手動） (1) IP アドレスの変更（変更しない事も可能） (2) 各種サーバ、仮想マシンの起動
Active Directory に関する機能要件	
基盤	• ドメインコントローラ（メインサイト、バックアップサイト）は冗長構成（2 台以上）とし、サイト間複製を適切に設計すること。 • バックアップおよび復旧手順を整備すること。 • タイムサーバ（NTP）は AD の構成に準拠し、外部時刻同期との整合を取ること。
認証機能	• ActiveDirectory を使用した認証方式であること。 • ドメイン参加端末において、AD 認証によるシングルサインオン(SSO)が行えること。
グループポリシー	• グループポリシーについては、既存のグループポリシーを利用するのではなく、新規に作成すること。 • 外部から入手した実行形式ファイルに対する特定拡張子の実行形式ファイルに対し、実行可否の制御が可能であること。 • 制御の対象は OA システムが管理する端末に限ることとする。 • 特定の実行形式ファイルまたは特定のフォルダ単位でのホワイトリスト形式による実行許可設定が可能であること。 • ドメインおよびローカルのビルトイン Administrator ユーザは実行制御によるブロックが動作しないこと。 • GPO の適用範囲を OU 単位で柔軟に設定できること。（OU 設計を前提とするため） • GPO の適用状況（成功 / 失敗）のログ確認が可能であること。 • ローカル管理者権限の付与方針（LAPS の利用など）を基本設計で定義すること。

	• その他詳細については、基本設計の中で実施すること。
連携機能	• Microsoft Entra ID P1（クラウドサービス）とユーザ情報同期すること。 • 同期対象 OU・属性を基本設計で定義し、不要な同期を行わないこと。 • クラウドサービスで使用する UPN サフィックスがオンプレミス AD と整合するよう設計すること。 • Entra ID 側で多要素認証（MFA）を利用する場合、AD との整合性を取ること。
セキュリティ	• Kerberos の暗号化方式および NTLM 無効化方針を基本設計で検討すること。 • 監査ポリシー（ログオン、アカウントロック、特権操作など）の定義と設定を行うこと。
ログ収集・保管に関する機能要件	
基本要件	• サーバ、ネットワーク機器等のアクセスログ、オペレーションログの収集が可能であること。（クライアント PC については、IT 資産管理にて収集・保管しているため、対象外とする） • 収集したログを検索し閲覧することが可能であること。 • ログ収集対象機器の追加・削除が柔軟に行えること。 • ログ転送プロトコル（Syslog、Syslog over TLS、API 連携など）に対応していること。
収集機能	• 収集対象の機器がリアルタイムでログを収集できること。 • データ量が膨大なアクセスログ等は、負荷の低い夜間/早朝など時間にログ収集の収集/制御ができること。 • ログの重複排除（Deduplication）機能を備えていること。 • ログ受信停止時（機器停止・ネットワーク断等）のアラート通知が可能であること。 • ログ収集失敗時の再送処理が可能であること。
保管機能	• データ量が膨大なログであっても保管とすること。 • 収集したログはアーカイブが可能であること。 • 保持期間を任意に設定できること。 • アーカイブしたログを復元し閲覧できること。 • 保管領域の容量監視が可能であること。
保護機能	• AND/OR 条件を用いたログの検索が可能であること。 • 任意のキーワードによるログの検索が可能であること。 • 異なるフォーマットのログでも横断的にログの検索ができること。 • 検索条件をテンプレートとして保存が可能であること。 • 検索結果の表示を任意の形式にカスタマイズが可能であること。 • 検索結果として表示されたログに対して、絞り込み検索が可能であること。 • 検索結果一覧のエクスポート（CSV、TSV 等）が可能であること。 • 検索実行に関する操作ログ（誰が、いつ、何を検索したか）を記録できること。（内部統制目的） • ログの改ざんを防止する保護機能（改ざん検知／電子署名／ハッシュ化）があること。
集計機能 （任意）	• 収集したログを使用して、表・グラフを使用した集計結果が表示可能であること。 • カスタムダッシュボードの作成が可能であること。 • 異常値や急増ログなどのアラート検知が可能であること。

レポート機能 (任意)	• 検索や集計の結果をレポートとしてファイル出力可能であること。 • レポートに出力する内容やファイル形式を任意のフォーマットにカスタマイズ可能であること。 • 出力したレポートを任意のメールアドレスに自動送信可能であること。 • 定期レポート（毎日／毎週／毎月など）の自動作成スケジュール設定が可能であること。
運用管理機能 (任意)	• 管理者のみがログの検索を可能であること。 • ユーザロール・権限に応じた機能制御（検索／閲覧／設定変更など）が可能であること。 • ログ管理システム自体の操作ログ（設定変更、収集設定、削除操作）が残ること。 • 管理者以外のユーザに対しては必要最小限の権限付与が可能であること。
SSO 認証に関する機能要件	
基本要件	• 現行システムで実装されている機能要件等については、原則としてすべて継続して利用できること。
リバースプロキシ機能	• クライアントから以下システムへの接続に対し、リバースプロキシ機能を提供すること。 ① スイッチング支援システム（本番） ② 広域システム（一般利用者－本番） ③ 広域システム（登録利用者－本番） ④ 広域システム（登録利用者－本番プレ） • 広域機関内の SSO 用として、ID/PW 認証による ID または固定のダミーID をプロキシ先へ連携できること。 • 電子証明書認証時、クライアント証明書（PEM）およびシリアル番号をプロキシ先へ連携できること。 • HTTP ヘッダー追加に対応し、必要な属性を安全に付加できること。
ID・パスワード認証機能	• 接続ユーザに対し、ID/PW 認証機能を提供すること。 • 初期 ID・パスワード情報は、各システムから認証サーバへ登録できること（連携機能を持つこと）。 • パスワード保護のため TLS1.2 以上で通信すること。
電子証明書認証機能	• クライアント証明書により認証し、認証可の場合のみ SSO に接続できること。 • 以下の妥当性確認を実施できること。 ① 証明書提示の有無 ② 証明書の改ざん有無 ③ 発行認証局の確認 ④ 有効期限 ⑤ 失効状況（CRL/OCSP） • 許可されたシリアル番号のみ接続可能とする機能を提供すること。 • 利用事業者単位で証明書を共用することを許容すること。 • 許可証明書シリアル番号の登録・変更・削除機能を提供すること。 • 証明書は広域機関指定の CA 発行を利用し、発行機能は本スコープ外とする。
SAML 認証機能	• 一般送配電事業者システム（10 サイト）に対し、SAML IDP 機能を提供すること。 • 認証ディレクトリ情報を事業者ごとに連携できること。

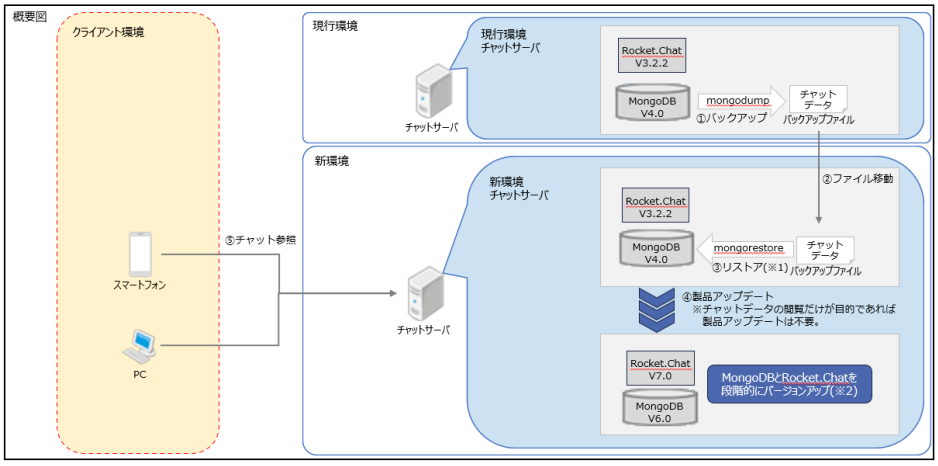
	• 送配電側では、IceWall Federation Agent を使用しているため、これに対応すること。 • SAML2.0 準拠であること。
API 通信認証機能	• 外部 API クライアントからの接続に対し、クライアント証明書認証を行うこと。 • 妥当性確認（証明書提示の有無、改ざん、有効期限、失効、CA 確認）を行うこと。 • 事業者単位での証明書共用に対応すること。 • PEM とシリアル番号を API 連携先へ連携できること。 • 対象： ① スイッチング支援システム API（本番） ② 広域システム API（本番） ③ 広域システム API（本番プレ）
ログアウト機能	• ログアウト用 URL により、認証セッションを完全に切断できること。 • SAML 利用時は SP 連携を含めたシングルログアウトに対応することが望ましい。
認可機能	• 利用者ごとに許可されたリバースプロキシ先にのみ接続を許可すること。 • 権限設定は認証ディレクトリ（LDAP）と連携し、一元管理できること。
認証サーバ	• LDAP による認証プロトコルを提供すること。 • SSO サーバと連携し動作できること。 • 各システムから ID/PW 情報を連携し登録する機能を提供すること。 • 認証サーバ間でデータ同期機能を有すること（多重化構成）。 • LDAP over TLS（LDAPS）に対応すること。
運用管理機能	• パスワード管理 ➢ 利用者自身がパスワードを変更できること。 ➢ 有効期限切れ時にパスワード変更画面へ遷移すること。 ➢ パスワードポリシー設定機能（現行設定を満たすこと）。 ➢ パスワード履歴管理機能（再利用禁止設定）。 • パスワード有効期限管理 ➢ パスワード変更時に有効期限を設定可能であること。 ➢ 有効期限前に警告を行う機能を有すること。 • 証明書管理 ➢ 許可されたシリアル番号の登録・変更・削除を広域機関側で実施可能にすること。
ソフトウェア	• ユーザ画面（ID/PW 入力、エラー画面等）は広域機関指定デザインへカスタマイズできること。 • SSO ソフトウェアは以下を使用すること： ➢ IceWall SSO（IceWall SSO Forwarder、IceWall Federation、SSO 認証モジュール等） ➢ IceWall のバージョンはサポート期間内の最新を使用すること。
システム運用	• 以下の運用機能を提供し、操作マニュアルを提供すること。 ① ログ保管（アクセスログ／システムログ／認証ログ等、5 年間保管） ② バックアップ・リストア ③ システム監視（死活／リソース監視）

	④ ログローテーション・不要ログ削除等の維持管理機能 • 障害発生時のアラートメール通知機能を有すること。
負荷分散機能	• 以下に対し負荷分散（LB）機能を提供すること。 ① 広域システム（一般利用者） ② 広域システム（登録利用者－本番） ③ 広域システム（登録利用者－本番プレ） ④ 広域システム API（本番） ⑤ 広域システム API（本番プレ） • 以下の条件時に指定エラーメッセージを表示できること。 ① 高負荷（アクセス数超過） ② 全ノードダウン ③ LB 冗長化切替（Active → Standby） • セッション固定化（セッションピンニング）を必要に応じて設定可能であること。
その他	• セキュリティ必須要件：TLS/LDAPS、証明書失効確認、HTTP ヘッダーの安全追加など • 実運用に必須の要件：アラート通知、パスワード履歴、SAML2.0 準拠など • IceWall 利用時の抜け漏れ対策：バージョン明記、SLO など
ネットワークに関する機能要件	
基本要件	• 外向けインターネット回線は、既存回線の 2 回線を利用すること。（Active−Active 構成にすること。） ※回線内容 ➢KDDI イーサ 1Gbps(帯域保証型) × 2回線 （メインサイト） ➢オプテージ インターネットハイグレードタイプ G 100Mbps(帯域保証型) × 1 回線（バックアップサイト） • 本番環境とバックアップ環境間については、既存回線の 2 回線を利用すること。 ※回線内容 ➢NTT コミュニケーションズ専用線 200Mbps(帯域保障型) ➢TOKAI コミュニケーションズ広域イーサ 1Gbps(帯域保障型) • 拠点（事務所）とデータセンタ間についても、既存の回線を利用すること。 ※回線内容 ➢データセンタ構内配線光ケーブル 1Gbps(帯域保証型)) × 2 回線（メインサイト⇔A 拠点） ➢TOKAI コミュニケーションズ広域イーサ 100Mbps(帯域保証型) × 1 回線（メインサイト⇔B 拠点） ➢TOKAI コミュニケーションズ広域イーサ 100Mbps(帯域保証型) × 1 回線（バックアップサイト⇔B 拠点） ➢オプテージ イーサネット網 100Mbps(ベストエフォート型) × 1 回線（バックアップサイト⇔バックアップ拠点） • 各回線については、既存の回線を利用するものとする。なお、回線の増強等が必要な場合には、その内容を提案書に記載することとし、増強等の実施は当機関が行うものとする。 • 重要回線・装置については、冗長化（HA 構成）を実施すること。（ファイアウォール、ロードバランサー、コアスイッチ等） • 回線障害時に自動フェイルオーバーし、復旧後に自動復旧（フォールバック）できること。 • 他システムを収容するための追加ポートを確保すること。

ルーティング・冗長化要件	• 本番環境とバックアップ環境間の回線では、回線障害での迂回を実現する為に、ルーティングプロトコルを使ったネットワークの経路交換が可能なこと。 • 対応ルーティングプロトコル（OSPF/BGP 等）を明示すること。 • メトリック制御が可能で、意図しない経路切替が発生しないこと。 • ルートフラッピング抑制が可能であること。
セキュリティ（FW/IPS/SSL）	• インターネット境界に侵入防御システム（IPS）を配置すること。 • 不正侵入検知・防御が可能なこと。 • FW によるアクセス制御が可能なこと。 • 脅威情報（Threat Intelligence）連携対応があること。 • ファイアウォールはアプリケーション制御（L7）に対応していること。（次世代 FW） • ログの長期保管・外部連携（SIEM）に対応していること。 • SSL/TLS 可視化機能（HTTPS インスペクション）への対応していること。 • TLS1.0 および TLS1.1 は非推奨であるため、利用目的および想定されるリスクを明確に説明し、可能な限り利用を停止すること。
SSL アクセラレータ要件（SSO 連携）	• 他システムとの SSO 連携の為、インターネットからの SSL 通信(HTTPS)を SSL アクセラレータ機能にて暗号化/復号化することが可能なこと。 • SSL セッション保証数：50,000 • 無通信時間：2 時間（SSL セッションのアイドルタイムアウト時間） • 暗号化スイート：IPA が発行するガイドラインに準拠すること。 • OCSP / CRL による失効確認方式を明記すること。 • SSL アクセラレータの冗長化（Active-Standby または Active-Active）が可能であること。 • 認証方式はクライアント認証方式として、クライアント証明書から HTTP ヘッダーへクライアント証明書のシリアル番号を追加できること。 • クライアント証明書の妥当性を確認する手法として以下が可能なこと。 ➢ 証明書の有無 ➢ 証明書の改ざん有無 ➢ 発行認証局の確認 ➢ 証明書の有効期限と失効状況の確認 • 証明書失効確認に OCSP または CRL を利用できること。 • 認証成功／失敗、証明書の妥当性確認結果をログ出力できること。 • 証明書関連設定の変更や証明書登録／失効処理について運用ログを記録できること。
スイッチング / LAN 要件	• 機器間を接続の通信帯域は 10Gbps とすること。それ以外については 1Gbps の通信帯域で接続すること。 • 本番環境の業務用端末を接続するスイッチは最大で 350 台～600 台が収容できるポート数を用意すること。 • バックアップ環境の業務用端末を接続するスイッチは最大で 100 台～200 台が収容できるポート数を用意すること。 • スイッチ 2 台で筐体間をまたいだリンクアグリゲーション構成が可能であること。スパニングツリーを使用しないループフリーのネットワーク構成を実現できること。

	• 冗長コアスイッチ構成（VSS/MLAG/Stacking 等）が可能であること。 • PoE+/PoE++ の要否（特に無線 AP・電話機）を提案書に明記すること。 • 端末向けスイッチは ACL による簡易アクセス制御が可能であること。 • STP は使用しない前提でも、BPDU ガード等の保護機能は必要。
無線 LAN 要件	• 事務所エリアの業務端末を接続する有線 LAN と無線 LAN アクセスポイントは、Radius 認証装置と連携することで、802.1X によって認証を行い、許可された端末のみが接続できる認証方式とすること。 • 802.1X 認証はデジタル証明書で認証する方式であること。 • プリンタなどの 802.1x 認証に対応していない機器は MAC アドレスによる認証が可能であること。 • 最新規格 Wi-Fi6（802.11ax）の対応を検討すること。 • 無線 LAN の通信規格は、IEEE802.11a/b/g/n/ac/ax が利用できること。 • 無線 LAN への接続時は、自動的に最適なアクセスポイントを選択すること。 • 無線 LAN もアクセスポイントについては、一元管理できること。 • ローミング最適化（802.11r/k/v）に対応していること。 • 電波干渉の自動調整（チャネル最適化）が可能であること。
QoS / トラフィック制御要件	• 電話システムは他のサービスよりも優先的に音声パケットを転送する必要がある為、電話システムで付与された音声パケットの COS 値を参照して優先制御(QoS 機能)ができること。 • OA システムからインターネット向けの通信に対して、SSO 認証機能については最低保証帯域を設定して、他のサービスにより帯域が圧迫されても通信が可能なこと。 • DiffServ（DSCP）ベースの QoS 設定が可能であること。 • 帯域制御（シェーピング/ポリシング）が可能であること。
ミラーリング要件（SOC 連携）	• OA システムで流れるトラフィックデータを SOC システムで解析する為、任意のポートに流れるトラフィックを、指定した宛先ポートへミラーリング(複製)することが可能なこと。入力、出力双方向のトラフィックをミラーリングできること。 • 複数ミラーセッションの同時実行が可能であること。 • SPAN / RSPAN / ERSPAN の対応状況を記載すること。
障害管理	• SNMPv3 による監視も検討し提案すること。 • Syslog によるログ出力が可能であること。 • ハードウェア故障（電源・ファン等）の監視が可能であること。
保守要件	• 設定情報のバックアップが取得可能であること。 • ファームウェア更新は、無停止で実施可能、または停止時間を極力最小限に抑えて実施できること。
その他要件	• 今回提案するサーバのポートに加えて、他システムを収容する為のポート数を用意すること。 • プライベートアドレスがインターネットに通信する際にグローバルアドレスへアドレス変換をすることで通信できる機能を有すること。 • 同一セグメント内で負荷分散通信をする場合もアドレス変換の機能を有すること。 • 推奨される安全な鍵長および署名アルゴリズム（例：RSA 2048bit 以上、SHA-256 以上）をサポートすること。

	• アドレス変換（NAT）の同時セッション数／スループットが業務継続を満たす性能を有すること。 • NAT 機能は冗長構成（Active-Standby または Active-Active）で提供され、障害時もアドレス変換が継続できること。 • HTTP ヘッダーに追加するフィールド名（例：X-Client-Cert, X-Serial-Number）を任意に設定できること。 • セキュリティについては、現行と同等以上の水準を確保すること。
内部 DNS 機能に関する機能要件	
基本機能	• 内部ネットワークにおける名称解決機能を提供すること。 • 内部ドメインのゾーン管理（A／AAAA／PTR／CNAME／MX 等）が可能であること。 • 外部向け名称解決について、指定したフォワーダ DNS へ問い合わせを転送できること。 • DNS キャッシュ機能を有し、外部問い合わせの負荷を低減できること。
冗長構成・同期	• プライマリ・セカンダリの冗長構成に対応し、いずれか障害時でも名称解決が可能であること。 • ゾーン情報の自動同期（AXFR/IXFR）、または AD 統合 DNS の場合はマルチマスターレプリケーションで同期できること。
クライアント連携	• クライアントが DHCP またはグループポリシーにより自動的に内部 DNS を利用できること。 • （AD 統合の場合）Secure Dynamic Update に対応し、クライアント自身のレコードを自動登録・更新できること。
アクセス制御・セキュリティ機能	• DNS クエリ受付に対して ACL を設定し、内部ネットワークのみからの問い合わせを許可できること。 • DNSSEC の検証または署名に対応していること。
管理機能	• GUI または Web ベースの管理画面により、ゾーン・レコードの作成／更新／削除操作が可能であること。 • 操作履歴（誰が、いつ、何を変更したか）が記録され、確認できること。 • DNS ログ（問い合わせ・更新ログ）が取得でき、外部のログ基盤へ転送可能であること。 • バックアップ／リストア機能を備え、ゾーン情報の復旧が可能であること。
チャット閲覧に関する機能要件	
基本要件	• 現行環境で利用しているチャット機能（Rocket.Chat）を新環境で過去のデータを閲覧できるようにすること。 • 現行環境にて DB バックアップを実施し、新環境へリストアすることでチャットデータ（過去データ）を参照できること。 • RocketChat のデータが格納されている DB(MongoDB)から「mongodump」コマンドを実行し、全データのバックアップを行うこと。（DB バックアップ：バックアップデータはリストアを行うことで、参照可能となる。）
算出条件	• 閲覧目的のみのサーバであるため、公式のシステム要件の最低条件である。 • 「同時接続数：49 台以下」を基準に算出する。

	※公式サイト(システム要件)：https://docs.rocket.chat/docs/system-requirements
CPU(最低スペック)	• 仮想 CPU4 コア 算出の内訳： OS：1 コア、Rocket.Chat：1 コア、MongoDB：2 コア
メモリ(最低スペック)	• 8GB 算出の内訳： OS：1.5GB、Rocket.Chat：2GB、MongoDB：2GB
ディスク(最低スペック)	• 300GB(現行データ閲覧だけを目的とする) 算出の内訳： OS：100GB、現行で使用しているチャットデータ量：125GB、バックアップファイルのサイズ：25GB、作業/予備領域：50GB
Rocket.Chat	• モジュール入手方法 https://github.com/RocketChat/Rocket.Chat/releases/tag/3.2.2 • ドキュメント(インストール手順など) https://docs.rocket.chat/docs/deploy-rocketchat • 対象 OS： Windows / macOS / Linux ※現行で利用している OS：Red Hat Enterprise Linux 8.2
MongoDB	• モジュール入手方法 https://www.mongodb.com/try/download/community-edition/releases/archive • ドキュメント(インストール手順など) https://www.mongodb.com/ja-jp/docs/legacy/ • 対象 OS： Windows / macOS / Linux ※現行で利用している OS：Red Hat Enterprise Linux 8.2
構成図	

(2) 非機能要件

① 規模及び性能

本書で調達する設備に関する規模及び性能について記載する。本機関の通信量を考慮し、十分な性能が発揮できる機種等を選定すること。また、既存のインターネット回線では十分な性能は発揮できない場合は、回線増強（追加）を提案すること。

項目	内容
共通基盤に関する非機能要件	
基盤	• 物理サーバとして設置が必要か検討を実施し、可能であれば仮想サーバとして実装すること。

	➢ Active Directory サーバ ➢ ログ収集・保管サーバ 等
性能・拡張性	• CPU,メモリについては、各サーバおよび導入するミドルウェアの性能要件を満たす製品を選定すること。 • メモリの空きスロット等を残すなど拡張性を考慮した構成とすること。また、スケールアウトが容易な構成とすること。（仮想基盤のみ）
信頼性	• RAID 構成による冗長性を考慮すること。ホットスペアも搭載すること。 • その他サーバに搭載するコンポーネントは冗長性を考慮した構成とすること。 • 電源は冗長構成とすること。
セキュリティ	• ログインしたユーザにより操作の権限が分けられる製品であること。
法令・規程準拠	• 当機関の情報セキュリティ対策規程および関連規程に準拠して設計・構築・運用できること。
システム構成・環境	• メインサイトに本番環境及びバックアップサイトにバックアップ環境を構築すること。 • メインサイトに検証環境を構築すること。 • DMZ セグメント用と内部セグメント用に仮想サーバを分けて配置すること。 • 一元管理用サーバ、バックアップ用サーバは自分自身に DB を持ち、DB には環境に適したソフトウェアを導入すること。
運用・保守	• ハードウェア障害検知が可能であること。 • ハードウェアのメンテナンス時もサーバを停止することなく業務継続可能な仕組みを持つこと。
災害対策	• 本番サイト災害時における、バックアップサイトでのリカバリ開始から OS 起動完了までの復旧時間（RTO）は、以下とすること。 ➢ リカバリ実施：10 分程度（手動実行） ➢ OS 起動：20 分程度 ※サービスレベルの正常確認等は含まない。 • 対象サーバの目標復旧時点は、前回のレプリケーション実行時点とすること。 • 対象サーバの目標復旧レベルは、本番サイト時と同等レベルとすること。
Active Directory に関する非機能要件	
性能・拡張性・信頼性	• 性能見積の範囲は次の業務を対象とすること。 ➢ ドメイン統合認証 ➢ グローバルカタログ ➢ グループポリシー ➢ DNS ➢ NTP • ディスクは RAID により冗長化し、データの信頼性を確保すること。 • 電源は 2 電源により冗長化し、サーバの電源故障による停止を防ぐこと。 • ドメインコントローラを複数台で構成することにより冗長化を行うこと。（本番環境×2、バックアップ環境×1 の冗長構成とすること。） • 長時間 80%を超えた状態が続く場合に CPU 及びメモリの拡張を検討すること。※基準となる CPU リソース量、メモリリソース量のサイジング根拠については各製品の基本設計書に記載すること。

	• ディスク使用率が 80%を超えたらディスク増設を検討すること。 ※基準となるディスクリソース量、サイジング根拠については各製品の基本設計書に記載すること。
ユーザ数	• 利用者数：350 ユーザ ～ 600 ユーザ
同時ユーザアクセス数	• 同時接続数 ： 350 ユーザ ～ 600 ユーザ • 接続端末数 ： 350 台 ～ 600 台
バックアップ	• ActiveDirectory はシステムバックアップとして取得を想定。 • システムバックアップ+システム状態(AD データベースを含む) • 保存世代 ： 3 世代
オンラインリクエスト件数	• 通常運用時のピーク時間帯において、10 分間あたり延べ約 350～600 台程度のクライアント端末からのオンラインリクエストが発生することを想定する。 • なお、当該数値は、ログオン時の認証要求およびディレクトリ参照、DNS 参照等を含む一般的な利用を前提とした想定値であり、性能保証値ではない。
レスポンス制約	• レスポンス制約は、通常運用時における目標値として以下のとおりとする。なお、以下の数値は性能保証値ではなく、システム全体設計および運用により達成を目指すものとする。 ① ログオン時間： 利用者がログオン操作を行ってから、デスクトップ画面が表示されるまでの時間として、概ね 5 秒以内を目標とする。 ② グローバルカタログ応答時間： グローバルカタログ（GC）への認証・検索要求については、要求受付から応答までの時間が、概ね 2 秒以内となることを目標とする。 ③ DNS 参照応答時間： DNS 参照については、要求受付から応答までの時間が、概ね 2 秒以内となることを目標とする。
スループット制約	• 通常運用時のピーク時間帯において、以下の処理が安定的に行えることを目標とする。なお、システム設計における想定値であり、性能保証値を示すものではない。 • 業務システム利用時の統合認証要求については、10 分間あたり延べ約 350～600 ユーザ程度の要求発生を想定する。 • 名前解決（DNS）要求については、10 分間あたり延べ約 350～600 台程度のクライアント端末からの要求発生を想定する。
負荷分散	• 性能と拡張性を確保するため、アプリケーションで必要に応じて負荷分散機能の導入を実施すること。（但し、バックアップ環境は、シングル構成であるため DR 発動時には負荷分散は実施しない。）
管理権限の認証	• システム管理者の認証方式は ID/パスワード方式とすること。 • パスワードは広域機関のセキュリティポリシーにあったパスワードを設定すること。 ※但し、製品に設定可能なパスワードの制約がある場合は例外とすること。 • 認証失敗時の動作については以下とすること。 ① 認証エラーを認証要求元へ返すこと。 ② 認証要求元のエラー受信時の動作に従うこと。 ③ ドメインコントローラへのログオン要求の場合は、ログオンを拒否すること。

	④ 連続で一定回数以上の認証エラーが発生した場合は、アカウントロックを行うこと。 • 多重ログインの制御は以下とすること。 ① ドメインコントローラへの同時ログオンを許可すること。 ② ドメインコントローラへのログオンに関しては、同一のセッションへのログオンとすること。（自動的にログオン済みのセッションへ再ログオンすること。）
利用者の認証	• システム利用者の認証方式は ID/パスワード方式とすること。 • パスワードは広域機関のセキュリティポリシーにあったパスワードを設定すること。 ※但し、製品に設定可能なパスワードの制約がある場合は例外とすること。 • 認証失敗時の動作は以下とすること。 ① 認証エラーを認証要求元へ返すこと。 ② 認証要求元のエラー受信時の動作に従うこと。 ③ PC へのログオン要求の場合は、ログオンを拒否すること。 ④ 連続で一定回数以上の認証エラーが発生した場合は、アカウントロックを行うこと。 • 多重ログインの制御は・同一ユーザによる複数の PC への同時ログオンを許可すること。 • サーバのアクセスコントロールはサーバの性質（用途、重要度など）やユーザの役割（部門管理者、利用者など）に応じて、適切にアクセス権を設定する事で実現可能であること。 • ActiveDirectory のアカウント管理でコントロールすることが可能なこと。
バックアップ・復旧	• バックアップ対象とするデータのリストアのみで問題なくシステムが復旧可能であること。Windows ドメイン統合認証では、データ保全の対象として、データ領域（データベース、DNS データ）等を考慮すること。 • Windows Server バックアップにより、データ領域をオンラインバックアップする事により実現すること。 • Primary リストア により、最終バックアップ時点の状態へ復元すること。 • ２重障害時は、バックアップ採取時点に復旧できること。（ActiveDirectory はバックアップサイトの生存している機器からのデータ同期で復旧できること。） • 片系障害時は、生存している機器からのデータ同期で復旧できること。 • データの完全性/整合性の確認を各動作アプリケーションの検出機能によって行えること。
障害対応	• ハードウェアが故障した際、以下の障害復旧施策を実施すること。 ① 片系筐体故障時（冗長構成）：片系で継続動作可能なこと。 ② 両系筐体故障時（冗長構成）：多重障害時はバックアップサイト側へ認証経路を自動的に切り替えることにより、業務を継続できること。 • OS/ミドルウェアが動作しなくなった際、以下の障害復旧施策を実施すること。 ① 片系 OS/ミドルウェア障害時（冗長構成）：片系で継続動作可能なこと。 ② 両系 OS/ミドルウェア障害時（冗長構成）：多重障害時は認証経路（認証を処理する経路（本番⇔BU））を自動で切り替わることにより業務を継続すること。

	• スローダウン障害が発生した際、以下の障害復旧施策を実施すること。 ① 片系スローダウン発生時（冗長構成）：業務継続不可と判断された場合は、切替を実施し原因を調査したうえで、障害箇所の保守を実施すること。復旧時には通常運用時の状態に切り戻すこと。 ② 両系スローダウン発生時（冗長構成）：業務停止時間を最小限に留め、最短で保守を実施すること。 ③ 単一構成スローダウン発生時：業務停止時間を最小限に留め、最短で保守を実施すること。
DR 対応	• 本番環境からバックアップ環境への切り替え方法について、機能停止時に自動で切り替わること。 • 目標復旧時間は、数分以内での切り替えを実現すること。 ※オペレーターの準備時間含まないものとする。 ※マルチマスターであるため、切り替えは自動的に行われること。 • 目標復旧時点は、災害・障害発生時点のデータを復旧できること。 • 目標復旧レベルは、災害・障害発生前と同等とすること。
セキュリティ対策	• 設計開始時に各製品ベンダーから提供される最新の修正プログラムを導入すること。 • 各製品ベンダーから提供される修正プログラムの適用については、システムにて自動配布ではなく、個別の適用とすること。 • 各製品ベンダーから提供される不具合解消やセキュリティ上の問題を解決する緊急性の高い必要プログラムを適用すること。 • 各製品ベンダーから提供される修正プログラムの適用については、事前に検証環境で検証を行った上で適用を実施すること。 • 各製品ベンダーから提供される修正プログラムの適用頻度については、緊急性の高い修正プログラムは必要に応じて早急に適用すること。緊急性の高くない修正プログラムは定期的にまとめて適用すること。 • 不正監視（証跡管理）とし、ログオン履歴、アカウント変更履歴、ポリシー変更履歴等のログが取得可能なこと。 • ログの保存期間は 5 年間とすること。
管理者教育	• 当機関側で実施する作業がある場合には、手順書を作成すること。
法令・規程準拠	• 当機関の情報セキュリティ対策規程および関連規程に準拠して設計・構築・運用できること。
SSO 認証機能に関する非機能要件	
基本方針	• 現行構成を維持しつつリプレースし、稼働に影響を与えない移行方式とすること。 • 365 日 24 時間稼働を前提とし、一部サーバ障害や計画作業によって 認証全体が停止しない冗長構成 とすること。 • 障害発生時も認証セッションが途切れないようセッション維持を可能とすること。 • 本番環境の主要コンポーネントは冗長化し、L7/L4 ロードバランサによる負荷分散を行うこと。 • 大規模災害時は、バックアップサイト（大阪 or 東京）へ速やかに切替可能な DR 構成を実装すること。

	• 本運用拠点が被災した場合でも、インターネット経由で公開サーバへのアクセスを継続できる機能を有すること。
処理能力・性能目標	• 想定ユーザ ➢ 外部：130,000 ユーザ ➢ 内部：350～600 ユーザ • 最大同時アクセス：3,000 hit/min（50 hit/sec） • ピーク同時ログインユーザ数：40,000 • 想定トラフィック：ピーク 16Mbps、通常時 4.8Mbps
応答時間	• リバースプロキシ応答 ⇒ 通常：1 秒以内、輻輳：5 秒以内 • 認証応答 ⇒ 通常：2 秒以内、輻輳：10 秒以内
拡張性	• システム停止を伴わず、CPU・メモリ等のスケールアップ、ノード追加によるスケールアウトが可能であること。 • ユーザ増加（特に電子証明書失効管理数増）に対応可能なアーキテクチャとすること。 • 将来的な拠点増設にも対応できる構成とすること。
信頼性・保守性	• バックアップ ➢ システム領域：最新 1 世代 ➢ データ領域：14 世代（14 日分） ➢ すべてのバックアップは専用ネットワークでセンター間同期されること。 ➢ システムバックアップは構築完了後および設定変更の都度取得すること。 • リストア ➢ ソフトウェア機能およびログ管理サーバと連動し復元可能とすること。 ➢ データ破損時は最新バックアップから復旧できること。 ※バックアップ対象外データ（当日ログ等）は復旧不可である旨を明確化すること。 ➢ ディスク障害でバックアップが参照できない場合は手動再作成が可能なこと。
運用手順	• 以下の運用マニュアルを整備すること。 ① 障害・災害対応手順 ② バックアップ／リストア手順 ③ 停止・起動手順 ④ 証明書シリアル番号管理手順 ⑤ ログ監査手順 ⑥ 監視アラート対応手順 ⑦ データ補正手順 ⑧ 接続システム向け技術資料
障害復旧要件（RPO / RTO / RLO）	• 本調達に係るシステムについて、以下の障害発生パターンを想定し、復旧要件（RPO／RTO／RLO）を満たすこと。 ✓ 本番パターン：通常運用時の本番環境における障害復旧シナリオ ✓ 別パターン：災害時または縮退運用時等、本番環境とは異なる構成・運用形態（バックアップ環境等）における障害復旧シナリオ • パターン 1：HW／SW 障害（本番パターン） ➢ RPO：システム＝最新バックアップ、データ＝リアルタイム同期

	➢ RTO：基盤復旧完了後、4 時間以内 ➢ RLO：100% • パターン 2：データ破損（本番パターン） ➢ RPO：最新バックアップ ➢ RTO：復旧作業開始後、4 時間以内 ➢ RLO：100 • パターン 3：HW／SW 障害（別パターン） ➢ RPO：システム＝最新バックアップ、データ＝前夜バックアップ ➢ RTO：OS 復旧後、即時に業務再開可能であること ➢ RLO：100% • パターン 4：データ破損（別パターン） ➢ RPO：最新バックアップ ➢ RTO：翌営業日までに業務を開始できること ➢ RLO：100 ※別パターンにおいては、当日分ログの復旧は対象外とする。
セキュリティ	• 認証時通信は HTTPS を使用すること。（※一般利用者向け広域システムは除外） • リバースプロキシ接続・API 連携は原則 HTTP だが、HTTPS 対応可能とすること。 • パスワードは非可逆暗号化方式で保管すること。 • FW によりネットワーク境界で IP/ポート制御を実施すること。 • 各種ログ（アクセスログ、認証ログ、操作ログ）は保存し、追跡可能とすること。 • 不正アクセス検知および証跡保全を実施すること。 • NTP により全サーバ時刻同期を行うこと。
接続要件	• 東京／大阪の 2 データセンタで稼働し、センター間の同期が可能であること。 • 運用拠点（東京×2・大阪×1）が増加しても対応可能なネットワーク設計とすること。
運用	• バックアップ・同期・監視など、運用に必要な作業は可能な限り自動化すること。 • 監視システムと連動し、プロセス死活・ジョブ結果・リソース状況を監視すること。 • 手動バックアップおよびリカバリ手順も提供すること。 • 検証環境はシングル構成とし、ユーザ数は 100 未満で運用する想定である。
移行	• 現行 SSO 認証システムのユーザデータは引き継ぎ、業務継続性を確保すること。 • 本番切替時はユーザ影響を最小化し、停止時間を極力短くすること。 • 必要に応じ、接続システム向けに仕様変更資料を作成・説明すること。
教育	• 本番移行前に職員・運用者向けの説明会を実施すること。 • 検証環境の運用開始前に、運用者向けの操作説明をマニュアル等を用いて実施すること。
監視機能に関する非機能要件	
運用	• 24 時間 365 日無停止要件 ➢ 全体要件として「24 時間 365 日無停止」を前提とする。 ➢ ただし、バックアップ取得に伴う OS 停止が必要な時間については、監視機能が維持される範囲で停止を許容することとする。

	➢ システムを停止する場合は、事前調整のうえ計画停止として実施すること。 • 本番／バックアップ相互監視 ➢ 本番環境とバックアップ環境間で監視サーバを相互運用し、監視システム自体の無停止を確保すること。 ➢ バックアップ拠点の監視サーバ導入前に限り、システムバックアップや OS 停止時に 監視が一時停止することを許容する。
目標復旧水準（RPO ／ RTO ／RLO）	• RPO（Recovery Point Objective） ➢ シングル構成（本番のみ）：1 営業日前（前日のバックアップ） ➢ 主従構成（メイン・BU 間の相互監視時）：ほぼゼロ（即時切替により業務継続） • RTO（Recovery Time Objective） ➢ シングル構成（本番のみ） • 監視業務再開：3 時間以内 • 製品機能の復旧：3 時間以内 ➢ 主従構成（相互監視時） • 監視業務：即時（片系へ自動切替） • 障害側サイトの本復旧：24 時間以内 • RLO（Recovery Level Objective） ➢ シングル構成 • 日次バックアップより復旧 → 2 時間以内に監視業務再開 • イベント DB の復旧は監視再開後に実施 ➢ 主従構成 • バックアップ環境側で即時監視再開
災害復旧（DR）	• 本番・バックアップ環境の相互監視により、片側被災時でも監視を継続できる構成とすること。 • 監視サーバの切替は自動または最小オペレーションで可能とすること。
性能・拡張性	• 監視対象規模 ➢ 監視対象ノード：本提案のサーバ群を 1 台の監視サーバで一元管理できること。 ➢ 監視対象サービス・プロセス：サーバ 1 台あたり、合計で 100 サービスまたは 100 プロセスまで監視できる製品であること。 • 拡張性 ➢ ノード増加に伴い、監視対象の追加登録に制約がないこと。 ➢ 必要に応じて監視サーバのスケールアウトができることを必須要件とする。
ログ保管	• 保管期間：5 年間 • 保管対象：監視製品の製品ログ、監査ログ、アラート履歴 • ログは検索可能かつ改ざん防止措置（アクセス制御・ロール管理）を講じること。 • ログのエクスポート（CSV/TSV/XML）に対応していること。 • 保管領域が不足する場合は自動ローテーションが可能なこと。
運用・保守	• 監視体制 ➢ 本番環境は 24 時間 365 日の監視が可能 な仕組みとすること。

	➢ 24 時間監視のため、必要に応じ 遠隔地から監視可能なステークホルダ（運用者）を配置できること。 • 検証環境 ➢ 検証環境には監視サーバを設置すること。 ➢ 検証環境のアラートは運用管理サーバへ通知のみ行い、監視業務としての対応は不要とする。 • 監視対象の通知 ➢ 検証環境、本番、BU すべての障害通知が運用者へ送信されること。 • その他 ➢ 監視テンプレート、閾値設定が GUI で変更可能であること。 ➢ アラートはメール・SNMP・Webhook いずれかで通知可能なこと。 ➢ 重要アラートはエスカレーションルールを設定可能なこと。
開発用環境	• メインサイトに検証環境を設置し、検証環境の監視は検証環境側の監視サーバから行うこと。 • 本番・BU 環境は、検証環境側監視サーバから対象外とし、相互監視は本番・BU 間で完結させること。
セキュリティ	• 監視サーバ・監視画面へのアクセスはパスワード認証を必須とすること。 • FW にてアクセスを制御し、登録済み監視端末からのみアクセス可能とすること。 • 管理者権限の分離（閲覧・設定変更）を行えること。
法令・規程準拠	• 当機関の情報セキュリティ対策規程および関連規程に準拠して設計・構築・運用できること。 • リモート監視に関するデータ取り扱いも内部規程に従うこと。
ログ収集・保管に関する非機能要求	
可用性 / 信頼性	• ログ収集・検索・閲覧機能が継続的に利用できるよう、システム全体として高可用性を確保すること。（システム稼働率 99.9%以上） • ログ収集処理が失敗した場合、再実行やリトライにより確実にログを取得できる仕組みを備えること。 • 収集対象機器からのログ転送において、通信断・機器障害時にも一定期間のバッファリングが可能であること。 • ログデータの破損防止・整合性を保証できる仕組み（チェックサム等）を有すること。
性能要件	• 同時複数のログ検索や大量データの処理において、一定の検索応答性能を確保すること。（例：通常検索は数秒以内に応答） • 膨大なアクセスログのバッチ収集について、夜間・早朝の時間帯内で処理が完了できること。 • 取り扱うログデータ量は、年あたり数億レコード規模（数百 GB～数 TB／年）のログデータ量が発生することを想定し、保存期間中の累積データ量を含め、性能劣化なく運用できること。
拡張性 / スケーラビリティ	• 対象装置やログの増加に応じ、性能を維持したままストレージ容量や収集ノードを拡張できること。 • 異なるフォーマットのログ（サーバ・ネットワーク機器・アプリケーション等）が追加されても対応できる柔軟な構造であること。

	• アーカイブデータの増加に伴い、長期保存用ストレージを容易に拡張・移行できること。
運用性 / メンテナンス性	• 運用担当者が日常的に収集状況・稼働状況を把握できる管理 UI を備えること。 • 障害発生時には原因特定に必要なシステムログ・処理ログが取得できること。 • 管理者による設定変更（収集スケジュール、検索テンプレート、アーカイブ設定等）が容易に行えること。 • 定期的な保守作業（パッチ適用、データ削除、アーカイブ処理）が運用負荷なく実行できること。
セキュリティ要件	• ログ閲覧・検索・設定変更を行えるのは権限を付与された管理者のみであること（アクセス制御）。 • ログデータが改ざんされないよう、保存領域および転送経路でのセキュリティ確保（暗号化、署名等）が可能であること。 • 管理者用アカウントには認証強化（多要素認証など）が適用可能であること。 • ログデータの閲覧履歴や検索履歴も監査ログとして取得できること。 • 保存するログデータについては、当機関のセキュリティ規程に準拠した保管方式と保存期間を満たすこと。
保管要件 / データ耐久性	• ログデータが紛失・消失しないよう、保存領域は高耐久性ストレージ（冗長化構成）を使用すること。 • 一定期間保存後はアーカイブ領域へ自動移行し、長期保存に耐えうる媒体で保管すること。 • バックアップ／リストア機能により、障害時でもログデータを復旧可能であること。 • 保存期間（５年間）が満了するまでは確実にデータが維持されること。
可観測性（監視）	• ログ収集プロセス、ストレージ容量、収集エラーなどを監視システムと連携して通知できること。 • ログ収集の失敗や異常検知時に、管理者へ自動的にアラート通知が行われること。
法令・規程・監査対応	• 当機関の「情報セキュリティ対策規程」および関連規程に適合すること。 • ログ管理に関する各種ガイドライン（例：総務省ガイドライン、監査要件等）に準拠すること。 • 保存されたログデータが監査時に参照・出力可能であること。
ネットワーク機器に関する非機能要件	
可用性	• 本番環境は、24 時間 365 日無停止稼働とする。 • 計画停止は必要に応じて実施可能とするが、事前に調整すること。 • 本番環境のネットワーク切替は 10 秒以内に完了すること。（（本番環境内の冗長経路切替等。） • 本番 DC の機器は、冗長構成とする。（電源冗長含む） • 多重障害時でも、機器間のパスが確保できる限り継続稼働できること。 • バックアップ環境・検証環境は、シングル構成とし、可用性要件の対象外とする。 • 回線・機器の交換による復旧が可能であること。 • 外部接続システムは 24 時間 365 日稼働であり、両系同時に停止しないこと。
性能・スケーラビ	• 本番環境のアクセス対象は、300～600 名。（同時アクセス含む）

リティ	• バックアップ拠点は、100～200 名。（同時アクセス含む） • 検証環境はユーザ数を規定しないものとする。 • グローバル IP の拡張は、/25 の範囲で行えること。 • プライベート IP アドレス拡張が可能であること。 • 回線帯域拡張は以下により実現可能であること。 ① 回線数の追加 ② 回線装置の増設・置換 ③ リンクアグリゲーションによる束ね ④ 回線種別の変更 • SSO 認証・広域機関システム（JX 手順）の通信帯域は、帯域保証の設定を行うこと。 • 負荷分散機能（LB）を導入すること。
信頼性	• 本番 DC／バックアップ DC のネットワークセグメントは同一構成とする。 • NW セグメントは重複しないこと。 • 障害発生時は切り戻しが可能なように、切替計画とバックアップ設定を保持すること。 • ハードウェア障害発生時も 継続可能な冗長構成とすること。 • バックアップ DC では、縮退運転により本番の構成を引き継げること。
保守性・運用性	• テストは計画書・成績書に基づき実施し、結果を記録すること。 • トラブル発生時には即座に切り戻し可能であること。 • システム運用者向けに、以下を整備すること。 ➢ 操作マニュアル ➢ 構築手順書 ➢ 障害復旧手順書 • 本番移行前にシステム運用者へ教育を実施すること。 • レイアウト変更等に伴う有線 LAN 敷設・HUB 増設/移設を当機関で実施可能とするため、構成管理および手順を提供すること。
セキュリティ	• 不正アクセス対策として、802.1X を用い正規端末以外は接続不可とすること。 • FW による外部攻撃防御、およびポリシー設定の標準化を実施すること。 • 管理者権限は必要最小限の者に付与し、不正な設定変更を防ぐこと。 • 機器コンフィグは確実にバックアップし、改ざんを防止すること。 • すべての設定変更はログを取得すること。 • 監査ログ・アクセスログは以下の期間保管すること。 ➢ 本番 DC、バックアップ DC：5 年間 ➢ 検証環境：1 年間 • SSH（暗号化通信）にて管理を行い、ID/Password は英数字混在、アカウントロックなしこと。 • 多重ログイン制御は行わないこと。 • 情報セキュリティ対策規程および関連規程に準拠すること。
テスト容易性	• すべての導入機器を対象にテストを実施すること。

	• バックアップ環境および検証環境もテスト実施に活用すること。 • システムテストではネットワーク診断（ペネトレーションテスト等）を実施すること。
拡張性	• 拠点数は増加する可能性があるため、追加拠点への対応が可能な構成とすること。 • IP アドレス枯渇を起こさないアドレス計画を採用すること。 • 機器のモジュール交換や増設により性能向上できること。
運用制約	• 計画停電は想定しない。 • 外部接続システムに対し、両系同時停止は禁止する。 • 被災時のみバックアップ拠点を利用する。 • 検証運用拠点は存在しない。
外部接続システム	• 本番環境およびバックアップ環境は、以下のシステムに接続できること。 ➢ 広域機関システム ➢ スイッチング支援システム ➢ 電話システム ➢ SOC システム • 検証環境は、広域機関システム、スイッチング支援システムのみとする。 • 外部接続システムは、 24 時間 365 日である。
その他	• 無線アクセスポイント数及び設置場所については、現状の数量、場所を参考に提案すること。（机上の検証だけでなく、実際に安定した接続・利用が出来るようにチューニングすること。）
内部 DNS 機能に関する非機能要件	
可用性	• システム全体として、DNS サービスが高可用であること（例：99.9%以上）。 • 障害時にはセカンダリへ自動的にフェイルオーバーし、利用者影響を最小化すること。
性能・スケーラビリティ	• 想定クライアント数（350～600 台）からの同時問い合わせに耐える性能を有すること。 • ゾーンレコード数が数千件規模になっても性能劣化なく運用できること。 • 名前解決のレスポンス時間が一定水準（例：10ms 以内：内部）を満たすこと。
保守性・運用性	• 運用担当者が容易に設定変更・確認を行える UI を備えること。 • 設定変更時には変更管理プロセスに基づき、構成情報を記録・保持しやすいこと。 • バージョンアップ、セキュリティパッチの適用が容易であること。
セキュリティ	• 管理アクセスは管理用ネットワークに限定され、不正アクセス防止措置（認証・多要素等）が実施可能であること。 • ログを一定期間（5 年間）保管できること。 • セキュリティインシデント発生時に迅速な原因追跡が可能なログ構造を有すること。
信頼性	• ゾーン情報の整合性が維持されること（レプリケーション異常時の検出機能を含む）。

	• 障害の検知・通知（死活監視・サービス監視）が監視システムと連携して行えること。
移行性	• 現行 DNS 環境からゾーン情報を移行できること（必要に応じてレコードのインポートが可能）。 • 設置から運用開始までの導入スケジュールに沿った構築が可能であること。
法令・規程準拠	• 当機関の情報セキュリティ対策規程および関連規程に準拠して設計・構築・運用できること。

② 信頼性・拡張性

本書で調達する設備に求める信頼性及び拡張性について記載する。

項目	内容
共通の要件	
稼働時間	• 24 時間 365 日の運用を前提とし、定期的な再起動やバージョンアップ以外の保守時の停止を要さないこと。
耐障害性	• 耐障害性の高い機器を選定すること。
信頼性	• 調達対象の設備に障害が発生しても、本機関の業務に影響を与えない製品を選定すること。
バックアップ	• 設定ファイルは、設定変更後の状態をリカバリポイントとすること。ただし、デバイス内に記録するログ等のデータは、リカバリ対象から除く。
拡張性	• 通信量が 2 倍となった場合でも、設備増強を必要としない製品を選定すること。

③ 情報セキュリティ

本書で調達する設備に求めるセキュリティについて記載する。本書の要件に鑑み、追加で考慮すべきセキュリティ施策がある場合は、本機関に提案すること。

項目	内容
ファームウェア	• 最新の OS 及びファームウェアを利用し、既知の脆弱性のない状態で納品すること。
管理者 ID	• 管理者 ID は、本機関及び受託者で異なる ID を発行し、必要最低限の権限のみ与えること。 • 当機関の管理者 ID は共有ではなく、個人単位で発行すること。 • 当機関の管理者が変更になった場合は、パスワード変更出来ること。変更することで設定変更等の作業が発生しないようにすること。

3. 役務に関する要件

(1) 業務要件

① 業務実施手順

本書で調達する役務について、要件を記載する。

フェーズ	作業内容
要件確認	• 本機関における要件（本書の要件）について、受託者との認識のずれや齟齬がないことを作業着手前に確認すること。

	• 受託者が作業開始までの作業を進めるにあたり、前提となる要件を本機関にヒアリングし、当該内容を要件確認書として取りまとめること。 • 要件確認の内容を本機関と合意のうえ、設計作業に着手すること。
設計	基本設計 • 要件確認に基づき、必要なシステム及びシステムで利用する全ての機能について設計し、基本設計書として取りまとめること。 • ネットワーク環境や機器のログ・アカウントなどの設計を行うこと。 • 現行ネットワークを維持しながら段階的に構築できること。 詳細設計 • 基本設計に基づき、必要なシステム及びシステムで利用する全ての機能について設計し、詳細設計書として取りまとめること。 運用設計 • 業務及びシステム運用における業務フロー、手順（判断基準を含む）、バックアップサイトへの切替手順、体制、連絡先を設計し、受託者のサービス仕様を運用設計書に取りまとめること。また、業務に係る通知メールやレポート等の内容についても、設計フェーズで本機関と合意すること。 • 運用設計書には、本機関と受託者との役割や責任及び情報連携方法などを含めること。 • システムの障害時に影響を受ける業務や業務復旧までの時間及び対応フローについて運用設計書に取りまとめること。 • システムの設定変更に関する依頼フォームを提示し、本機関と合意すること。 試験設計 • 単体試験、結合試験、障害試験、情報セキュリティの観点に基づく試験などの試験項目を計画し、その合否判定基準を設計すること。 • 運用設計にもとづき、業務及びシステム障害を想定したシナリオテストを行うこと。 移行設計 • 各環境の切替は、本番影響を最小化する方式で行うこと。 • 本機関の既存システムに影響をあたえないように、設置作業及び工事計画を立て移行設計書として取りまとめること。また、既存システムとの接続に際し、リスクや留意事項があれば、本機関に提示すること。 • 本機関の既存システムに設定変更を必要とする場合は、その内容や順序についても可能な限り支援すること。 • 移行については、限りなく無停止で実施できるように計画を立て移行設計書として取りまとめること。
構築	• 設計に基づき、システムの設定値を設計し、セットアップすること。 • 各ハードウェア、ソフトウェアは、既知の脆弱性がないソフトウェアで構築すること。 • システムのバックアップファイルを取得すること。
設置・工事	• 本機関の指定したサーバラックに機器を設置すること。（ラックマウントキットは用意すること） • インターネット回線の工事を行うこと。

	• 機器をラックに搭載し、各機器間をネットワークケーブルで結線すること。なお、本機関の既設機器との接続にあたっては、本機関の既存システムの停止は不可（停止が必要である場合は 2 重化を切り替えながら実施）であることを前提に、平日深夜又は休日の作業を想定すること。 • 接続に必要となるネットワークケーブル等は、本業務の受託者にて用意すること。 • データセンタでの工事にあたり必要な申請は本機関にて実施するが、申請内容の作成は受託者が実施すること。 • 当機関執務室（第一事務所、第二事務所、バックアップ拠点）に対し、無線アクセスポイントの設置、有線 LAN の敷設を実施すること。 • 既存の無線環境に影響を与えないように考慮し実施すること。
試験	• 試験設計に基づき、システムの試験を実施すること。 • 単体で、各機能が適切に動作していることを確認すること。 • 本調達に係るシステム及び各機能を結合し、設計通りに動作していることを確認すること。 • バックアップ及びリストアの試験を実施し、設計通りに障害からの復旧ができることを確認すること。 • 運用開始にあたり、本機関は情報セキュリティに関する検査を実施すること。
切替・移行	• 受託者は、試験が完了した後、あらかじめ本機関の承認を得た切替計画に基づき、現行システムから本調達に係るシステムへの切替及び移行作業を実施すること。 • 切替及び移行作業にあたっては、本機関の業務に与える影響を最小限に抑えるよう十分に配慮し、切替手順書、移行手順書及び作業スケジュールを作成し、本機関の承認を得ること。 • システム切替前後において、移行対象となるデータの完全性、正確性及び整合性が確保されていることを確認すること。 • 切替及び移行作業中または作業後に不具合等が発生した場合に備え、切戻し手順をあらかじめ定め、当該手順に基づき確実に切戻しが可能であることを確認すること。 • 切替及び移行完了後、本調達に係るシステムが設計どおりに稼働していることを確認し、本機関による運用開始に支障がないことを確認すること。

② 業務実施期間

本書で調達する役務について、本機関が想定している実施期間を記載する。

フェーズ	実施期間
要件確認	• 契約締結日～2026 年 7 月中旬
設計	• 2026 年 7 月中旬～2026 年 10 月中旬
構築	• 2026 年 10 月中旬～2026 年 12 月中旬
設置・工事	• 2027 年 1 月中旬
試験	• 2027 年 2 月中旬
切替・移行	• 2027 年 2 月下旬～2027 年 3 月末
チューニング	• 2027 年 2 月下旬～2027 年 3 月末

③ 業務実施場所

本調達に係る作業は、本機関が承認した作業場所でのみ実施を許可する。

項目	内容
作業場所	• 本役務の一部は、受託者の事業所内での実施を許可するが、事前に作業内容と作業場所について本機関の許可を得ること。 • 本役務に関する打合せ、レビュー、報告会議等については、本機関が提供する会議室で実施すること。 • 本役務における設置工事、試験については、本機関が指定するシステム設置場所で実施すること。

④ 業務管理

受託者は、次に示す管理業務を、本業務の全工程に渡り実施すること。

項目	内容
進捗管理	• 進捗管理については、プロジェクト計画書に基づき各タスクの状況把握及びスケジュール管理を行うこと。
リスク管理	• 各作業工程における目標の達成に対するリスクの抽出、リスクの影響を最小限にする対応策の実施等のリスク管理を行うこと。
文書管理	• 各作業工程において作成する設計書等の文書について、改ざん、漏えい、盗用及び目的外の利用を未然に防止するよう文書管理を行うこと。
課題管理	• プロジェクト遂行上様々な局面で発生する各課題について、課題の認識、対応案の検討、解決までの追跡等の課題管理を行うこと。
品質管理	• 品質評価計画の立案、検証及び品質改善策の検討、実施を管理する体制の構築等の品質管理を行うこと。
人的資源管理	• 本調達に参画する要員の選定、変更及び体制維持に関する管理を行うこと。 • 主たる要員に変更が生じた場合には、本機関へ報告すること。また、代替要員については、サービスレベルの低下を防ぐために、知識及び経験が妥当な者を選定すること。
コミュニケーション管理	• 各作業工程における各種作業に関する打ち合わせ、成果物等のレビュー、進捗確認、課題共有等を行うためのプロジェクト会議を開催すること。
構成・変更管理	• 構成管理対象（設計書等）を特定し、管理レベル（参照・更新権限、保存方法・期間等）を定めること。

4. 保守に関する要件

(1) 業務要件

① 業務実施内容

本書で調達する保守及び運用業務について、要件を記載する。

項目	内容
稼働監視	• 本システムのデバイス及び提供機能を監視し、障害発生を検知した場合は、速やかに本機関にメールと電話で報告を行うこと。 • 稼働状況が確認できるための監視ポータル（監視結果レポート画面）を用意すること。

	• トラフィック量やリソース情報を監視し、品質の低下が危惧される場合は通知すること。
障害対応	• システム障害を検知した場合は、速やかに切り分けを実施の上、事象及びその原因特定、及び復旧作業を行うこと。なお、障害対応においては、本機関と密に情報連携を行うこととする。（情報連携の方法等は運用設計で定義すること。） • 必要に応じて、ハードウェアを交換し、最新のバックアップファイルからリストアを行うこと。
運用支援	• ソフトウェアおよびファームウェアのバージョンアップ等のアップデートについては、保守サービスの範囲内で実施すること。 • ハードウェアおよびソフトウェアに係る脆弱性対応については、保守サービスの対象範囲とすること。ただし、重大な脆弱性が発見された場合には、本機関および受託者それぞれの業務範囲を明確にしたうえで説明を行い、速やかに対応を実施すること。 • 本システムの提供機能に係る設定変更（保守業務として実施する設定変更および本機関からの軽微な依頼（月 1～2 回程度を想定）を含む）を実施すること。なお、設定変更は本機関からの依頼日を起算日として、原則 5 営業日以内に実施すること。ただし、緊急性の高い設定変更については、原則 1 営業日以内に実施するものとする。また、緊急性の高い設定変更であっても、影響調査や情報分析等を要する場合に限り、両社協議のうえ合意した日程にて実施すること。 • 保守業務等に伴う設定変更、バージョンアップ等の作業については、本機関の業務に影響を与えないよう配慮したうえで実施すること。
バックアップ	• 設定変更及びバージョンアップ時には、設定ファイルのバックアップを取得すること。 • バックアップ保存期間は、5 世代又は 1 年のうち、保存期間の長いものを適用すること。
保守受付	• 本機関からの各種依頼に対して、電話、メールによる受付窓口を準備し、依頼事項に対する支援を実施すること。 • 本システムの動作仕様や技術的な質問に対して、電話及びメールにて回答を行うこと。 • 専任の担当者を設置し、本機関の環境を踏まえた回答やサポートを行うことが望ましい。なお、専任担当者は、本機関の専属である必要はなく、本機関の環境を理解した応対ができればよい。
保守情報通知	• ソフトウェア/ファームウェアのリリースや、当社にて使用中のソフトウェア/ファームウェアに脆弱性が発見された際、電話又はメールにて通知を行うこと。緊急性の高いものは即時情報を提供すること。 • メーカーサポート終了（EOL）が発表された場合、速やかに本機関へ通知すること。 • インターネット回線に保守作業による断時間が発生する場合、その内容を速やかに本機関に通知すること。

月次報告	• 稼働状況及び本機関からの各種依頼への対応状況を月次で報告すること。また、各機器の脆弱性やソフトウェア不具合情報を提供し、バージョンアップの要否について報告すること。
年次報告	• 稼働状況及び本機関からの各種依頼への対応状況を年次で報告すること。 • メーカーサポート終了（EOL）が発表された一覧を作成し、年次で報告すること。（本機関への通知日等も含めること。）
その他	• 本機関では情報システムのセキュリティ検査及びシステム監査を毎年実施していることから、受託者は本機関からの求めに応じ、問合せへの対応や必要な資料を提供すること。 • 対応言語は日本語とすること。

② 業務提供時間

受託者は保守契約の期間において、次の時間帯で保守業務を提供すること。

項目	内容
稼働監視	• 24 時間 365 日
障害対応	• 24 時間 365 日
運用支援	• 平日 9:00-18:00 • 平日 夜間、又は、休日（都度、本機関と調整すること）
バックアップ	• 平日 9:00-18:00 • 平日 夜間、又は、休日（都度、本機関と調整すること）
保守受付	• 受付：24 時間 365 日 • 回答：平日 9:00-18:00
保守情報通知	• 平日 9:00-18:00
月次報告	• 平日 9:00-18:00（毎月 10 営業日以内に報告すること）

③ 業務提供場所

本調達に係る保守作業は、原則として受託者の事業所とするが、予め本機関にその業務場所について開示すること。

項目	内容
作業場所	• 保守業務は、受託者の事業所内での実施を許可するが、事前に作業内容と作業場所について本機関に案内すること。 • 保守業務に関する打合せ、報告会議等については、本機関及び受託者が協議の上決定すること。

④ 業務管理

受託者は、次に示す管理業務を、本業務の全工程に渡り実施すること。

項目	内容
情報セキュリティ管理	• 各作業工程において、セキュリティに関する事故及び障害等の発生を未然に防ぐこと、並びに発生した場合に被害を最小限に抑えること。
課題管理	• 業務遂行上様々な局面で発生する各課題について、課題の認識、対応案の検討、解決までの追跡等の課題管理を行うこと。

品質管理	• 品質評価計画の立案、検証及び品質改善策の検討、実施を管理する体制の構築等の品質管理を行うこと。
人的資源管理	• 本調達に参画する要員の選定、変更及び体制維持に関する管理を行うこと。 • 主たる要員に変更が生じた場合には、本機関へ報告すること。また、代替要員については、サービスレベルの低下を防ぐために、知識及び経験が妥当な者を選定すること。
構成・変更管理	• 構成管理対象（設計書等）を特定し、管理レベル（参照・更新権限、保存方法・期間等）を定めること。

5. 外部サービスに関する要件

(1) 機能要件

外部サービスに求める要件を次に記載する。

項目	内容
外部 DNS 機能	・レコードの登録・修正等の作業は、サービス提供元で実施すること。 ・登録・修正等は、サービス利用料金内で行うこと。 ・24 時間 365 日の無停止の運用サービスであること。
NTP 機能	・各機器への時刻同期を行うこと。 ・外部接続しているシステム（広域機関システム等）についても時刻同期を行えるようにすること。なお、Active Directory 側に NTP 機能を実装し、外部接続システム側と時刻同期を行う方式としても問題ないもとする。 ・24 時間 365 日の無停止の運用サービスであること。
その他	・外部サービスへの切替に伴い、通常業務に影響がないようにすること。 ・本機関では情報システムのセキュリティ検査及びシステム監査を毎年実施していることから、受託者は本機関からの求めに応じ、問合せへの対応や必要な資料を提供すること。 ・本機関とのサービス契約終了時（途中解約等も含む）には、インシデント履歴やログデータ等の全ての情報を削除すること。

以上

別紙２

非機能要求グレード

電力広域的運営推進機関

２０２６年１月

非機能要求グレード															
項番	大項目	中項目	中項目	小項目説明	重複	重要	メトリクス（指標）	レベル						ネットワーク他	
								0	1	2	3	4	5	選択レベル	
	可用性	継続性	運用スケジュール	システムの稼働時間や停止運用に関する情報。	○	○		規定無し	定時内（9 時～17 時）	夜間のみ停止（9 時～21 時）	1 時間程度の停止有り（9 時～翌朝 8 時）	若干の停止有り（9 時～翌朝 8 時 55 分）	24 時間無停止	5	24 時間無停止
A.1.1.2					○	○	運用時間（特定日）	規定無し	定時内（9 時～17 時）	夜間のみ停止（9 時～21 時）	1 時間程度の停止有り（9 時～翌朝 8 時）	若干の停止有り（9 時～翌朝 8 時 55 分）	24 時間無停止	5	24 時間無停止
A.1.1.3					○	○	計画停止の有無	計画停止有り（運用スケジュールの変更可）	計画停止有り（運用スケジュールの変更不可）	計画停止無し				2	計画停止無し
A.1.2.1			業務継続性	可用性を保証するにあたり、要求される業務の範囲とその条件。		○	対象業務範囲	内部向けバッチ系業務	内部向けオンライン系業務	内部向け全業務	外部向けバッチ系業務	外部向けオンライン系業務	全ての業務	4	外部向けオンライン系業務
A.1.2.2						○	サービス切替時間	24 時間以上	24 時間未満	2 時間未満	60 分未満	10 分未満	60 秒未満	4	10 分未満
A.1.2.3						○	業務継続の要求度	障害時の業務停止を許容する	単一障害時は業務停止を許容せず、処理を継続させる	二重障害時でもサービス切替時間の規定内で継続する				2	二重障害時でもサービス切替時間の規定内で継続する
A.1.3.1			目標復旧水準（業務停止時）	業務停止を伴う障害が発生した際、何をどこまで、どれ位で復旧させるかの目標。		○	RPO（目標復旧地点）	復旧不要	5 営業日前の時点（週次バックアップからの復旧）	1 営業日前の時点（日次バックアップからの復旧）	障害発生時点（日次バックアップ+アーカイブからの復旧）			3	障害発生時点（日次バックアップ+アーカイブからの復旧）
A.1.3.2						○	RTO（目標復旧時間）	1 営業日以上	1 営業日以内	12 時間以内	6 時間以内	2 時間以内		4	2 時間以内
A.1.3.3						○	RLO（目標復旧レベル）	システムの復旧	特定業務のみ	全ての業務				2	全ての業務
A.1.4.1			目標復旧水準	大規模災害が発生した際、どれ位で復旧させるかの目標。 大規模災害とは、火災や地震などの異常な自然現象、あるいは人為的な原因による大きな事故、破壊行為により生ずる被害のことを指し、システムに甚大な被害が発生するか、電力などのライフラインの停止により、システム		○	システム再開目標	再開不要	数ヶ月以内に再開	一ヶ月以内に再開	一週間以内に再開	3 日以内に再開	1 日以内に再開	5	1 日以内に再開

				をそのまま現状に修復するのが困難な状態となる災害をいう。											
A.1.5.1			稼働率	明示された利用条件の下で、システムが要求されたサービスを提供できる割合。 明示された利用条件とは、運用スケジュールや、目標復旧水準により定義された業務が稼働している条件を指す。その稼働時間の中で、サービス中断が発生した時間により稼働率を求める。		○	稼働率	95%以下	95%	99%	99.9%	99.99%	99.999%	4	99.99%
A.2.1.1		耐障害性	サーバ	サーバで発生する障害に対して、要求されたサービスを維持するための要求。			冗長化（機器）	非冗長構成	特定のサーバで冗長化	全てのサーバで冗長化	–			1	特定のサーバで冗長化
A.2.1.2							冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化				1	特定のコンポーネントのみ冗長化
A.2.2.1			端末	端末で発生する障害に対して、要求されたサービスを維持するための要求。			冗長化（機器）	非冗長構成	共用の予備端末を設置	業務や用途毎に予備端末を設置				1	共用の予備端末を設置
A.2.2.2							冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化				0	非冗長構成
A.2.3.1			ネットワーク機器	ルータやスイッチなどネットワークを構成する機器で発生する障害に対して、要求されたサービスを維持するための要求。			冗長化（機器）	非冗長構成	特定の機器のみ冗長化	全ての機器を冗長化				1	特定の機器のみ冗長化
A.2.3.2							冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化				1	特定のコンポーネントのみ冗長化
A.2.4.1			ネットワーク	ネットワークの信頼性を向上させるための要求。			回線の冗長化	冗長化しない	一部冗長化	全て冗長化する				1	一部冗長化
A.2.4.2							経路の冗長化	冗長化しない	一部冗長化	全て冗長化する				1	一部冗長化
A.2.4.3							セグメント分割	分割しない	サブシステム単位で分割	用途に応じて分割				2	用途に応じて分割

A.2.5.1			ストレージ	ディスクアレイなどの外部記憶装置で発生する障害に対して、要求されたサービスを維持するための要求。			冗長化（機器）	非冗長構成	特定の機器のみ冗長化	全ての機器を冗長化				1	特定の機器のみ冗長化
A.2.5.2							冗長化（コンポーネント）	非冗長構成	特定のコンポーネントのみ冗長化	全てのコンポーネントを冗長化				1	特定のコンポーネントのみ冗長化
A.2.5.3							冗長化（ディスク）	非冗長構成	単一冗長	多重冗長				1	単一冗長
A.2.6.1			データ	データの保護に対しての考え方。	○		バックアップ方式	バックアップ無し	オフラインバックアップ	オンラインバックアップ	オフラインバックアップ+オンラインバックアップ			3	オフラインバックアップ+オンラインバックアップ
A.2.6.2					○		データ復旧範囲	復旧不要	一部の必要なデータのみ復旧	システム内の全データを復旧				2	システム内の全データを復旧
A.2.6.3							データインテグリティ	エラー検出無し	エラー検出のみ	エラー検出＆再試行	データの完全性を保障（エラー検出＆訂正）			2	エラー検出＆再試行
A.3.1.1		災害対策	システム	地震、水害、テロ、火災などの大規模災害時の業務継続性を満たすための要求。			復旧方針	復旧しない	限定された構成でシステムを再構築	同一の構成でシステムを再構築	限定された構成を DR サイトで構築	同一の構成を DR サイトで構築		4	同一の構成を DR サイトで構築
A.3.2.1			外部保管データ	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ･プログラムを運用サイトと別の場所へ保管するなどの要求。			保管場所分散度	外部保管しない	1 ヵ所	1 ヵ所（遠隔地）	2 ヵ所（遠隔地）			2	1 ヵ所（遠隔地）
A.3.2.2							保管方法	媒体による保管	同一サイト内の別ストレージへのバックアップ	DR サイトへのリモートバックアップ				2	DR サイトへのリモートバックアップ
A.3.3.1			付帯設備	各種災害に対するシステムの付帯設備での要求。			災害対策範囲	対策を実施しない	特定の対策を実施する	想定する全ての対策を実施する				1	特定の対策を実施する
A.4.1.1		回復性	復旧作業	業務停止を伴う障害が発生した際の復旧作業に必要な労力。	○		復旧作業	復旧不要	復旧用製品は使用しない手作業の復旧	復旧用製品による復旧	復旧用製品＋業務アプリケーションによる復旧			2	復旧用製品による復旧
A.4.1.2					○		代替業務運用の範囲	無し	一部の業務について代替業務運用が必要	全部の業務について代替業務運用が必要				1	一部の業務について代替業務運用が必要
A.4.2.1			可用性確認	可用性として要求された項目をどこまで確認するかの範囲。	–	○	確認範囲	実施しない。または単純な障害の範囲	業務を継続できる障害の範囲	業務停止となる障害のうち一部の範囲	業務停止となる障害の全ての範囲	–	–	2	業務停止となる障害のうち一部の範囲

B.1.1.1	性能・拡張性	業務処理量	通常時の業務量	性能・拡張性に影響を与える業務量。該当システムの稼働時を想定し、合意する。それぞれのメトリクスに於いて、単一の値だけでなく、前提となる時間帯や季節の特性なども考慮する。	○	○	ユーザ数	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用	—			1	上限が決まっている
B.1.1.2						○	同時アクセス数	特定利用者の限られたアクセスのみ	同時アクセスの上限が決まっている	不特定多数のアクセス有り	—			2	不特定多数のアクセス有り
B.1.1.3						○	データ量	全てのデータ量が明確である	主要なデータ量のみが明確である	—				1	主要なデータ量のみが明確である
B.1.1.4						○	オンラインリクエスト件数	処理毎にリクエスト件数が明確である	主な処理のリクエスト件数のみが明確である	—	—			1	主な処理のリクエスト件数のみが明確である
B.1.1.5						○	バッチ処理件数	処理単位毎に処理件数が決まっている	主な処理の処理件数が決まっている	—	—			1	主な処理の処理件数が決まっている
B.1.1.6							業務機能数	業務機能が整理されている	確定した業務機能一覧が作成されている	業務機能一覧はあるが、確定していない	—			0	業務機能が整理されている
B.1.2.1			業務量増大度	システム稼動開始からライフサイクル終了までの間で、開始時点と業務量が最大になる時点の業務量の倍率。 必要に応じ、開始日の平均値や、開始後の定常状態との比較を行う場合もある。		○	ユーザ数増大率	1 倍	1.2 倍	1.5 倍	2 倍	3 倍	10 倍以上	1	1.5 倍
B.1.2.2						○	同時アクセス数増大率	1 倍	1.2 倍	1.5 倍	2 倍	3 倍	10 倍以上	1	1.5 倍
B.1.2.3						○	データ量増大率	1 倍	1.2 倍	1.5 倍	2 倍	3 倍	10 倍以上	1	1.2 倍
B.1.2.4						○	オンラインリクエスト件数増大率	1 倍	1.2 倍	1.5 倍	2 倍	3 倍	10 倍以上	1	1.2 倍
B.1.2.5						○	バッチ処理件数増大率	1 倍	1.2 倍	1.5 倍	2 倍	3 倍	10 倍以上	1	1.2 倍
B.1.2.6							業務機能数増大率	1 倍	1.2 倍	1.5 倍	2 倍	3 倍	10 倍以上	1	1.2 倍
B.1.3.1			保管期間	システムが参照するデータのうち、OS やミドルウェアのログなどのシステム基盤が利用する		○	保管期間	6 ヶ月	1 年	3 年	5 年	10 年以上有期	永久保管	3	5 年

B.1.3.2				データに対する保管が必要な期間。 必要に応じて、データの種別毎に定める。 保管対象のデータを選択する際には、対象範囲についても決めておく。			対象範囲	オンラインで参照できる範囲	アーカイブまで含める					
B.2.1.1		性能目標値	オンラインレスポンス	オンラインシステム利用時に要求されるレスポンス。 システム化する対象業務の特性をふまえ、どの程度のレスポンスが必要かについて確認する。ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に順守率を決める。具体的な数値は特定の機能またはシステム分類毎に決めておくことが望ましい。(例:Web システムの参照系/更新系/一覧系など)	–	○	通常時レスポンス順守率	順守率を定めない	60%	80%	90%	95%	99%以上	3	90%
B.2.1.2						○	ピーク時レスポンス順守率	順守率を定めない	60%	80%	90%	95%	99%以上	2	80%
B.2.1.3							縮退時レスポンス順守率	縮退をしない	60%	80%	90%	95%	99%以上		
B.2.2.1			バッチレスポンス(ターンアラウンドタイム)	バッチシステム利用時に要求されるレスポンス。 システム化する対象業務の特性をふまえ、どの程度のレスポンス(ターンアラウンドタイム)が必要かについて確認する。更に、ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に順守率を決める、具体的な数値は特定の機能またはシステム分類毎に決めておくことが望ましい。 (例:日次処理/月次処理/年次処理など)	–	○	通常時レスポンス順守度合い	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				2	再実行の余裕が確保できる
B.2.2.2						○	ピーク時レスポンス順守度合い	順守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				2	再実行の余裕が確保できる
B.2.2.3							縮退時レスポンス順守度合い	縮退をしない	所定の時間内に収まる	再実行の余裕が確保できる					
B.2.3.1			オンラインスループット	オンラインシステム利用時に要求されるスループット。システム化する対象業務の特性をふまえ、単位時間にどれだけの量の作業ができるかを確認する。更に、ピーク特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時毎に処理余裕率を決める、具体的な数値は特定の機能またはシステム分類毎に決めておくことが望ましい。(例:データエントリ件数/時間、頁めくり回数/分、TPS など)			通常時処理余裕率	1 倍(余裕無し)	1.2 倍	1.5 倍	2 倍	3 倍	10 倍以上		
B.2.3.2							ピーク時処理余裕率	1 倍(余裕無し)	1.2 倍	1.5 倍	2 倍	3 倍	10 倍以上		
B.2.3.3							縮退時処理余裕率	縮退をしない	通常時の 1/2 の処理が出来る	通常時と同様に処理が出来る					

B.2.4.1			バッチスループット	バッチシステム利用時に要求されるスループット。 システム化する対象業務の特性をふまえ、どの程度のスループットを確保すべきか確認する。更に、ピーク特性や、障害時の運用を考慮し、通常時･ピーク時･縮退運転時毎に処理余裕率を決める。具体的な数値は特定の機能またはシステム分類毎に決めておくことが望ましい。 （例：人事異動情報一括更新処理、一括メール送信処理など）	－	－	通常時処理余裕率	1 倍(余裕無し)	1.2 倍	1.5 倍	2 倍	3 倍	10 倍以上		
B.2.4.2							ピーク時処理余裕率	1 倍(余裕無し)	1.2 倍	1.5 倍	2 倍	3 倍	10 倍以上		
B.2.4.3							縮退時処理余裕率	縮退をしない	通常時の 1/2 の処理が出来る	通常時と同様に処理が出来る					
B.2.5.1			帳票印刷能力	帳票印刷に要求されるスループット。 業務で必要な帳票の出力時期や枚数を考慮し、どの程度のスループットが必要かを確認する。 更に、ピーク特性や、障害時の運用を考慮し、通常時･ピーク時･縮退運転時毎に余裕率を決める。具体的な数値は特定の帳票や機能毎に決めておくことが望ましい。			通常時印刷余裕率	1 倍(余裕無し)	1.2 倍	1.5 倍	2 倍	3 倍	10 倍以上		
B.2.5.2							ピーク時印刷余裕率	1 倍(余裕無し)	1.2 倍	1.5 倍	2 倍	3 倍	10 倍以上		
B.2.5.3							縮退時印刷余裕率	縮退をしない	通常時の 1/2 の印刷が出来る	通常時と同様に印刷が出来る					
B.3.1.1		リソース拡張性	CPU 拡張性	CPU の拡張性を確認するための項目。 CPU 利用率は、将来の業務量の増加に備え、どれだけ CPU に余裕をもたせておくかを確認するための項目。 CPU 拡張性は、物理的もしくは仮想的に、どれだけ CPU を拡張できるようにしておくかを確認するための項目。 CPU の専有の有無については「B.4.1 HW リソース専有の有無」で確認する。		○	CPU 利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			1	50%以上 80%未満
B.3.1.2						○	CPU 拡張性	1 倍(拡張要求なし)	1.5 倍の拡張が可能	2 倍の拡張が可能	4 倍の拡張が可能	8 倍以上の拡張が可能		1	1.5 倍の拡張が可能
B.3.2.1			メモリ拡張性	メモリの拡張性を確認するための項目。 メモリ利用率は、将来の業務量の増加に備え、どれだけメモリに余裕をもたせておくかを確認するための項目。 メモリ拡張性は、物理的もしくは仮想的に、どれだけメモリを拡張できるようにしておくかを確認するための項目。 メモリの専有の有無については「B.4.1 HW リソース専有の有無」で確認する。		○	メモリ利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満			1	50%以上 80%未満
B.3.2.2						○	メモリ拡張性	1 倍(拡張要求なし)	1.5 倍の拡張が可能	2 倍の拡張が可能	4 倍の拡張が可能	8 倍以上の拡張が可能		1	1.5 倍の拡張が可能

B.3.3.1			ディスク拡張性	ディスクの拡張性を確認するための項目。 ディスク利用率は、将来の業務量の増加に備え、どれだけディスクに余裕をもたせておくかを確認するための項目。 ディスク拡張性は、物理的もしくは仮想的に、どれだけディスクを拡張できるようにしておくかを確認するための項目。			ディスク利用率	80%以上	50%以上 80%未満	20%以上 50%未満	20%未満				
B.3.3.2						ディスク拡張性	1 倍(拡張要求なし)	1.5 倍の拡張が可能	2 倍の拡張が可能	4 倍の拡張が可能	8 倍以上の拡張が可能			
B.3.4.1			ネットワーク	システムで使用するネットワーク環境の拡張性に関する項目。 既存のネットワーク機器を活用する場合は既存ネットワークの要件を確認するために利用する。 ネットワークの帯域については「B.4.1 帯域保証機能の有無」で確認する。			ネットワーク機器設置範囲	無し	フロア内の LAN	同一拠点(ビル)内の LAN	社内複数拠点間の接続(LAN、WAN)	社外拠点との接続			
B.3.5.1			サーバ処理能力増強	サーバ処理能力増強方法に関する項目。 将来の業務量増大に備える方法(スケールアップ/スケールアウト)をあらかじめ考慮しておくこと。どちらの方法を選択するかはシステムの特徴によって使い分けることが必要。 スケールアップは、より処理能力の大きなサーバとの入れ替えを行うことで処理能力の増強を行う。 スケールアウトは同等のサーバを複数台用意し、サーバ台数を増やすことで処理能力の増強を行う。			スケールアップ	スケールアップを行わない	一部のサーバのみを対象	複数のサーバを対象					
B.3.5.2						スケールアウト	スケールアウトを行わない	一部のサーバのみを対象	複数のサーバを対象					
B.4.1.1		性能品質保証	帯域保証機能の有無	ネットワークのサービス品質を保証する機能の導入要否およびその程度。 伝送遅延時間、パケット損失率、帯域幅をなんらかの仕組みで決めているかを示す。回線の帯域が保証されていない場合性能悪化につながることがある。			帯域保証の設定	無し	プロトコル単位で設定	各サーバ毎に設定	アプリケーションのエンドツーエンドで検証・保証			
B.4.1.2			HW リソース専有の有無	サーバのリソース(CPU やメモリ)を専有するか、共有するかを示す。HW リソースを他のサーバと共有する場合、他のサーバの影響を受けて、性能悪化につながることがある。			HW リソース専有の設定	無し(共有)	有り(専有)					

B.4.2.1			性能テスト	構築したシステムが当初/ライフサイクルに渡っての性能を発揮できるかのテストの測定頻度と範囲。			測定頻度	測定しない	構築当初に測定	運用中、必要時に測定可能	運用中、定常的に測定				
B.4.2.2							確認範囲	確認しない	一部の機能について、目標値を満たしていることを確認	全ての機能について、目標値を満たしていることを確認					
B.4.3.1			スパイク負荷対応	通常時の負荷と比較して、非常に大きな負荷が短時間に現れることを指す。業務量の想定されたピークを超えた状態。 特に B2C システムなどクライアント数を制限できないシステムで発生する。システムの処理上限を超えることが多いため、Sorry 動作を実装し対策する場合が多い。			トランザクション保護	トランザクション保護は不要である	同時トランザクション数の制限機能	同時トランザクション数の制限機能に加え、Sorry 動作	独立した Sorry 動作を行うサーバの設置				
C.1.1.1	運用・保守性	通常運用	運用時間	システム運用を行う時間。利用者やシステム管理者に対してサービスを提供するために、システムを稼動させ、オンライン処理やバッチ処理を実行している時間帯のこと。	○	○	運用時間（通常）	規定無し	定時内（9 時～17 時）	夜間のみ停止（9 時～21 時）	1 時間程度の停止有り（9 時～翌朝 8 時）	若干の停止有り（9 時～翌朝 8 時 55 分）	24 時間無停止	5	24 時間無停止
C.1.1.2					○	○	運用時間（特定日）	規定無し	定時内（9 時～17 時）	夜間のみ停止（9 時～21 時）	1 時間程度の停止有り（9 時～翌朝 8 時）	若干の停止有り（9 時～翌朝 8 時 55 分）	24 時間無停止	5	24 時間無停止
C.1.2.1			バックアップ	システムが利用するデータのバックアップに関する項目。	○		データ復旧範囲	復旧不要	一部の必要なデータのみ復旧	システム内の全データを復旧					
C.1.2.2						○	外部データの利用可否	全データの復旧に利用できる	一部のデータ復旧に利用できる	外部データは利用できない				2	外部データは利用できない
C.1.2.3						○	バックアップ利用範囲	バックアップを取得しない	障害発生時のデータ損失防止	ユーザエラーからの回復	データの長期保存（アーカイブ）			3	データの長期保存（アーカイブ）
C.1.2.4						○	バックアップ自動化の範囲	全ステップを手動で行う	一部のステップを手動で行う	全ステップを自動で行う				2	全ステップを自動で行う
C.1.2.5						○	バックアップ取得間隔	バックアップを取得しない	システム構成の変更時など、任意のタイミング	月次で取得	週次で取得	日次で取得	同期バックアップ	5	同期バックアップ
C.1.2.6						○	バックアップ保存期間	バックアップを保存しない	1 年未満	3 年	5 年	10 年以上有限	永久保存	3	5 年

C.1.2.7					○		バックアップ方式	バックアップ無し	オフラインバックアップ	オンラインバックアップ	オフラインバックアップ+オンラインバックアップ			
C.1.3.1			運用監視	システム全体、あるいはそれを構成するハードウェア・ソフトウェア(業務アプリケーションを含む)に対する監視に関する項目。 セキュリティ監視については本項目には含めない。「E.7.1 不正監視」で別途検討すること。		○	監視情報	監視を行わない	死活監視を行う	エラー監視を行う	エラー監視(トレース情報を含む)を行う	リソース監視を行う	パフォーマンス監視を行う	4	リソース監視を行う
C.1.3.2						○	監視間隔	監視を行わない	不定期監視(手動監視)	定期監視(1 日間隔)	定期監視(数時間間隔)	リアルタイム監視(分間隔)	リアルタイム監視(秒間隔)	5	リアルタイム監視(秒間隔)
C.1.3.3							システムレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					
C.1.3.4							プロセスレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					
C.1.3.5							データベースレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					
C.1.3.6							ストレージレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					
C.1.3.7							サーバ(ノード)レベルの監視	監視を行わない	一部監視を行う	全て監視を行う					
C.1.3.8							端末/ネットワーク機器レベルの監視	監視を行わない	一部監視を行う	全て監視を行う					
C.1.3.9							ネットワーク・パケットレベルの監視	監視を行わない	一部監視を行う	全て監視を行う					
C.1.4.1			時刻同期	システムを構成する機器の時刻同期に関する項目。			時刻同期設定の範囲	時刻同期を行わない	サーバ機器のみ時刻同期を行う	サーバおよびクライアント機器について時刻同期を行う	ネットワーク機器も含めシステム全体で時刻同期を行う	システム全体を外部の標準時間と同期する			
C.2.1.1		保守運用	計画停止	点検作業や領域拡張、デフラグ、マスターデータのメンテナンス等、システムの保守作業の実施を目的とした、事前計画済みのサ	○	○	計画停止の有無	計画停止有り(運用スケジュールの変更可)	計画停止有り(運用スケジュールの変更不可)	計画停止無し				2	計画停止無し

C.2.1.2				ービス停止に関する項目。			計画停止の事前アナウンス	計画停止が存在しない	計画停止は年間計画によって確定する	1ヶ月前に通知	1週間前に通知	前日に通知			
C.2.2.1			運用負荷削減	保守運用に関する作業負荷を削減するための設計に関する項目。		○	保守作業自動化の範囲	保守作業は全て手動で実施する	一部の保守作業を自動で実行する	全ての保守作業を自動で実行する				1	一部の保守作業を自動で実行する
C.2.2.2						–	サーバソフトウェア更新作業の自動化	サーバへの更新ファイル配布機能を実装しない	サーバへの更新ファイル配布機能を実装し、手動にて配布と更新処理を実行する	サーバへの更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する	サーバへの更新ファイル配布機能を実装し、配布と更新処理を自動で実行する			–	–
C.2.2.3						–	端末ソフトウェア更新作業の自動化	端末への更新ファイル配布機能を実装しない	端末への更新ファイル配布機能を実装し、手動にて配布と更新処理を実行する	端末への更新ファイル配布機能を実装し、自動で配布したのち、更新処理を手動で実行する	端末への更新ファイル配布機能を実装し、配布と更新処理を自動で実行する			–	–
C.2.3.1			パッチ適用ポリシー	パッチ情報の展開とパッチ適用のポリシーに関する項目。			パッチリリース情報の提供	ユーザの要求に応じてベンダが受動的にパッチリリース情報を提供する	ベンダが定期的にユーザへパッチリリース情報を提供する	ベンダがリアルタイムに(パッチリリースと同時に)ユーザへパッチリリース情報を提供する					
C.2.3.2							パッチ適用方針	パッチを適用しない	推奨されるパッチのみを適用する	全てのパッチを適用する					
C.2.3.3							パッチ適用タイミング	パッチを適用しない	障害発生時にパッチ適用を行う	定期保守時にパッチ適用を行う	新規のパッチがリリースされるたびに適用を行う	–			
C.2.3.4							パッチ検証の実施有無	パッチ検証を実施しない	障害パッチのみパッチ検証を実施する	障害パッチとセキュリティパッチの両方でパッチ検証を実施する					
C.2.4.1			活性保守	サービス停止の必要がない活性保守が可能なコンポーネントの範囲。			ハードウェア活性保守の範囲	活性保守を行わない	一部のハードウェアにおいて活性保守を行う	全てのハードウェアにおいて活性保守を行う					
C.2.4.2							ソフトウェア活性保守の範囲	活性保守を行わない	一部のソフトウェアにおいて活性保守を行う	全てのソフトウェアにおいて活性保守を行う					

C.2.5.1			定期保守頻度	システムの保全のために必要なハードウェアまたはソフトウェアの定期保守作業の頻度。			定期保守頻度	定期保守を実施しない	年１回	半年に１回	月１回	週１回	毎日		
C.2.6.1			予防保守レベル	システム構成部材が故障に至る前に予兆を検出し、事前交換などの対応をとる保守。			予防保守レベル	予防保守を実施しない	定期保守時に検出した予兆の範囲で対応する	（定期保守とは別に）一定間隔で予兆検出を行い、対応を行う	リアルタイムに予兆検出を行い、対応を行う				
C.3.1.1		障害時運用	復旧作業	業務停止を伴う障害が発生した際の復旧作業に必要な労力。	○		復旧作業	復旧不要	復旧用製品は使用しない手作業の復旧	復旧用製品による復旧	復旧用製品＋業務アプリケーションによる復旧				
C.3.1.2					○		代替業務運用の範囲	無し	一部の業務について代替業務運用が必要	全部の業務について代替業務運用が必要					
C.3.2.1			障害復旧自動化の範囲	障害復旧に関するオペレーションを自動化する範囲に関する項目。			障害復旧自動化の範囲	障害復旧作業は全て手動で実施する	一部の障害復旧作業を自動化する	全ての障害復旧作業を自動化する				－	－
C.3.3.1			システム異常検知時の対応	システムの異常を検知した際のベンダ側対応についての項目。			対応可能時間	ベンダの営業時間内（例：9時～17時）で対応を行う	ユーザの指定する時間帯（例：18時～24時）で対応を行う	24 時間対応を行う					
C.3.3.2							駆けつけ到着時間	保守員の駆けつけ無し	保守員到着が異常検知から数日中	保守員到着が異常検知からユーザの翌営業日中	保守員到着が異常検知からユーザの翌営業開始時まで	保守員到着が異常検知から数時間内	保守員が常駐		
C.3.3.3							SE 到着平均時間	SE の駆けつけ無し	SE 到着が異常検知から数日中	SE 到着が異常検知からユーザの翌営業日中	SE 到着が異常検知からユーザの翌営業開始時まで	SE 到着が異常検知から数時間内	SE が常駐		
C.3.4.1			交換用部材の確保	障害の発生したコンポーネントに対する交換部材の確保方法。			保守部品確保レベル	確保しない	保守契約に基づき、部品を提供するベンダが規定年数の間保守部品を確保する	保守契約に基づき、保守を提供するベンダが当該システム専用として規定年数の間保守部品を確保する					
C.3.4.2							予備機の有無	予備機無し	一部、予備機有り	全部、予備機有り					

C.4.1.1		運用環境	開発用環境の設置	ユーザがシステムに対する開発作業を実施する目的で導入する環境についての項目。		○	開発用環境の設置有無	システムの開発環境を設置しない	運用環境の一部に限定した開発環境を設置する	運用環境と同一の開発環境を設置する				1	運用環境の一部に限定した開発環境を設置する
C.4.2.1			試験用環境の設置	ユーザがシステムの動作を試験する目的で導入する環境についての項目。		○	試験用環境の設置有無	システムの試験環境を設置しない	システムの開発用環境と併用する	専用の試験用環境を設置する				1	システムの開発用環境と併用する
C.4.3.1			マニュアル準備レベル	運用のためのマニュアルの準備のレベル。		○	マニュアル準備レベル	各製品標準のマニュアルを利用する	システムの通常運用のマニュアルを提供する	システムの通常運用と保守運用のマニュアルを提供する	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供する			3	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供する
C.4.4.1			リモートオペレーション	システムの設置環境とは離れた環境からのネットワークを介した監視や操作の可否を定義する項目。		○	リモート監視地点	リモート監視を行わない	構内 LAN を介してリモート監視を行う	遠隔地でリモート監視を行う	—			2	遠隔地でリモート監視を行う
C.4.4.2						○	リモート操作の範囲	リモート操作を行わない	定型処理のみリモート操作を行う	任意のリモート操作を行う				2	任意のリモート操作を行う
C.4.5.1			外部システム接続	システムの運用に影響する外部システムとの接続の有無に関する項目。		○	外部システムとの接続有無	外部システムと接続しない	社内の外部システムと接続する	社外の外部システムと接続する				2	社外の外部システムと接続する
C.4.5.2							監視システムの有無	監視システムは存在しない	既存監視システムに接続する	新規監視システムに接続する					
C.4.5.3							ジョブ管理システムの有無	ジョブ管理システムは存在しない	既存ジョブ管理システムに接続する	新規ジョブ管理システムに接続する					
C.5.1.1		サポート体制	保守契約(ハードウェア)	保守が必要な対象ハードウェアの範囲。		○	保守契約(ハードウェア)の範囲	保守契約を行わない	ベンダの自社製品(ハードウェア)に対してのみ保守契約を行う	マルチベンダのサポート契約を行う(一部対象外を許容)	マルチベンダのサポート契約を行う(システムを構成する全製品を対象)			3	マルチベンダのサポート契約を行う(システムを構成する全製品を対象)
C.5.2.1			保守契約(ソフトウェア)	保守が必要な対象ソフトウェアの範囲。		○	保守契約(ソフトウェア)の範囲	保守契約を行わない	ベンダの自社製品(ソフトウェア)に対してのみ保守契約を行う	マルチベンダのサポート契約を行う(一部対象外を許容)	マルチベンダのサポート契約を行う(システムを構成する全製品を対象)			2	マルチベンダのサポート契約を行う(一部対象外を許容)

C.5.3.1			ライフサイクル期間	運用保守の対応期間および、実際にシステムが稼動するライフサイクルの期間。		○	ライフサイクル期間	3 年	5 年	7 年	10 年以上			1	5 年
C.5.4.1			メンテナンス作業役割分担	メンテナンス作業に対するユーザ/ベンダの役割分担、配置人数に関する項目。			メンテナンス作業役割分担	全てユーザが実施	一部ユーザが実施	全てベンダが実施					
C.5.5.1			一次対応役割分担	一次対応のユーザ/ベンダの役割分担、一次対応の対応時間、配備人数。			一次対応役割分担	全てユーザが実施	一部ユーザが実施	全てベンダが実施					
C.5.6.1			サポート要員	サポート体制に組み入れる要員の人数や対応時間、スキルレベルに関する項目。			ベンダ側常備配備人数	常駐しない	1 人	複数人					
C.5.6.2							ベンダ側対応時間帯	対応無し	ベンダの定時時間内(9～17 時)	夜間のみ非対応(9～21 時)	引継ぎ時に 1 時間程度非対応有り(9～翌 8 時)	24 時間対応			
C.5.6.3							ベンダ側対応者の要求スキルレベル	指定無し	有識者の指導を受けて機器の操作を実施できる	システムの構成を把握し、ログの収集・確認が実施できる	システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できる	システムの開発や構築に携わり、業務要件やユーザの事情にも通じている			
C.5.6.4							エスカレーション対応	指定無し	オンコール待機	拠点待機	現地待機				
C.5.7.1			導入サポート	システム導入時の特別対応期間の有無および期間。			システムテスト稼働時の導入サポート期間	無し	当日のみ	1 週間以内	1 ヶ月以内	1 ヶ月以上			
C.5.7.2							システム本稼働時の導入サポート期間	無し	当日のみ	1 週間以内	1 ヶ月以内	1 ヶ月以上			

C.5.8.1			オペレーション訓練	オペレーション訓練実施に関する項目。			オペレーション訓練実施の役割分担	実施しない	全てユーザが実施	一部ユーザが実施	全てベンダが実施			
C.5.8.2							オペレーション訓練範囲	実施しない	通常運用の訓練を実施	通常運用に加えて保守運用の訓練を実施	通常運用、保守運用に加えて、障害発生時の復旧作業に関する訓練を実施			
C.5.8.3							オペレーション訓練実施頻度	実施しない	システム立ち上げ時のみ	定期開催				
C.5.9.1			定期報告会	保守に関する定期報告会の開催の要否。			定期報告会実施頻度	無し	年 1 回	半年に 1 回	四半期に 1 回	月 1 回	週 1 回以上	
C.5.9.2							報告内容のレベル	無し	障害報告のみ	障害報告に加えて運用状況報告を行う	障害および運用状況報告に加えて、改善提案を行う			
C.6.1.1		その他の運用管理方針	内部統制対応	IT 運用プロセスの内部統制対応を行うかどうかに関する項目。		○	内部統制対応の実施有無	内部統制対応について規定しない	既存の社内規定に従って、内部統制対応を実施する	新規に規定を制定し、内部統制対応を実施する				1	既存の社内規定に従って、内部統制対応を実施する
C.6.2.1			サービスデスク	ユーザの問合せに対して単一の窓口機能を提供するかどうかに関する項目。		○	サービスデスクの設置有無	サービスデスクの設置について規定しない	既存のサービスデスクを利用する	新規にサービスデスクを設置する				1	既存のサービスデスクを利用する
C.6.3.1			インシデント管理	業務を停止させるインシデントを迅速に回復させるプロセスを実施するかどうかに関する項目。			インシデント管理の実施有無	インシデント管理について規定しない	既存のインシデント管理のプロセスに従う	新規にインシデント管理のプロセスを規定する					
C.6.4.1			問題管理	インシデントの根本原因を追究し、可能であれば取り除くための処置を講じるプロセスを実施するかどうかに関する項目。			問題管理の実施有無	問題管理について規定しない	既存の問題管理のプロセスに従う	新規に問題管理のプロセスを規定する					
C.6.5.1			構成管理	ハードウェアやソフトウェアなどの IT 環境の構成を適切に管理するためのプロセスを実施するかどうかに関する項目。			構成管理の実施有無	構成管理について規定しない	既存の構成管理のプロセスに従う	新規に構成管理のプロセスを規定する					
C.6.6.1			変更管理	IT 環境に対する変更を効率的に管理するためのプロセスを実施するかどうかに関する項目。			変更管理の実施有無	変更管理について規定しない	既存の変更管理のプロセスに従う	新規に変更管理のプロセスを規定する					

C.6.7.1			リリース管理	ソフトウェア、ハードウェア、IT サービスに対する実装を管理するためのプロセスを実施するかどうかに関する項目。			リリース管理の実施有無	リリース管理について規定しない	既存のリリース管理のプロセスに従う	新規にリリース管理のプロセスを規定する					
D.1.1.1	移行性	移行時期	移行のスケジュール	移行作業計画から本稼働までのシステム移行期間、システム停止可能日時、並行稼働の有無。（例外発生時の切り戻し時間や事前バックアップの時間等も含むこと。）		○	システム移行期間	システム移行無し	3 ヶ月未満	半年未満	1 年未満	2 年未満	2 年以上	4	2 年未満
D.1.1.2						○	システム停止可能日時	制約無し（必要な期間の停止が可能）	5 日以上	5 日未満	1 日（計画停止日を利用）	利用の少ない時間帯（夜間など）	移行のためのシステム停止不可	5	移行のためのシステム停止不可
D.1.1.3						○	並行稼働の有無	無し	有り					1	有り
D.2.1.1		移行方式	システム展開方式	システムの移行および新規展開時に多段階による展開方式をどの程度採用するかの程度。		○	拠点展開ステップ数	単一拠点のため規定無し	一斉展開	5 段階未満	10 段階未満	20 段階未満	20 段階以上	2	5 段階未満
D.2.1.2						○	業務展開ステップ数	単一業務のため規定無し	全業務一斉切り替え	4 段階未満	6 段階未満	10 段階未満	10 段階以上	2	4 段階未満
D.3.1.1		移行対象（機器）	移行設備	移行前のシステムで使用していた設備において、新システムで新たな設備に入れ替え対象となる移行対象設備の内容。		○	設備・機器の移行内容	移行対象無し	移行対象設備・機器のハードウェアを入れ替える	移行対象設備・機器のハードウェア、OS、ミドルウェアを入れ替える	移行対象設備・機器のシステム全部を入れ替える	移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する		2	移行対象設備・機器のハードウェア、OS、ミドルウェアを入れ替える
D.4.1.1		移行対象（データ）	移行データ量	旧システム上で移行の必要がある業務データの量（プログラムを含む）。		○	移行データ量	移行対象無し	1TB 未満	1PB 未満	1PB 以上			1	1TB 未満
D.4.1.2						○	移行データ形式	移行対象無し	移行先と形式が同一	移行先と形式が異なる				1	移行先と形式が同一
D.4.2.1			移行媒体	移行対象となる媒体の量と移行時に必要となる媒体種類数。			移行媒体量	移行対象無し	10 本未満（1TB 未満）	1000 本未満（1PB 未満）	1000 本以上（1PB 以上）				
D.4.2.2							移行媒体種類数	移行対象無し	1 種類	2 種類	3 種類	4 種類	5 種類以上		
D.4.3.1			変換対象（DB	変換対象となるデータの量とツールの複雑度（変換ルール数）。			変換データ量	変換対象無し	1TB 未満	1PB 未満	1PB 以上				

D.4.3.2						移行ツールの複雑度(変換ルール数)	移行ツール不要または既存移行ツールで対応可能	変換ルール数が10未満の移行ツールの複雑度	変換ルール数が50未満の移行ツールの複雑度	変換ルール数が100未満の移行ツールの複雑度	変換ルール数が100以上の移行ツールの複雑度			
D.5.1.1		移行計画	移行作業分担	移行作業の作業分担。			移行のユーザ/ベンダ作業分担	全てユーザ	ユーザとベンダと共同で実施	全てベンダ				
D.5.2.1			リハーサル	移行のリハーサル(移行中の障害を想定したリハーサルを含む)。			リハーサル範囲	リハーサル無し	主要な正常ケースのみ	全ての正常ケース	正常ケース+移行前の状態に切り戻す異常ケース	正常ケース+システム故障から回復させる異常ケース		
D.5.2.2							リハーサル環境	リハーサル無し	本番データ使用可能	本番データ使用不可				
D.5.2.3							リハーサル回数	リハーサル無し	1回	2回	3回	4回	5回以上	
D.5.2.4							外部連携リハーサルの有無	無し	有り(外部接続仕様の変更無し)	有り(外部接続仕様の変更有り)				
D.5.3.1			トラブル対処	移行中のトラブル時の対応体制や対応プラン等の内容。			トラブル対処の規定有無	規定無し	対応体制のみ規定有り	対応体制と対応プランの規定有り				
E.1.1.1	セキュリティ	前提条件・制約条件	情報セキュリティに関するコンプライアンス	順守すべき情報セキュリティに関する組織規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。 なお、順守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 例) ・国内/海外の法律 ・資格認証 ・ガイドライン ・その他ルール		○	順守すべき社内規程、ルール、法令、ガイドライン等の有無	無し	有り					1	有り
E.2.1.1		セキュリティリスク分析	セキュリティリスク分析	システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目。 なお、適切な範囲を設定するためには、資産の洗い出しやデータのライフサイクルの確認等を行う必要がある。 また、洗い出した脅威に対して、対策する範囲を検討する。		○	リスク分析範囲	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	開発範囲				2	開発範囲

E.3.1.1		セキュリティ診断	セキュリティ診断	対象システムや、各種ドキュメント(設計書や環境定義書、実装済みソフトウェアのソースコードなど)に対して、セキュリティに特化した各種試験や検査の実施の有無を確認するための項目。		○	ネットワーク診断実施の有無	無し	有り					1	有り
E.3.1.2						○	Web 診断実施の有無	無し	有り					1	有り
E.3.1.3							DB 診断実施の有無	無し	有り						
E.4.1.1		セキュリティリスク管理	セキュリティリスクの見直し	対象システムにおいて、運用開始後に新たに発見された脅威の洗い出しとその影響の分析をどの範囲で実施するかを確認するための項目。 セキュリティリスクの見直しには、セキュリティホールや脆弱性、新たな脅威の調査等が含まれる。			セキュリティリスク見直し頻度	無し	セキュリティに関するイベントの発生時に実施(随時)	セキュリティに関するイベントの発生時に実施(随時)＋定期的に実施				
E.4.1.2							セキュリティリスクの見直し範囲	分析なし	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				
E.4.2.1			セキュリティリスク対策の見直し	対象システムにおいて、運用開始後に発見された脅威に対する対策の方針を確認するための項目。 また、検討するにあたり、発見された脅威についての対応範囲について明らかにする。			運用開始後のリスク対応範囲	対応しない	重要度が高い資産に関連する、あるいは、外接部分の脅威に対応	洗い出した脅威全体に対応				
E.4.2.2							リスク対策方針	無し	有り					
E.4.3.1			セキュリティパッチ適用	対象システムの脆弱性等に対応するためのセキュリティパッチ適用に関する適用範囲、方針および適用のタイミングを確認するための項目。 これらのセキュリティパッチには、ウィルス定義ファイル等を含む。 また、セキュリティパッチの適用範囲は、OS、ミドルウェア等毎に確認する必要があり、これらセキュリティパッチの適用を検討する際には、システム全体への影響を確認し、パッチ適用の可否を判断する必要がある。 なお、影響の確認等については保守契約の内容として明記されることが望ましい。			セキュリティパッチ適用範囲	セキュリティパッチを適用しない	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				
E.4.3.2							セキュリティパッチ適用方針	セキュリティパッチを適用しない	緊急性の高いセキュリティパッチのみ適用	全てのセキュリティパッチを適用				
E.4.3.3					–		セキュリティパッチ適用タイミング	セキュリティパッチを適用しない	障害パッチ適用時に合わせて実施	定期保守時に実施	パッチ出荷時に実施			
E.5.1.1		アクセス・利	認証機能	資産を利用する主体(利用者や機器等)を識別するための認証を実施するか、また、どの程度実施するのかを		○	管理権限を持つ主体の認証	実施しない	1 回	複数回の認証	複数回、異なる方式による認証			2	複数回の認証

E.5.1.2				確認するための項目。複数回の認証を実施することにより、抑止効果を高めることができる。なお、認証するための方式としては、ID/パスワードによる認証や、IC カード等を用いた認証等がある。			管理権限を持たない主体の認証	実施しない	1 回	複数回の認証	複数回、異なる方式による認証				
E.5.2.1			利用制限	認証された主体(利用者や機器など)に対して、資産の利用等を、ソフトウェアやハードウェアにより制限するか確認するための項目。 例) ドアや保管庫の施錠、USB や CD-RW やキーボードなどの入出力デバイスの制限、コマンド実行制限など。		○	システム上の対策における操作制限度	無し	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可					1	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみを許可
E.5.2.2							物理的な対策による操作制限度	無し	必要最小限のハードウェアの利用や操作のみを許可						
E.5.3.1			管理方法	認証に必要な情報(例えば、 ID/パスワード、指紋、虹彩、静脈など、主体を一意に特定する情報)の追加、更新、削除等のルール策定を実施するかを確認するための項目。			管理ルールの策定	実施しない	実施する						
E.6.1.1		データの秘匿	データ暗号化	機密性のあるデータを、伝送時や蓄積時に秘匿するための暗号化を実施するかを確認するための項目。		○	伝送データの暗号化の有無	無し	認証情報のみ暗号化	重要情報を暗号化				2	重要情報を暗号化
E.6.1.2						○	蓄積データの暗号化の有無	無し	認証情報のみ暗号化	重要情報を暗号化				2	重要情報を暗号化
E.6.1.3							鍵管理	無し	ソフトウェアによる鍵管理	耐タンパデバイスによる鍵管理					
E.7.1.1		不正追跡・監視	不正監視	不正行為を検知するために、それらの不正について監視する範囲や、監視の記録を保存する量や期間を確認するための項目。 なお、どのようなログを取得する必要があるかは、実現するシステムやサービスに応じて決定する必要がある。 また、ログを取得する場合には、不正監視対象と併せて、取得し		○	ログの取得	実施しない	実施する					1	実施する
E.7.1.2						○	ログ保管期間	6 ヶ月	1 年	3 年	5 年	10 年以上有期	永久保管	3	5 年

E.7.1.3				たログのうち、確認する範囲を定める必要がある。		○	不正監視対象(装置)	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				2	システム全体
E.7.1.4						○	不正監視対象(ネットワーク)	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				2	システム全体
E.7.1.5						○	不正監視対象(侵入者・不正操作等)	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				2	システム全体
E.7.1.6							確認間隔	無し	セキュリティに関するイベントの発生時に実施(随時)	セキュリティに関するイベントの発生時に実施(随時)＋定期的に実施	常時確認				
E.7.2.1			データ検証	情報が正しく処理されて保存されていることを証明可能とし、情報の改ざんを検知するための仕組みとしてデジタル署名を導入するかを確認するための項目。			デジタル署名の利用の有無	無し	有り						
E.7.2.2							確認間隔	無し	セキュリティに関するイベントの発生時に実施(随時)	セキュリティに関するイベントの発生時に実施(随時)＋定期的に実施	常時確認				
E.8.1.1		ネットワーク対策	ネットワーク制御	不正な通信を遮断するための制御を実施するかを確認するための項目。		○	通信制御	無し	有り					1	有り
E.8.2.1			不正検知	ネットワーク上において、不正追跡・監視を実施し、システム内の不正行為や、不正通信を検知する範囲を確認するための項目。		○	不正通信の検知範囲	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				1	重要度が高い資産を扱う範囲、あるいは、外接部分
E.8.3.1			サービス停止攻撃の回避	ネットワークへの攻撃による輻輳についての対策を実施するかを確認するための項目。		○	ネットワークの輻輳対策	無し	有り					1	有り
E.9.1.1		マルウェア対策	マルウェア対策	マルウェア(ウィルス、ワーム、ボット等)の感染を防止する、マルウェア対策の実施範囲やチェックタイミングを確認するための項目。		○	マルウェア対策実施範囲	無し	重要度が高い資産を扱う範囲、あるいは、外接部分	システム全体				2	システム全体

E.9.1.2				対策を実施する場合には、ウィルス定義ファイルの更新方法やタイミングについても検討し、常に最新の状態となるようにする必要がある。			リアルタイムスキャンの実施	実施しない	実施する					
E.9.1.3							フルスキャンの定期チェックタイミング	無し	不定期（フルスキャンを行えるタイミングがあれば実施する）	1回/月	1回/週	1回/日		
E.10.1.1		Web 対策	Web 実装対策	Web アプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。		○	セキュアコーディング、Web サーバの設定等による対策の強化	無し	対策の強化					1	対策の強化
E.10.1.2						○	WAF の導入の有無	無し	有り					0	無し
E.11.1.1		セキュリティインシデント対応/復旧	セキュリティインシデント対応/復旧	セキュリティインシデントが発生した時に、早期発見し、被害の最小化、復旧の支援等をするための体制について確認する項目。			セキュリティインシデントの対応体制	無し	有り					
F.1.1.1	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	構築時の制約となる社内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX 法 ・ISO/IEC27000 系 ・政府機関の情報セキュリティ対策のための統一基準 ・FISC ・プライバシーマーク ・構築実装場所の制限など		○	構築時の制約条件	制約無し	制約有り（重要な制約のみ適用）	制約有り（全ての制約を適用）				1	制約有り（重要な制約のみ適用）
F.1.2.1			運用時の制約条件	運用時の制約となる社内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・J-SOX 法 ・ISO/IEC27000 系 ・政府機関の情報セキュリティ対策のための統一基準 ・FISC ・プライバシーマーク ・リモートからの運用の可否など		○	運用時の制約条件	制約無し	制約有り（重要な制約のみ適用）	制約有り（全ての制約を適用）				1	制約有り（重要な制約のみ適用）

F.2.1.1		システム特性	ユーザ数	システムを使用する利用者(エンドユーザ)の人数。	○	○	ユーザ数	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用				2	不特定多数のユーザが利用
F.2.2.1			クライアント数	システムで使用され、管理しなければいけないクライアントの数。		○	クライアント数	特定クライアントのみ	上限が決まっている	不特定多数のクライアントが利用				2	不特定多数のクライアントが利用
F.2.3.1			拠点数	システムが稼働する拠点の数。		○	拠点数	単一拠点	複数拠点					1	複数拠点
F.2.4.1			地域的広がり	システムが稼働する地域的な広がり。		○	地域的広がり	拠点内	同一都市内	同一都道府県内	同一地方	国内	海外	4	国内
F.2.5.1			特定製品指定	ユーザの指定によるオープンソース製品や第三者製品(ISV/IHV)などの採用の有無を確認する項目。採用によりサポート難易度への影響があるかの視点で確認を行う。		○	特定製品の採用有無	特定製品の指定がない	一部に特定製品の指定がある	サポートが困難な製品の指定がある				0	特定製品の指定がない
F.2.6.1			システム利用範囲	システム利用者が属する属性の広がり。			システム利用範囲	部門内のみ	社内のみ	社外(BtoB)	社外(BtoC)				
F.2.7.1			複数言語対応	システム構築の上で使用が必要、またはサービスとして提供しなければならない言語。扱わなければならない言語の数や各言語スキル保持者へのアクセシビリティを考慮。			言語数	数値などのみ扱う	1	2	5	10	100		
F.3.1.1		適合規格	製品安全規格	提供するシステムに使用する製品について、UL60950 などの製品安全規格を取得していることを要求されているかを確認する項目。		○	規格取得の有無	規格取得の必要無し	UL60950 相当取得	—				0	規格取得の必要無し
F.3.2.1			環境保護	提供するシステムに使用する製品について、RoHS 指令などの特定有害物質の使用制限についての規格の取得を要求されているかを確認する項目。		○	規格取得の有無	規格取得の必要無し	RoHS 指令相当取得	—				0	規格取得の必要無し
F.3.3.1			電磁干渉	提供するシステムに使用する製品について、VCCI などの機器自身が放射する電磁波をある一定以下のレベルに抑える規格を取得していることを要求されて		—	規格取得の有無	規格取得の必要無し	VCCI ClassA 取得	VCCI ClassB 取得				—	—

				いるかを確認する項目。										
F.4.1.1		機材設置環境条件	耐震/免震	地震発生時にシステム設置環境で耐える必要のある実効的な最大震度を規定。建屋が揺れを減衰するなどの工夫により、外部は震度 7 超でも設置環境では実効的に最大震度 4 程度になる場合には震度 4 よりレベルを設定する。なお、想定以上の揺れではサービスを継続しないでも良い場合には、その想定震度でレベルを設定する。		○	耐震震度	対策不要	震度 4 相当(50 ガル)	震度 5 弱相当(100 ガル)	震度 6 弱相当(250 ガル)	震度 6 強相当(500 ガル)	震度 7 相当(1000 ガル)	4	震度 6 強相当(500 ガル)
F.4.2.1			スペース	どの程度の床面積(WxD)/高さが必要かの項目。保守作業用スペースについても考慮する。また、移行時には新旧システムが並行稼働可能なスペースの確保が可能か否かについても確認が必要である。可能であれば事前確認を実施する。		○	設置スペース制限(マシンルーム)	スペースに関する制限無し	フロア設置用機材を用いて構成	ラックマウント用機材を用いて構成				2	ラックマウント用機材を用いて構成
F.4.2.2						○	設置スペース制限(事務所設置)	スペースに関する制限無し	専用のスペースを割当て可能	人と混在するスペースに設置必要	—			2	人と混在するスペースに設置必要
F.4.2.3							並行稼働スペース(移行時)	専用スペースの確保が可能	共用スペースの確保が可能	確保不可					
F.4.2.4							設置スペースの拡張余地	十分な拡張余地有り	一部制約有り(既製品で対応できるレベル)	制約有り(特注対応や工事が必要)					
F.4.3.1			重量	建物の床荷重を考慮した設置設計が必要となることを確認する項目。低い床荷重の場合ほど、設置のための対策が必要となる可能性が高い。			床荷重	2,000Kg/㎡以上	1,200Kg/㎡	800Kg/㎡	500Kg/㎡	300Kg/㎡	200Kg/㎡		
F.4.3.2							設置対策	不要	荷重を分散するための資材(鉄板など)を配備する	ラック当りの重量を制限して、分散構成を採る	設置環境固有の条件(梁の場所など)を考慮して、設置設計を行う				
F.4.4.1			電気設備適合性	ユーザが提供する設置場所の電源条件(電源電圧/電流/周波数/相数/系統数/無停止性/必要工事規模など)と導入システムの適合性に関する項目。同時に空調についても評価対象とする。また、移行時の並行稼動が可能か否かについても確認が必要であ			供給電力適合性	現状の設備で特に制限無し	電源工事は必要だが、分電盤改造など二次側の工事のみで対応可能	電源工事は必要だが、一次、二次とも工事可能	工事などができず、規模に対して容量が少し足りない	まったく対応できず、設置場所を再考する必要がある		
F.4.4.2							電源容量の制約	制約無し(必要な電源容量の確保が可能)	制約有り(既製品で対応できるレベル)	制約有り(カスタマイズや工事が必要)					

F.4.4.3				る。可能であれば事前確認を実施する。			並行稼働電力(移行時)	全面的に確保が可能	部分的に確保が可能	確保が困難				
F.4.4.4							停電対策	無し	瞬断(10ms 程度)	10 分	1 時間	1 日間	1 週間	
F.4.4.5							想定設置場所の電圧変動	±10%以下	±10%を超える					
F.4.4.6							想定設置場所の周波数変動	±2%以下	±2%を超える					
F.4.4.7							接地	接地不要	接地が必要	専用接地が必要				
F.4.5.1			温度(帯域)	システムが稼働すべき環境温度の帯域条件。 周囲環境によってはシステムを正常稼動させるには特別な対策が必要となることがある。			温度(帯域)	対策不要	16 度から 32 度(多くのテープ装置の稼働可能条件)	5 度から 35 度(多くの機器の稼働可能条件)	0 度～40 度	0 度～60 度	-30 度～80 度	
F.4.6.1			湿度(帯域)	システムが稼働すべき環境湿度の帯域条件。 周囲環境によってはシステムを正常稼動させるには特別な対策が必要となることがある。			湿度(帯域)	対策不要	45%～55%	20%～80%	0%～85%	結露無し条件のみ		
F.4.7.1			空調性能	システムを稼働させるのに十分な冷却能力を保持し、特定のホットスポットが存在する場合にはそれを考慮した冷気供給を行える能力。			空調性能	十分な余力有り	ホットスポットなどへの部分的な対策が必要	能力が不足しており、対策が必要				
F.4.7.2							空調設備の制約	制約無し(必要な空調の確保が可能)	制約有り(既製品で対応できるレベル)	制約有り(カスタマイズや工事が必要)				
F.5.1.1		環境マネージメント	環境負荷を抑える工夫	環境負荷を最小化する工夫の度合いの項目。 例えば、グリーン購入法適合製品の購入など、環境負荷の少ない機材･消耗品を採用する。 また、ライフサイクルを通じた廃棄材の最小化の検討を行う。例えば、拡張の際に既設機材の廃棄が不要で、必要な部材の増設、入れ替えのみで対応可能な機材を採用するなどである。また、ライフサイクルが長い機材ほど廃棄材は少ないと解釈できる。			グリーン購入法対応度	対処不要	グリーン購入法の基準を満たす製品を一部使用	グリーン購入法の基準を満たす製品のみを使用	—	—		
F.5.1.2							同一機材拡張余力	無し	2 倍	4 倍	10 倍	30 倍	100 倍以上	
F.5.1.3							機材のライフサイクル期間	3 年	5 年	7 年	10 年以上			

F.5.2.1			エネルギー消費効率	本来はシステムの仕事量をそのエネルギー消費量で除した単位エネルギー当りの仕事量のこと。ただし、汎用的な仕事量の定義が存在しないため、効率を直接求めることは困難である。また、同じ仕事を行う別のシステムも存在しないことが多いため、比較自体も困難である。このため、エネルギー消費効率に関しては、少し視点を変えて、ユーザからの目標値の提示の有無などでレベル化を行っている。なお、電力エネルギーを前提とするシステムでは、消費電力≒発熱量である。 また、システムの仕事量の視点ではなく、データセンターのエネルギー効率を示す指標に PUE(Power Usage Effectiveness)や、DPPE(Datacenter Performance Per Energy)などがある。			エネルギー消費の目標値	目標値無し	目標値の提示有り	目標値の提示が有り、更なる追加削減の要求も有る					
F.5.3.1			CO2 排出量	システムのライフサイクルを通じて排出される CO2 の量。ただし、単純な CO2 排出量でレベル化するのは困難であるため、少し視点を変えて、ユーザからの目標値の提示の有無などでレベル化を行っている。			CO2 排出量の目標値	目標値の設定不要	目標値の提示有り	目標値の提示が有り、更なる追加削減の要求も有る					
F.5.4.1			低騒音	機器から発生する騒音の低さの項目。特にオフィス設置の場合などには要求度が高くなる傾向がある。また、データセンターなどに設置する場合でも一定以上の騒音の発生は労働環境として問題となることがある。			騒音値	対策不要	87dB(英国 RoSPA の騒音基準による防音保護具の使用も考慮に入れた許容限界値)以下	85dB(英国 RoSPA の騒音基準による第 2 アクションレベル)以下	80dB(英国 RoSPA の騒音基準による第 1 アクションレベル)以下	40dB(図書館レベル)以下	35dB(寝室レベル)以下		

「電力広域的運営推進機関　OAシステムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託」に関する質問等

電力広域的運営推進機関

No.	質問日	質問者 （会社名、所属、役職、氏名）	仕様書等該当箇所 （ページ、項目等）	質　問
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

OAシステムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託

御 社 名

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿㊞

適合証明書

電力広域的運営推進機関

区分	入札説明書 記載箇所	機能	適合※1	補足※2
入札資格	2.1（1）	令和０７・０８・０９年度の競争参加資格（全省庁統一資格）、「物品の販売」及び「役務の提供等」において、「A」以上の等級に格付けされていること。		
	2.1（2）	各省各庁から指名停止又は一般競争入札資格停止若しくは営業停止をうけていない者であること。		
	2.1（3）	入札説明会に参加した者であること。		
	2.1（4）	予算決算及び会計令(昭和22年勅令第165号)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。		
	2.1（5）	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。		
	2.1（6）	会社更生法（平成14年法律第154号）に基づく更生手続開始の申立て又は民事再生法（平成11年法律第225号）に基づく再生手続開始の申立てがなされている者でないこと。（但し、会社更生法に基づく更生手続開始の申立て又は民事再生法に基づく再生手続開始の申立てがなされている者で、手続開始の決定後、競争参加資格の再認定を受けている者を除く。）		
	2.1（7）	自己、自社若しくはその役員等（注1）が、暴力団員による不当な行為の防止等に関する法律第2条に定める暴力団、暴力団員又はその他反社会的勢力（注2）でない者であること。 （注１）取締役、監査役、執行役、支店長、理事等、その他経営に実質的に関与している者。 （注２）暴力団準構成員、総会屋等、社会運動等標ぼうゴロ又は特殊知能暴力集団、暴力団又は暴力団員と社会的に非難されるべき関係を有する者、暴力団員でなくなった時から5年を経過しない者等、その他これに準じる者。		
	2.1（8）	破壊活動防止法（昭和２７年法律第２４０号）に定めるところの破壊的団体およびその構成員でない者であること。		

※1　適合については，“○（要件を満たしている）”，“△（条件付きで要件を満たしている，代替手段で要件を満たす）”，“×（要件を満たしていない）”で記述をお願いします。また，“△”を記入した場合は，補足欄に説明をご記入ください。

※2　補足すべき事項がある場合は，その内容を補足欄に記入してください。また，添付資料がある場合は同封し提出をお願いします。

電力広域的運営推進機関　OAシステムリプレースに係るネットワークならびに認証機能等の設計・構築及び運用保守の業務委託　評価項目一覧　ー提案要求事項一覧ー

電力広域的運営推進機関

提案書の目次			提案要求事項	仕様書の該当項目(※) (仕)は入札仕様書に記載している該当項目 (要)は要件定義書に記載している該当項目	評価区分	得点配分			評価基準		提案書番号
大項目	中項目	小項目				合計	基礎点	加点	基礎点	加点	
1 背景・目的											
	1.1	背景・目的	本調達の背景・目的を理解したうえで、目的が電力広域的運営推進機関の目的と合致しているか。	(仕)1. 調達案件の概要に関する事項	必須	2	2	ー	・電力広域的運営推進機関の社会的役割・社会的要請を考慮し、本OAシステムリプレースの背景・目的を捉え、理解している。 ・電力業界を取り巻く状況、社会環境の変化を考慮した上で、本OAシステムリプレースの背景・目的について、深堀り・分析し、提案されている。	-	
2 プロジェクト計画・構成											
	2.1	調達対象の理解	・OAシステムリプレースの対象範囲を正しく理解し記載されているか。	(仕)1. 調達案件の概要に関する事項 (要)1. 調達要件	必須	4	2	2	・OAシステムリプレースのハードウェア、ソフトウェア、役務、保守、外部サービスの対象範囲を正しく理解している。 ・業務を遂行するための、対象外(広域機関システム、スイッチング支援システム)を明確に区別している。	・調達対象ごとの役割・範囲(ハードウェア／ソフトウェア／役務／保守／外部サービスについて)表または構成図で役割分担が明示されている。 ・「広域機関システム」や「スイッチング支援システム」が対象外である理由・責任範囲まで明記されている。	
	2.2	構成の妥当性、プロジェクト体制	本OAシステムリプレースの全体構成について記載されている。	(仕)1. 調達案件の概要に関する事項 (仕)2. 作業の実施内容に関する事項 (要)1. 調達要件	必須	3	2	1	本調達の構成図・構成説明が要件を満たし、実現性がある。	・将来の拡張性(台数増加、拠点追加、クラウド移行等)を考慮した構成になっている説明がある。 ・実施体制・運用体制(役割分担図(RACI等))について、記載がなされている。	
	2.3	スケジュール	全体スケジュールが記載されているか。	(仕)1. 調達案件の概要に関する事項 (要)3. 役務に関する要件	必須	4	2	2	本調達の作業スケジュールを理解したうえで、全体スケジュールを記載している。	・スケジュール短縮化に資する、具体的な方策(並行作業、事前準備、標準化など)工程短縮の具体策が工程表と紐づいている。 ・スケジュールについて、具体的かつ合理的(マイルストーン、依存関係、クリティカルパス等が分かる)に提案されている。	
	2.4	コスト低減	具体的、効率的に実施できる方策が記載されているか。	-	任意	2	ー	2		・中長期的な視野による各システム及びネットワークのコスト低減の策(保守費用・更新費用の抑制策、中長期でのコスト最適化)を全て講じているか。	
3 機能要件の理解と実現											
	3.1	要件確認・設計	要件確認方法、設計方針が明確に記載されているか。	(仕)2.作業の実施内容に関する事項 (要)3. 役務に関する要件	必須	7	5	2	要件確認方法、設計方針が明確に記載されているか。	・業務継続性を考慮したシステム構築方針(障害・切替・冗長構成を前提とした設計方針)が具体的に記載されている。 ・関連システムを考慮した構成(OA以外の関連システムとの関係が図または表で説明)が記載されている。	
	3.2	構築・設置	構築・設置・工事内容が具体的に記載されているか。	(仕)2.作業の実施内容に関する事項 (要)3. 役務に関する要件	必須	7	5	2	構築・設置・工事内容が具体的に記載されているか。	・各拠点についての設置・工事が明記(設置場所、機器種別、作業内容が拠点別に表または図で整理)されている。 ・提案コンセプトに即した、具体的な実現手段(構築・設置作業の工事方法・手順・順序)について記載されている。	
	3.3	試験計画	試験項目、実施方法、合否基準が明確になっているか。	(仕)2.作業の実施内容に関する事項 (要)3. 役務に関する要件	必須	7	5	2	試験項目、実施方法、合否基準が明確になっているか。	・試験項目(単体試験、結合試験、運用・切替試験、障害／異常系試験等)が表形式または章立てで確認出来、再現性が高い記載になっている。	
	3.4	チューニング	性能・安定性を考慮した調整方針が示されているか。	(仕)2.作業の実施内容に関する事項 (要)3. 役務に関する要件	必須	5	3	2	性能・安定性を考慮した調整方針が示されているか。	・WiFi環境(無線)についてのチューニングが具体的(帯域、遅延、パケットロス、アプリケーションのタイムアウト、同時接続数等)に2項目以上記載されている。	
4 非機能要件の理解と実現											
	4.1	サービス継続性の理解	業務継続性を正しく理解しているか。	(要)1. 調達要件 (要)2.(2) 非機能要件	必須	7	5	2	・メインサイトおよびバックアップサイトを前提とした業務継続性の考え方を理解し提案されている。	・障害等の色々な状況を考慮し、業務継続性の提案(メインサイト・バックアップサイトの役割が図または表で整理されている、通常時/障害時/災害時のサイトごとの役割分担が明示)がされている。	
	4.2	DR対策内容	DR対策の内容が記載されているか。	(要)1. 調達要件 (要)2.(2) 非機能要件	必須	7	5	2	・災害時を想定した(DR対策)構成・運用が提案されている。	・各システム単位でDRを発動した場合(DR発動条件・切替手順等)を考慮し、実運用を想定した提案(DR可否・優先度)がされている。	
	4.3	復旧時の考え方	機能単位の復旧方針の記載がされているか。	(要)1. 調達要件 (要)2.(2) 非機能要件	必須	7	5	2	・各機能ごとに、復旧手順・優先度の考え方が記載されている。	・各機能ごとに、実運用を想定した切替・復旧手順の記載(機能・システム単位で復旧優先度(高/中/低 等)が整理されている、業務影響度を踏まえた復旧の考え方(重要業務優先 等)が明示)がされている。	
5 運用・保守要件の実現											
	5.1	稼働監視・障害対応	稼働監視・障害対応の記載がされているか。	(要)4. 保守に関する要件	必須	11	8	3	・24時間365日の監視・障害対応体制が明確か記載されている。 ・体制及び連絡先等の記載がされている。	・現行システムの運用内容を調査(現行運用の調査・ヒアリング、課題整理、改善案の検討・提案)の上、より良い運用方式を検討するプロセスとなっている。 ・災害発生時の運用・保守(災害発生時の監視継続方法、障害対応体制の切替、通常時と異なる連絡経路・指揮系統の整理)について検討されている。	
	5.2	運用支援	運用支援についての具体的な記載がされているか。	(要)4. 保守に関する要件	必須	10	8	2	・設定変更、アップデート、脆弱性対応が要件通りに記載されている。	・脆弱性情報の能動提供など(脆弱性情報の定期提供、重要度CVSSに応じた対応区分の考え方、緊急性の高い脆弱性に対する連絡・対応フローの明示)が記載されている。 ・システム運用者の業務負荷を軽減する方策(定型作業の代行・自動化、申請・依頼フローの簡素化)が検討されている。	
	5.3	バックアップ	バックアップについて具体的に記載されているか。	(要)4. 保守に関する要件	必須	7	5	2	・取得方法・保存世代が要件を満たしている。	・障害時および災害、サイバーセキュリティインシデント発生時発生時の対応(対象機器、データ、設定情報、取得方法(フル/差分 等)、保存世代・保存期間)が検討されている。	
	5.4	保守受付・通知	保守受付・通知について具体的な記載がされているか。	(要)4. 保守に関する要件	必須	4	4	ー	・受付窓口、情報通知、EOL通知が明確に記載されている。	-	
	5.5	報告・管理	報告・業務管理について記載されているか。	(要)4. 保守に関する要件	必須	6	4	2	・月次・年次報告、業務管理が適切に記載されている。	・報告対象、報告手段、報告タイミング等 内容の良し悪しは問わず、分かる形で書いてある。 ・月次報告に改善提案を含む内容(障害・問い合わせの集計・分析、定例会やレビューの実施、改善提案・フィードバックの仕組み等何が報告されるかイメージできるか)が記載されている。	

合計	100	70	30