

容量市場システム  
(一次開発)  
要件定義書

2018年12月19日

電力広域的運営推進機関

# 目次

1. 調達件名 .....	1
2. 業務要件の定義 .....	1
3. 機能要件の定義 .....	1
3.1. 機能に関する事項 .....	1
3.1.1. 機能に関する基本事項 .....	1
3.2. 画面に関する事項 .....	3
3.2.1. 画面設計に関する基本事項 .....	3
3.2.2. 画面設計要件 .....	3
3.3. 帳票に関する事項 .....	5
3.3.1. 帳票設計に関する基本事項 .....	5
3.3.2. 帳票設計要件 .....	6
3.4. 情報・データに関する事項 .....	6
3.5. 外部インタフェースに関する事項 .....	6
3.5.1. 連携システム .....	6
4. 非機能要件の定義 .....	6
4.1. ユーザビリティ及びアクセシビリティに関する事項 .....	6
4.1.1. ユーザビリティ要件 .....	6
4.1.2. アクセシビリティ要件 .....	7
4.2. システム方式に関する事項 .....	7
4.2.1. 情報システムの構成に関する全体の方針 .....	7
4.2.2. 情報システムの全体構成 .....	7
4.2.3. 開発方式及び開発手法 .....	7
4.3. 規模に関する事項 .....	7
4.4. 性能に関する事項 .....	7
4.4.1. 応答時間 .....	8
4.5. 信頼性に関する事項 .....	8
4.5.1. 可用性要件 .....	8
4.5.2. 完全性要件 .....	8
4.6. 拡張性に関する事項 .....	8
4.7. 上位互換性に関する事項 .....	9
4.8. 中立性に関する事項 .....	9
4.9. 継続性に関する事項 .....	9
4.9.1. 継続性に関する目標値 .....	9
4.9.2. 継続性に係る対策 .....	9
4.10. 情報セキュリティに関する事項 .....	10
4.10.1. 基本事項 .....	10

4.10.2. 権限要件 .....	10
4.10.3. 情報セキュリティ対策要件 .....	10
4.11. 情報システム稼働環境に関する事項 .....	13
4.11.1. 基本要件 .....	13
4.11.2. 構築すべき環境 .....	14
4.11.3. 保守端末・監視端末要件 .....	14
4.11.4. 保守拠点の要件 .....	14
4.11.5. クライアント環境要件 .....	14
4.12. テストに関する事項 .....	14
4.12.1. テスト工程共通要件 .....	14
4.12.2. テストデータ要件 .....	15
4.12.3. 単体テスト要件 .....	15
4.12.4. 結合テスト要件 .....	15
4.12.5. 総合テスト要件 .....	15
4.12.6. 受入テスト支援要件 .....	15
4.12.7. 参加者テスト支援要件 .....	16
4.13. 移行に関する事項 .....	16
4.14. 教育に関する事項 .....	16
4.15. 運用に関する事項 .....	17
4.15.1. 基本事項 .....	17
4.15.2. 情報システムの操作・監視等要件 .....	17
4.15.3. 運用サポート業務に係る要件 .....	18
4.15.4. ログ管理要件 .....	19
4.16. 保守に関する事項 .....	20
4.16.1. アプリケーションプログラムの保守 .....	20
5. 附属文書 .....	22

## 1. 調達件名

容量市場システム（一次開発）の設計開発及び運用保守業務委託

## 2. 業務要件の定義

業務要件については以下を参照のこと。

なお、業務の実施場所については、電力広域的運営推進機関（以下、「本機関」という。）の事務所（東京都江東区）及びバックアップ拠点（大阪府大阪市北区）とする。

表 2-1：業務要件と参照すべき資料

No	業務要件	参照すべき資料
1	業務の実施手順及びそれらを記載した業務フロー図	別紙 1. 「業務概要設計書」 別紙 2. 「業務詳細設計書」
2	情報システムの利用者数及び期間当たりの処理件数等、業務の規模	別紙 3. 「業務量定義書」
3	業務の実施・提供期間	別紙 1. 「業務概要設計書」
4	情報システムを用いて実施する業務の範囲及び情報システムを用いずに実施する業務の範囲	別紙 2. 「業務詳細設計書」

また、各業務については、経済産業省の総合資源エネルギー調査会電力・ガス事業分科会電力・ガス基本政策小委員会制度検討作業部会、及び本機関主催の「容量市場の在り方等に関する検討会」の議事内容を確認し、十分に理解すること。

## 3. 機能要件の定義

### 3.1. 機能に関する事項

#### 3.1.1. 機能に関する基本事項

容量市場システム（一次開発）（以下、「本システム」という。）の機能については、「別紙4. 機能一覧」を参照のこと。

なお、本システムの機能は各機能間で類似点が多いことから、共通要件として原則、以下を実現すること。

表 3-1：共通要件

No	機能	内容
1	照会（検索）系機能	<ul style="list-style-type: none"><li>検索条件に基づき各データを抽出できること。</li><li>抽出結果は一覧で表示可能とするとともに、CSV形式等の汎用的なデータ形式で一括ダウンロードを可能とすること。</li><li>事業者が利用するユーザ（以下「事業者ユーザ」）は自事業者分のみ、本機関が利用するユーザ（以下「広域機関ユーザ」）は全事業者分を対象にデータを照会（検索）できること。</li></ul>

No	機能	内容
2	登録（入力）系機能	<ul style="list-style-type: none"> <li>事業者ユーザ及び広域機関ユーザは、各入力情報に基づき登録申込ができること。</li> <li>登録申込にあたっては、入力情報の妥当性（必須記載事項の記載有無、各項目の記載形式（文字・数字などの型式）等が正しいか）、重複チェック等を実施した上で、問題がある場合にはダイアログを表示し、登録申込できないようにすること。</li> <li>広域機関ユーザが審査管理機能において、審査結果を登録・反映するまで、データベースの更新を行わないこと。</li> <li>事業者ユーザは自事業者分のみ、広域機関ユーザは全事業者分を対象にデータを入力できること。</li> <li>登録履歴を管理すること。</li> </ul>
3	変更（更新）系機能	<ul style="list-style-type: none"> <li>事業者ユーザ及び広域機関ユーザは、各入力情報に基づき変更申込できること。</li> <li>変更申込にあたっては、入力情報の妥当性（必須記載事項の記載有無、各項目の記載形式（文字・数字などの型式）等が正しいか）重複チェック等を実施した上で、問題がある場合にはダイアログを表示し、変更申込できないようにすること。</li> <li>審査が必要な項目に対する変更申込は、広域機関ユーザが審査管理機能において、審査結果を登録・反映するまで、データベースの更新を行わないこと。また、審査が不要な項目に対する変更申込は、変更内容を即時に反映すること。</li> <li>事業者ユーザは自事業者分のみ、広域機関ユーザは全事業者分を対象にデータを入力できること。</li> <li>変更履歴を管理すること。</li> </ul>
4	取消（削除）系機能	<ul style="list-style-type: none"> <li>物理削除ではなく論理削除（有効期間による削除、削除フラグによる削除等）とすること。</li> <li>削除履歴を管理すること。</li> </ul>
5	審査系機能	<ul style="list-style-type: none"> <li>各審査業務について、本システム内で保持している情報との突合により審査可能なものは、システム的に審査を行うこと。</li> <li>各審査の状況（審査中、合格、不合格等）が一覧で分かるようにすること。</li> <li>審査結果の登録にあたっては、広域機関ユーザにより</li> </ul>

No	機能	内容
		<p>個別の審査結果を登録の後、バッチ処理にて登録結果をデータベース等記憶領域に反映すること。(但し、例外処理として手動により即時に反映することも可能とすること。)</p> <ul style="list-style-type: none"> <li>審査結果の登録については、1件の申込に対して審査項目ごとに、異なる広域機関ユーザが審査結果を同時に登録できること。</li> <li>審査結果の登録について、複数の広域機関ユーザが1つの申込に対して項目ごとに審査結果を同時に登録可能とすること。</li> </ul>

### 3.2. 画面に関する事項

#### 3.2.1. 画面設計に関する基本事項

- ・本システムの画面は、「別紙5. 主な画面一覧」を参照のこと。
- ・「別紙4. 機能一覧」及び「別紙5. 主な画面一覧」を基に画面設計を実施すること。

#### 3.2.2. 画面設計要件

##### 3.2.2.1. 画面形式パターン

- ・画面構成（メニューの表記・位置、色等の個別要素や、レイアウト等外観）の統一を図ること。
- ・一画面につき一意になるような画面ID、画面名を付けること。
- ・同じ機能、意味合いのフィールドは包括的な名称により統一された名称体系とすること。
- ・システム内の共通要素（画面名、ユーザ名、システム日付等）は、原則、どの画面でも同じ場所に配置すること。
- ・画面上の表記は、事業者ユーザ及び広域機関ユーザを含む本システムを利用する者（以下、「ユーザ」という。）が日常使用している用語とすること。
- ・提供する機能が同一もしくは類似の場合、可能な限り同一の画面を使用すること。
- ・タブの遷移（画面中入力項目間の移動等）については、入力の流れに沿った遷移とし、統一すること。
- ・システムの階層やプロセス等のナビゲーションを表示すること（判りやすい言葉を使用したタイトルと階層化された業務番号を一定のルールのもとにつける等）。
- ・特定の画面を操作している際も、別ウィンドウにて他の画面を立ち上げて参照することができること。
- ・本システム全体のメニュー表記等のユーザインターフェースのデザインを統一すること。
- ・本システムで用いられる業務アプリケーションプログラム全般にわたる画面の操作性を統一すること。

##### 3.2.2.2. 画面サイズ

- ・画面の大きさに関わらず、画面の表示項目の閲覧に支障のないようにすること。
- ・ユーザが画面サイズを変更した場合でも、情報の参照及び操作に支障がないようにすること。

### 3.2.2.3. 画面機能

- ・Webブラウザの印刷機能等を用いて、ユーザが随時画面情報を紙媒体に出力できること。
- ・照会結果の一覧系表示画面全般について、任意の表示項目を指定し、当該項目の入力内容をキーとした表示情報の並び替えが可能であること。

### 3.2.2.4. 色、字体、サイズ、数値表現

- ・文字色と背景色のコントラストを十分に取り、文字を読みやすくすること。
- ・字体・文字サイズの種類を多用することは避け、システムで統一を図ること。
- ・数値はアラビア数字を基本とし、表示はカンマ形式とすること。

### 3.2.2.5. ダイアログ表示

- ・ダイアログは、システムからユーザへの注意喚起や対処を要求したりするためのメッセージの表示及び入力支援機能とし、ダイアログは表示元の画面の中央に表示することを基本とすること。
- ・ダイアログの表示中は表示元の画面の操作ができないようにすること。
- ・エラー、警告、情報等によってダイアログを区別し、ユーザが通知内容を直観的に理解できるように表示すること。
- ・重要度が高い操作を行う等、誤操作の防止を要する際には、確認メッセージを表示し、ユーザの確認を促すこと。

### 3.2.2.6. 表

- ・横スクロールは可能な限り使用しないこと。
- ・スクロールする場合でも、入力及び出力のキーとなる項目を画面上に固定し、表示できるようにすること。
- ・表中の項目の間に空行を作らないこと。また、削除処理を行った際に、削除した行を空行として残さないこと。

### 3.2.2.7. ボタン

- ・同じ機能、意味合いのボタンは名称を統一すること。
- ・ボタン名称は、ユーザがボタン押下時の処理内容を推測できるようにすること。
- ・ボタン位置は、ユーザの利便性を考慮した配置とすること。

### 3.2.2.8. 画面要素

- ・メニュー部、ガイド部、一覧表示部等表示する内容と画面位置を統一化すること。
- ・テキストボックス、チェックボックス、リストボックス、プルダウンメニュー等については業務の利便性を考慮し選択すること。

- ・ユーザの利便性を高めるため、定型的な入力項目についてはリストボックスでの選択を可能にする等の機能を準備すること。
- ・情報の全削除や他画面への複写処理等、ユーザの利便性向上に資する機能を容易に実行できるよう、必要に応じて、当該機能を実行するためのボタンを配置すること。

### 3.2.2.9. 遷移方法

- ・画面遷移を体系化し、画面の階層が深くなりすぎないように配慮すること。
- ・基点となるメニュー画面、関連する検索・一覧画面等に遷移するためのボタンを各画面に配置する等、ユーザの利便性を考慮した体系とすること。
- ・「戻る」ボタン押下後及び登録・変更処理後の画面遷移は、一度入力した情報を引継ぐようにする等、ユーザにとって業務の効率性を考慮した方式とすること。
- ・表示等の処理に時間を要する機能を実行する遷移の前には、確認画面を表示すること。
- ・遷移する際には、遷移元の情報を可能な限り遷移先に引継ぎ、ユーザによる再入力の負荷を低減すること。

### 3.2.2.10. 入力時チェック

- ・入力画面においては、エラーチェックを行い、ユーザに正しい入力を促すようにすること。

### 3.2.2.11. データ更新の一貫性

- ・業務上、重要な情報を登録、更新、削除を行う際は、データ更新前に確認メッセージを提供し、誤った情報の更新を未然に防ぐこと。
- ・画面遷移を行う際、前画面において表示した情報を再度表示させる場合は同じ場所に表示することを基本とすること。

### 3.2.2.12. エラー扱いの方針

- ・入力のエラーがある場合には、入力した情報を破棄せずに登録画面を再表示し、ユーザの登録作業の負荷を軽減すること。
- ・入力のエラーがある項目を全て明示する仕組みを設けるなど、入力操作の繰り返しが最低限となるようすること。
- ・入力のエラー発生時にユーザがエラー状況を理解できるような表示を行うこと。
- ・業務アプリケーションプログラムを実行する際にエラーが発生した場合には、エラーの内容をユーザに分かりやすく表示するとともに、定義されたエラーの種類を示す番号、発生日時、実行中の画面の番号等を可能な限り表示すること。

## 3.3. 帳票に関する事項

### 3.3.1. 帳票設計に関する基本事項

- ・本システムの帳票は、「別紙6. 主な帳票・ファイル一覧」を参照のこと。
- ・「別紙4. 機能一覧」及び「別紙6. 主な帳票・ファイル一覧」を基に帳票設計を実施すること。

### 3.3.2. 帳票設計要件

#### 3.3.2.1. 帳票形式パターン

- ・業務アプリケーションプログラム全般にわたる帳票の標準化を行うこと。
- ・帳票名やヘッダ、フッタ情報等の帳票構成及び概観の統一を図ること。
- ・帳票上の表記は、ユーザが日常使用している用語とすること。
- ・提供する情報が同一もしくは類似の場合、可能な限り同一の帳票を使用すること。

#### 3.3.2.2. 用紙サイズ

- ・帳票についての用紙サイズは、A4サイズを基本とすること。

#### 3.3.2.3. 出力形式

- ・「別紙6. 帳票・ファイル一覧」を参照のこと。

#### 3.3.2.4. 色、字体、サイズ、数値表現

- ・帳票はモノクロ帳票を標準として統一すること。
- ・字体・文字サイズの種類を多用することは避け、統一を図ること。
- ・数値はアラビア数字を基本とし、表示はカンマ形式とすること。
- ・類似の帳票については、帳票間で行間、行数にばらつきが出ないように、統一を図ること。

#### 3.3.2.5. 出力タイミング

- ・ユーザの指示により、随時出力できること。

### 3.4. 情報・データに関する事項

本システムの情報・データは、「別紙7. 主な情報・データ一覧」を参照すること。

### 3.5. 外部インターフェースに関する事項

#### 3.5.1. 連携システム

法人登録の有無を確認するため、国税庁法人番号システムにWeb-APIにて連携すること。

その他、通信回線等で接続し、自動的に処理を行う等、本システムと直接的に接続する連携システムは存在しないものの、本システムから出力した情報（応札情報等）を約定処理ツールに読み込ませる、また、約定処理ツールから出力した情報（オークション結果情報等）を本システムに取り込む等のファイル間での連携は存在する。

## 4. 非機能要件の定義

### 4.1. ユーザビリティ及びアクセシビリティに関する事項

#### 4.1.1. ユーザビリティ要件

ユーザの操作性を考慮した設計・開発を行うこと。詳細は、「3.2.2. 画面設計要件」及び「3.3.2. 帳

票設計要件」を参照すること。

#### 4.1.2. アクセシビリティ要件

ユーザにとって操作しやすく、誤操作が生じないシステムを構築すること。

### 4.2. システム方式に関する事項

#### 4.2.1. 情報システムの構成に関する全体の方針

本システムの構成に関する全体方針を以下に示す。

表 4-1：全体方針

No	全体方針の分類	全体方針
1	システムアーキテクチャー	・本システムのシステムアーキテクチャーは、Web アプリケーションシステムとすること。
2	アプリケーションプログラムの設計方針	・本システムを構成する各コンポーネント（ソフトウェアの機能を特定単位で分割したまとまり）間の疎結合化、再利用性の確保を基本とすること。
3	システム基盤の方針	・柔軟で拡張性の高さを考慮しクラウドサービスの利用を基本とすること。 ・受託者以外の者であっても同様のサービスを一般的な手段で調達することが可能であること。
4	ソフトウェア製品の活用方針	・受託者以外の者であっても市場等一般的な手段で調達することが可能である製品であること。 ・利用するソフトウェアは、サポート期間を考慮して選定し、当該ソフトウェアを提供する事業者（以下、「ソフトウェアベンダー」という。）によるサポート又は他の事業者によるサポートサービスの提供を必須とする。

#### 4.2.2. 情報システムの全体構成

本システムの全体構成について「別紙8. 全体システム概要図」を参照のこと。

#### 4.2.3. 開発方式及び開発手法

本システムの開発手法は、ウォーターフォール型を基本とすること。

### 4.3. 規模に関する事項

規模については、「別紙 3. 業務量定義書」を参照すること。

### 4.4. 性能に関する事項

性能に関する要件を以下に示す。当該要件を満たすことができない処理がある場合には、設計・開発期間において、受託者とその根拠・考え方を提示し、本機関と協議のうえ承認を得ること。

#### 4.4.1. 応答時間

表 4-2： 応答時間

No	項目	内容
1	オンラインレスポンスタイム	・ 検索、参照、登録、更新及び削除に係る処理については、業務の繁忙期においても平均処理応答時間3秒以内を実現可能とすること。なお、過剰な設備投資にならないよう配慮すること。 ・ 但し、縮退運転時はこの限りではない。
2	バッチレスポンスタイム	・ 日次で処理を完了すること。 ・ オンライン業務（平日 9 時～18 時）への影響がでないよう処理を完了すること。

#### 4.5. 信頼性に関する事項

本システムは容量市場における電源情報管理や応札情報管理を行うことから、滞りのない安定運用が求められる。これを踏まえ、システムの構築・運用・保守において、十分な信頼性の確保に努めること。

##### 4.5.1. 可用性要件

可用性に係る指標は、「稼働率」として目標値を99%とする。ただし、本機関と事前に合意した時間帯で実施するパッチ適用等の計画的な作業に伴う停止時間は、稼働率の算出対象には含めないこととする。

##### 4.5.2. 完全性要件

- ・ 機器の故障に起因するデータの滅失や改変を防止する対策を講ずること。
- ・ 異常な入力や処理を検出し、これらによるデータの滅失や改変を防止する対策を講ずること。
- ・ 処理の結果を検証可能とするため、ログ等の証跡を残すこと。
- ・ データの複製や移動を行う際にその内容が毀損した場合でも、毀損したデータ及び毀損していないデータを特定するための措置を行うこと。

#### 4.6. 拡張性に関する事項

以下の事項を考慮し、大幅な改修をしなくとも対応可能な、柔軟性・拡張性を有すること。

- ・ 再生可能エネルギーの固定価格買取制度対象電源の期間満了に伴う電源情報の増加
- ・ 本システムのユーザの増加
- ・ 本システムで取り扱う業務量・データ量の増加
- ・ 管理する情報項目の追加・削除

#### 4.7. 上位互換性に関する事項

以下の事項を考慮すること。

- ・ 応札時点において、OS、ソフトウェア等のバージョンアップ情報が公開されている場合、バージョンアップに対応できるように構築すること。
- ・ 契約期間中のバージョンアップは、影響範囲を調査し、その対応方針を本機関に報告すること。また、バージョンアップについて、技術的な問題等がある場合は、本機関と協議すること。

#### 4.8. 中立性に関する事項

特定の事業者、製品、技術等に依存することなく、システム拡張時、あるいは次期更改時等において、他の事業者等に必要な情報を、支障なく引継ぐことが可能なシステム構成とすること。

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

#### 4.9. 継続性に関する事項

##### 4.9.1. 継続性に関する目標値

大規模災害（地震、火災及び風水害等又は第三者による本システムへの攻撃時による直接的な設備及びシステムの損壊、あるいは、ライフライン（電力、通信及び交通等）の機能不全による本システムの長時間停止）が発生した場合を除いて、本システムを用いた業務処理が維持できること。

継続性に関する指標及び目標値は以下のとおりとする。

表 4-3：継続性に関する目標値

No	指標名	目標値
1	目標復旧地点（RPO）	・ 1 日前時点
2	目標復旧時間（RTO）	・ 12 時間以内

##### 4.9.2. 継続性に係る対策

災害・事故発生時においても、本システムを用いた事業継続に支障をきたすことのないよう、業務上重要なデータ、並びにシステム稼働に必要なデータの障害に備え、主に以下のデータをバックアップ対象とする。詳細は設計工程にて確定するものとする。

なお、バックアップは、定期的に自動バックアップを行うこととし、可能な限り統合管理が可能なバックアップソフトウェアにてバックアップを行うこと。また、バックアップデータの取得は、業務に支障を与えない夜間や、休日等に自動で取得できるように構築すること。

また、業務関連データ等の重要情報のバックアップはデータを暗号化した上で実施すること。

表 4-4：バックアップ対象と設定内容

No	バックアップ対象	バックアップの設定
1	システム環境設定情報	2 世代（システム環境変更時）
2	各種ログ情報	日次データを半年分

No	バックアップ対象	バックアップの設定
3	業務関連情報	日次/週次（日次は差分バックアップ、週次はフルバックアップ） 2世代分

#### 4.10. 情報セキュリティに関する事項

##### 4.10.1. 基本事項

受託者においては、以下に示す情報セキュリティ要件を満たすことができるよう、本システムに用いるアプリケーションプログラムの設計・開発を行うこと。

##### 4.10.2. 権限要件

本システムで用いるデータへのアクセスコントロールの要件は以下を想定しているが詳細は設計工程で確定する。なお、今後、新たな区分が必要となった場合に機能毎に利用可否を設定できるようにすること。

表 4-5：想定している権限表

No	区分	内容
1	広域機関管理者ユーザ	重要情報等を含め全ての情報にアクセス可能なユーザ
2	広域機関一般ユーザ	重要情報等へのアクセスは不可とし、必要最小限の情報へのみアクセスが可能なユーザ
3	事業者管理者ユーザ	事業者が利用する一般ユーザの作成及び自事業者の全ての情報へのアクセスが可能なユーザ
4	事業者一般ユーザ	自事業者の情報へのアクセスが可能なユーザ

##### 4.10.3. 情報セキュリティ対策要件

###### 4.10.3.1. セキュリティ機能

###### 4.10.3.1.1. 主体認証機能

- ・本機関が指定する電子証明書（本機関の他の情報システムで利用中の電子証明書）を用いて、事業者を識別するための主体認証機能を導入すること。なお、認証機能は連携する別サイトとして外部に切り出して構築することも可能とするが、その場合には相互のサイト間はSAML連携とすること。
- ・事業者の中においてユーザを識別するため、ユーザ毎にID、パスワードを付与すること。
- ・ユーザのID、パスワード認証等による認証の機能を設けること。
- ・ログイン時のパスワードはマスク表示すること。
- ・ユーザのパスワード等の情報を暗号化して保存する機能を設けること。
- ・ユーザが自らのパスワードを変更できる機能を設けること。
- ・パスワードについては、文字数及び使用する文字の種類を制限する設定ができること。
- ・管理者権限をもつユーザ（以下、「システム管理者」という。）が最終パスワード変更日を確認できる機能を設けること。

- ・パスワード等を他者に使用された場合又はその危険が発生した場合に、直ちにパスワード等による主体認証を停止する機能を設けること。
- ・不正ログイン行為を検知又は防止する機能として、パスワードの誤入力に複数回検知された場合に、当該IDによる本システムへのログインを無効にする機能を設けること。その際、検知の回数によるログインの無効化を可能とすること。また、無効になったIDの無効状態を解除することができる機能を設けること。
- ・パスワード等が他者に使用された場合又はその危険が発生した場合に、そのユーザが使用していたパスワードの変更等をシステム管理者が行うことができる機能を設けること。

#### 4.10.3.1.2. 通信の暗号化機能

- ・ネットワーク上の通信の暗号化を実施することにより、盗聴・漏えい等の技術的な脅威に対し、システムの機密性を確保すること。

#### 4.10.3.1.3. データの暗号化機能

- ・応札情報等の重要情報の秘匿を保持し、重要情報等への不正アクセス及び改ざんができないよう、暗号化すること。
- ・暗号化の対象範囲は、少なくとも項目単位で設定できること。
- ・暗号化に使用するアルゴリズムは、原則として「電子政府推奨暗号リスト」に記載されているものの中から選択すること。

#### 4.10.3.1.4. データ・マスキング（匿名化）機能

- ・応札情報等の重要情報等については、画面を盗聴されても知ることができないよう項目単位でマスキングできること。

#### 4.10.3.1.5. ウィルス対策機能

- ・ウィルス対策として、ウィルスチェックパターンファイル（以下「パターンファイル」という。）は常に最新にすること。
- ・パターンファイルの更新については、ソフトウェアベンダー等において、パターンファイルが公開された時点で、迅速に本システムに適用できる仕組みを構築すること。また、ユーザ及び本機関職員の作業負担のない方法を実現すること。
- ・ウィルス検出時は、本機関職員に電子メール等で日本語（ウィルス名等を除き）により通知すること。
- ・ウィルススキャンの実施頻度は、1日に1回以上とすること。

#### 4.10.3.1.6. ログ管理機能

- ・本システムへの不正操作を監視し、各種証跡ログから情報漏えい時に迅速に対応できるよう、原則として、次のログ情報を取得可能とすること。なお、ログ管理機能に求める要件は、「4.15.4. ログ管理要件」を参照すること。

表 4-6：ログ取得情報

No	ログ情報
1	ログイン・ログアウト等の事象を発生させる主体となるユーザ又は機器の識別コード
2	事象の種類（ログイン・ログアウト、ファイルへのアクセス、アプリケーションプログラムへのアクセス、起動等）
3	事象の対象（アクセスしたファイル、アクセスしたアプリケーションプログラム、機器等操作指令の対象等）
4	日付及び時刻
5	事象の結果（成功、失敗、エラー等）

#### 4.10.3.2. 脆弱性対策の実施

##### 4.10.3.2.1. 脆弱性情報の提供

- ・本システムに導入されるOSもしくはソフトウェア（ファームウェア、ウイルス対策ソフトウェア等）の脆弱性情報がソフトウェアベンダー等から公表された場合、影響分析結果を基に本システムにおける緊急度を判断し、本機関職員に報告すること。
- ・提供する脆弱性情報は、原則、日本語による情報であること。

##### 4.10.3.2.2. 脆弱性の影響度の判断

- ・セキュリティパッチが対応している脆弱性に対する影響度の判断は、深刻度、脆弱性の影響、影響を受ける対象等の脆弱性情報に基づき行うこと。

##### 4.10.3.2.3. 脆弱性検査

- ・第三者による脆弱性検査を実施し、その結果を本機関に書面にて報告すること。
- ・なお、本機関主導での脆弱性検査を定期的実施することから、受託者は協力すること。

##### 4.10.3.2.4. セキュリティパッチ適用

- ・セキュリティパッチ適用により、本システムの正常稼働に影響がないことを確認するため、スケジュール、環境、要員、手順等を定めた検証作業計画を策定すること。
- ・検証の結果、回避できない影響がある場合は、ソフトウェアベンダー等の提供する代替策を検証すること。また、OSもしくはソフトウェアの設定ファイルの変更等による対応可能な方法があれば、設定ファイル及び手順を作成し、検証すること。
- ・本システムの運用に影響を与えないために、スケジュール、要員及び手順等を定めたセキュリティパッチ適用計画を策定すること。

- ・必要に応じて、再起動を要すること等を事前にユーザ等の関係者に周知すること。

#### 4.10.3.3. 情報セキュリティが侵害された場合の対策

本調達に係る業務の遂行において情報セキュリティが侵害され又はその恐れがある場合には、速やかに本機関に報告すること。これに該当する場合には、以下の事象を含む。

- ・受託者に提供し、又は受託者によるアクセスを認める本機関の情報の外部への漏えい及び目的外利用
- ・受託者による本機関のその他の情報へのアクセス

#### 4.10.3.4. 情報セキュリティ対策の履行状況の報告

本業務の遂行におけるセキュリティ対策の履行状況について、本機関から報告を求めた場合には速やかに提出すること。

#### 4.10.3.5. 情報セキュリティ監査への対応

本機関が第三者機関等による情報セキュリティ監査を受ける場合には、受託者はその監査の実施について本機関の求めに応じ支援すること。情報セキュリティ監査の結果、対策が必要な場合は、本機関と協議を行い、合意した対策を実施すること。

#### 4.10.3.6. 情報セキュリティ対策の履行が不十分な場合の対処

本業務の遂行において、受託者における情報セキュリティ対策の履行が不十分であると認められる場合には、受託者は、本機関の求めに応じ、本機関と協議の上、合意したセキュリティ対策を実施すること。

### 4.11. 情報システム稼働環境に関する事項

#### 4.11.1. 基本要件

- ・情報資産（有形、無形を問わず本システムに含まれる情報とし、帳票、記憶媒体、電気通信等で伝達される情報等を含むものとする。）を管理するデータセンタの物理的所在地が日本国内にあること。また、継続性の観点から、日本国内で地理的に分散管理することが望ましい。
- ・本機関の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。
- ・情報資産の所有権は本機関であること。
- ・クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を第一審の専属的合意管轄裁判所とするものであること。
- ・情報資産が何らかの形で残留して外部に漏えいすることがないよう、必要な措置を講じること。
- ・クラウドサービスの提供に関して、セキュリティに関する認証（ISO/IEC 27017:2015、CS マーク（ゴールド）【クラウドセキュリティ推進協議会（日本セキュリティ監査協会の下部組織）が提供するクラウド情報セキュリティ監査制度】等）を取得していることが望ましい。
- ・本システムのドメイン名の登録先（DNS サーバ）は本機関所有のものに登録する。
- ・本システムの名前解決手段については、受託者の責任と負担において用意すること。

#### 4.11.2. 構築すべき環境

- ・ユーザが業務で用いる本番環境、ユーザがテストを行うための検証環境、及び受託者が開発を行う開発環境を用意すること。

#### 4.11.3. 保守端末・監視端末要件

- ・本システムに関するシステム障害（以下、「障害」という。）の解析、対応作業及び運用監視業務等を円滑に進めるため、保守拠点に、障害発生時の証跡取得等に用いる保守端末及び稼働状況の監視等に用いる監視端末を導入すること。
- ・本システムで作成された帳票等の確認、及び前述の障害解析・運用作業に係る証跡等の作成を行うため、Microsoft Word（バージョン2013以降）及びMicrosoft Excel（バージョン2013以降）形式のファイルを参照・編集が可能な仕組みを構築すること。
- ・PDF形式（バージョン1.5以上）で作成されたファイルが表示可能な仕組みを構築すること。
- ・作業時の可搬性や電源特性を考慮し、バッテリー稼働可能なノート型PCとすること。また端末をケーブル等で固定するためのセキュリティロック用ケーブルスロットを有すること。
- ・不正な持ち出し防止のため、保守端末及び監視端末はセキュリティロック用ケーブルで固定すること。

#### 4.11.4. 保守拠点の要件

- ・保守端末、監視端末等の機器は本番環境に接続すること。なお、接続に用いる回線は、受託者の責任と負担において用意することとし、IPアドレスによるアクセス制限等の適切なセキュリティ対策を施すこと。
- ・保守拠点は、受託者の責任と負担において用意すること。
- ・保守拠点のセキュリティ対策について本機関と協議し合意を得ること。

#### 4.11.5. クライアント環境要件

クライアントの環境要件として、少なくとも以下のブラウザに対応すること。なお、スマートフォン、タブレット端末等のモバイル端末については個別の対応は不要とする。

- ・Microsoft Edge（Windows10のリリース時同梱バージョン）
- ・Internet Explorer 11（Windows8.1, Windows10のリリース時同梱バージョン）
- ・Google Chromeの最新安定バージョン

### 4.12. テストに関する事項

#### 4.12.1. テスト工程共通要件

- ・受託者は、本業務で行うテストの環境及び手順に関して計画書（以下、「テスト計画書」という。）を定め、テストを実施し、その実施結果及び成果物の品質に責任を負うこと。
- ・テスト計画書の策定に当たっては、本機関職員の作業負荷の軽減に配慮すること。
- ・テストに使用する環境、ツール等については、受託者において用意すること。

#### 4.12.2. テストデータ要件

- ・テストに用いるデータは、原則として、受託者にて用意すること。
- ・テストに用いるデータは、受託者にて管理を実施しセキュリティを担保すること。

#### 4.12.3. 単体テスト要件

- ・単体テストは、「4.12.1. テスト工程共通要件」に示す要件に従って実施すること。

#### 4.12.4. 結合テスト要件

- ・結合テストは、「4.12.1. テスト工程共通要件」に示す要件に従って実施すること。
- ・機能間結合テスト、サブシステム間結合テスト等のテスト区分を設け、段階的にプログラムを結合することにより、品質を確保すること。

#### 4.12.5. 総合テスト要件

- ・総合テストは、「4.12.1. テスト工程共通要件」に示す要件に従って実施すること。
- ・本システムが本書に定めるシステム要件どおりに機能し、本番環境でユーザが行う業務運用（以下、「本番運用」という。）において、業務要件を満たすことを確認すること。
- ・システム要件の充足性の確認に当たっては、本書又は本業務の受託後に受託者にて実施する設計業務において作成したテスト仕様書に沿って、テストを実施すること。
- ・総合テストでは、一連の業務の流れ及び季節性サイクルに即したテストシナリオに基づき業務運用における機能性を確認するテスト（以下、「機能性テスト」という。）の他に、非機能性の確認として以下のテストを実施すること。

表 4-7：総合テスト実施項目

No	項目	内容
1	性能・負荷テスト	・性能に係る要件（応答時間等）に適合しているか確認する。 ・想定される負荷をかけ正常に機能するかを確認する。
2	信頼性テスト	・信頼性に関する事項に適合しているか確認する。 ・ソフトウェア、ハードウェア、回線等について、障害発生時の処理を確認する。
3	セキュリティテスト	・セキュリティ要件（主体認証、ウイルス対策、暗号化、ログ管理等）に適合しているか確認する。
4	運用テスト	・機能性テストの実施を通じて、動作等の非機能要件で問題ないか総合的に確認する。

#### 4.12.6. 受入テスト支援要件

- ・受入テストは本機関が主体となって行うが、本機関の求めに応じて受入テストをサポートするための体制を確保すること。
- ・受入テストで必要となるテストデータについては、受託者が本機関からの依頼内容を基に用意

すること。

- ・受託者は、受入テストで確認された障害について、解析を行い、原因及び対応方針案を提示すること。
- ・受託者は、上記の提示に基づき本機関が決定した障害についての対応方針に従い、プログラム及びドキュメントを修正すること。

#### 4.12.7. 参加者テスト支援要件

- ・参加者テストは本機関が主体となり、本システムを利用する事業者の協力をもって行うが、本機関の求めに応じて参加者テストをサポートするための体制を確保すること。
- ・受託者は、参加者テストで確認された障害について、解析を行い、原因及び対応方針案を提示すること。
- ・受託者は、上記の提示に基づき本機関が決定した障害についての対応方針に従い、プログラム及びドキュメントを修正すること。

#### 4.13. 移行に関する事項

本システムは、新たにシステムを構築し導入するため、既存システムからの移行データはないものとする。

なお、本番稼働を迎えるにあたり、システム稼働に必要な初期データの設定や本番環境で実施したテストデータの削除等の作業は発生する。

また、段階的な機能利用等により、本システム内での移行作業が必要な場合においては、受託者の責任で実施すること。

#### 4.14. 教育に関する事項

本システムを利用する事業者及び本機関職員（以下、「研修対象者」に対し、以下の要件に基づき教育を実施すること

- ・集合研修は、本機関が指定する場所にて実施すること。
- ・受託者は、教育に必要な機器及びソフトウェアを用意し、集合研修に必要なシステム環境（以下、「研修環境」という。）を構築すること。
- ・研修環境で使用する環境、ツール等は、原則、受入テストで検証が完了したものとすること。（研修環境はテスト環境とは独立して使用できること。）
- ・研修環境で使用するデータは、受託者が集合研修向けに作成したテストデータを準備し利用するものとし、本番環境で用いるデータを使用しないこと。
- ・研修対象者への教育に関しては、主として本機関にて実施するが、集合研修に必要な説明資料やマニュアル等の研修資料類の作成にあたり、受託者は本機関と協議し支援を行うこと。なお、研修資料類は各フェーズの稼働の2か月前を目途に準備すること。

表 4-8：教育に関する事項

No	教育対象者の範囲	教育内容	教育の実施時期	教育方法	対象者数
1	本機関職員	・システムの概要、操作方法	・本システム稼働開始前	・研修資料類を用いた集合研修 ・複数回に分けて研修を実施することも可とする。	・約 20 名
2	本システムを利用する事業者	・システムの概要、操作方法	・本システム稼働開始前	・研修資料類を用いた集合研修 ・説明主体は本機関にて実施	・約 3,000 名

#### 4. 15. 運用に関する事項

##### 4. 15. 1. 基本事項

受託者は、本機関が本要件定義書で示す要件を踏まえ、運用及び保守に関わる詳細を定める「運用保守計画書」を作成し、運用保守期間を通じて必要に応じて計画の変更・修正等を実施するなど、適切に管理すること。

特に、本システムを構成するクラウド基盤、アプリケーションプログラム、ドキュメント等を常に最新状態に維持し、本システムの変更作業の実施における影響範囲の特定や障害発生時における影響分析、原因分析等の様々な場面で活用できるようにすること。

表 4-9：運用に関する事項

No	項目	内容
1	システム運用時間(通常)	・平日 9 時～18 時とする。(長期間の運用停止も可能)
2	システム運用時間(特定)	・通常と異なる運用時間となる特定日は存在しない。
3	緊急対応時間	・本機関が「緊急」と判断する障害発生時に、担当者間で連絡・対応が可能な時間は 24 時間 365 日とする。
4	運用負荷削減	・業務機能の起動・停止等、定期的に行う処理は自動化するが、ログの削除等、非定期に実行する処理は運用保守管理者が手動で実施することを想定している。

##### 4. 15. 2. 情報システムの操作・監視等要件

監視対象は、サーバ、ストレージ、ネットワーク、データベース、ソフトウェアパッケージ、ネットワーク機器、アプリケーションプログラム、ログ等として、システムが正常に動作するために

必要な以下の監視を行うものとする。

表 4-10：監視項目

No	監視項目	内容
1	死活監視	・監視対象サーバの状態を定期的に監視すること。
2	プロセス監視	・監視対象サーバ上のアプリケーションプログラム等のシステムの稼働に必須となる常駐プロセスを監視すること。
3	ジョブ監視	・ジョブ管理用のソフトウェアと連携し、障害の検知を目的とした監視をすること。
4	ネットワーク監視	・本番環境のネットワーク監視をすること。
5	ログ監視	・不正アクセス発生の有無の確認のため、アプリケーションプログラムのログの確認を、月に1回、実施すること。
6	リソース使用状況監視	・監視対象の各サーバの CPU、メモリの使用状況を監視すること。 ・監視対象の各サーバ、ストレージのディスク使用状況を監視すること。 ・リソースの使用状況について、あらかじめ定めた閾値を超えた場合に、自動的に検知できる仕組みを用意すること。
7	性能監視	・応答時間等の状況を監視すること。
8	情報セキュリティ監視	・不正侵入、不正アクセス、データ改ざんの有無等を監視すること。

#### 4. 15. 3. 運用サポート業務に係る要件

##### 4. 15. 3. 1. 運用サポート業務

運用サポート業務として、以下の業務を実施すること。

表 4-11：運用サポート業務

No	運用項目	内容
1	バッチジョブ運用	・バッチジョブの定期的な動作（スケジュール）を管理すること。 ・バッチジョブによるインシデントを検知した場合、速やかにインシデント、問題管理の作業フローに従い対応すること。
2	時刻同期	・外部システムやユーザからの問合せ等に対する時刻整合性を保つため、NTP サーバを利用して、時刻同期を実現すること。
3	セキュリティパッチ・ウィルスパターン適用	・開発元、販売元からサポートを確実に受けられる体制を確保すること。 ・セキュリティパッチ、ウィルスパターン適用に関する影響の調査、検証を実施し、本機関が適用を判断する上で必要な情報（技術的な問題等の有無を本機関が判断するための情報等）を提供すること。 ・OS、ファームウェア、ウィルス対策ソフトウェア等のセキュリティパッチ及びウィルスパターン適用を実施すること。

No	運用項目	内容
		<ul style="list-style-type: none"> <li>・変更のリリースに際しては、リリースが与える影響等を考慮し、本機関に必要な情報を周知すること。</li> </ul>
4	ヘルプデスク	<ul style="list-style-type: none"> <li>・本機関職員からの問合せ対応を行うこと。</li> <li>・原則電話で受け付けること。(本システムを利用する事業者からの問合せについては、本機関が一次窓口となり、原則直接のやりとりは発生しない。)</li> <li>・問合せ受付に必要となる機器、回線については、受託者において用意すること。</li> <li>・操作方法等の頻度の高い問合せについては、FAQとして分類・蓄積をし、問合せ対応の迅速化を図ること。</li> <li>・ヘルプデスクの開設時間帯は平日 9 時～17 時 40 分とすること。</li> </ul> <p>※想定業務量として月 5 件程度の問合せを想定している。</p>

#### 4.15.3.2. 留意事項

本システムの運用開始当初（特に初回のメインアクションが完了するまでの間）は、操作方法の問合せ等のヘルプデスク業務が多くなることが想定されることから、迅速に対応できるような体制を構築すること。

#### 4.15.4. ログ管理要件

本システム運用におけるセキュリティインシデント、不正操作、ハードウェア・ソフトウェアに障害が発生した際の原因究明（調査・分析）、システムの性能監視等に必要となるログを管理する仕組みを構築すること。なお、サーバのOSが出力するログの開示ができない等のクラウドサービス側の制約がある場合においては、少なくとも、原因究明等の結果の報告が可能であることをもって代替可能とする。

##### 4.15.4.1. ログ出力・蓄積・監視要件

- ・サーバ、アプリケーション等の各種ログを出力できること。
- ・出力したログは、一定期間、蓄積が可能であること。また、長期保存が必要なログについては、外部の電磁的記録媒体に保存が可能であること。
- ・ログの保管期間について、詳細は設計工程において確定するが、少なくとも不正監視に対するログ、及び重要情報に対するアクセスログは 5 年間保持するものとする。
- ・バックアップしたログを期間が経過した後も参照できるように、特定のソフトウェアに依存しない形式（テキスト形式等）でログの保存が可能であること。
- ・出力されるログを監視できること。
- ・ログ監視に必要なレポートが生成されること。
- ・情報システムセキュリティに関する利用者及び本機関職員が不当に消去、改ざん又はアクセスすることのないように、ログ情報を保存したファイルに適切なアクセス制御ができること。

#### 4.15.4.2. ログ収集要件

- ・監視対象の各サーバに散在するセキュリティログ及び監視ログをソフトウェアの機能や OS の機能等を利用して自動的に一括収集することが可能であること。
- ・収集対象のログについては、以下の収集対象ログ一覧を参照のこと。詳細は設計工程において確定することとする。

表 4-12：収集ログ一覧

No	ログ種別	内容
1	各種サーバログ	<ul style="list-style-type: none"><li>・サーバへのアクセスユーザ（ログイン、ログアウトしたユーザ）の情報等が特定できるログ（セキュリティ、イベントログ等）</li><li>・サーバの OS が出力するシステムログ、アプリケーションプログラムのログ</li></ul>
2	Web サーバアクセスログ	<ul style="list-style-type: none"><li>・Web サーバにアクセスがあった時刻、クライアント IP アドレス、ホスト IP アドレス、ポート番号、要求コマンド、ステータス等の情報が特定できるログ</li></ul>
3	データベースアクセスログ	<ul style="list-style-type: none"><li>・データベースへアクセスしたユーザを特定することが可能なログ</li></ul>
4	アプリケーションプログラムのログ	<ul style="list-style-type: none"><li>・アプリケーションプログラムを実行したユーザ及びその操作内容を特定することが可能なログ</li></ul>

- ・保守拠点の保守端末及び監視端末からログ収集の設定・ログ収集の操作ができること。
- ・収集したログを分析し、相互に関連付け、保管できること。
- ・収集したログの閲覧が可能であること。

#### 4.16. 保守に関する事項

##### 4.16.1. アプリケーションプログラムの保守

###### 4.16.1.1. 障害対応

- ・本システムに関わる障害連絡の受付、管理、異常検知のための監視を行うこと。
- ・障害の切り分け、原因分析及び対応方針の立案を行うこと。
- ・ウィルス検知時の対策を実施すること。
- ・各種報告（インシデント発生・対策結果及び最新のセキュリティ脆弱性情報結果及び、ウィルス対策実施結果について月次で報告、各種システムメンテナンスの実施連絡、実施計画、実施結果を実施時に本機関に報告）を行うこと。
- ・本機関からの指示に基づき、アプリケーションプログラムの修正を実施すること。

###### 4.16.1.2. 作業環境

- ・アプリケーションプログラムの修正やテストは、開発環境及び検証環境で実施すること。

#### 4.16.1.3. 保守時間

平日 9 時～17 時 40 分（但し、本機関が「緊急」と判断したインシデントについては 24 時間 365 日対応とする。）

#### 4.16.1.4. 留意事項

本システムが安定稼働したと本機関が判断するまでの間は、迅速な障害対応を行うことができる体制を構築すること。

以上

## 5. 附属文書

- 別紙1. 「業務概要設計書」
- 別紙2. 「業務詳細設計書」
- 別紙3. 「業務量定義書」
- 別紙4. 「機能一覧」
- 別紙5. 「主な画面一覧」
- 別紙6. 「主な帳票・ファイル一覧」
- 別紙7. 「主な情報・データ一覧」
- 別紙8. 「全体システム概要図」