仕 様 書

1　件名

1.1　固定資産管理システム運用保守業務

2　受託者の基本条件

2.1　本件の受託者は、次の要件を満たすこと。

2.1.1　Windows 系サーバ（Windows Server 2019）を使ったシステムの運用経験が 5 か年以上あり、5 件以上の業務経験があること。

2.1.2　受託者は、「ピー・シー・エー株式会社製の PCA 固定資産 DX」の導入及び運用業務の経験があること。

2.1.3　システム運用保守にかかるプロジェクト管理等の経験が 5 か年以上あり、5 件以上の業務経験を有すること。

3　契約期間について

3.1　契約期間は、令和８年４月１日から令和９年３月３１日までとする。

4　作業場所

4.1　システム運用保守作業場所は、当会が指定する場所とする。

5　本契約に含む業務について

5.1　PCA 固定資産 DX with SQL 10CAL PSS1 年

5.2　PCA オンサイトサービス（基本）年間（数量　1）

本システムの稼働トラブル、バージョンアップ等作業は、ピー・シー・エー株式会社が提供するサービスとする。

5.3　サーバ運用保守作業

「7　運用保守」のとおり。なお、サーバのハードウェア障害や破損等の対応は対象外とする。

6　サーバ機器について

6.1　本番環境で使用するサーバ環境は当会が提供する環境を利用すること。

6.2　詳細は、以下とする。

6.2.1　当会ネットワークは、ローカル接続とする。

6.2.2　クライアント端末（10 台）との接続とする。

6.2.3　サーバ機器に関する仕様は以下のとおりとする。

＜当システムのハードウェア情報は以下とおり＞

No.	項目		内容
1	本体	メーカー・機種	HITACHI・HA8000V ML30 Gen10
3		型名	TQ-X1D-P21543-B21
4		製造番号	SGH033XR4M
5	ディスプレイ装置	型名	GQ-DT7173U

6		製造番号	08143
7	OS		Microsoft Windows Server 2019 Standard
14	プロセッサ		intl® Xeon® E-2224 CPU @ 3.40GHz、 3408Mhz、4 個のコア、4 個のロジカルプロセッサ
22	インストール済みの物理メモリ（RAM）		8.00 GB
27	内蔵ディスク		形名：TQ-WNC-C8S06A 品名：RDX USB 3.0 Docking Station 容量：500GB

7　運用保守

7.1　可用性要件

7.1.1 本システムの業務時間は、原則、平日午前 9 時から午後 6 時とする。

ただし、繁忙期等では、上記時間帯以外でも使用することがある。

7.2　完全性要件（データのバックアップ及びデータ復旧）

7.3　機密性要件（第三者や権限のない利用者がデータ参照できないよう、アクセス制限を設定し、必要に応じて暗号化を図る）

7.4　継続性

7.5　正常なシステム運用に必要な保守を行うこと。

7.5.1 システムのバージョンアップ対応

7.5.2 OS の更新作業対応

7.5.3 ウイルス対策ソフトの更新作業

7.5.4 時刻同期の確認

7.6　システムに不具合が発生した時は、当会の担当職員と協議の上、対応すること。

7.7　バックアップは、別内蔵の HDD へ保存する設定とし、世代管理は当会と協議の上決定する。但し、システム機能に装備されている場合は活用も可能とする。

7.8　システムの運用上疑義が生じた場合は、システムの保守サービスのサポート専用窓口の他、可能な限り当会の担当職員に対して助言を行うこと。

7.9　サーバに異常が発生した場合は、速やかに当会の担当職員に報告すること。

7.10 対応時間は、原則、平日午前 10 時から午後 5 時の間とすること。なお、緊急時においては、翌営業日対応できる体制を整えること。

7.11 業務報告の内容は当会と事前に協議の上、必要に応じて対面、メール又は WEB 会議等で行うこと。

8　成果物について

8.1　作業が完了した後、次の書類を提出すること。

8.1.1 業務完了報告書（任意様式）

8.1.2 月次運用保守報告書

なお、内容については、当会と協議の上、決定するものとする。

9　遵守する法令等

9.1　法令等の遵守

9.1.1 「国家公務員共済組合連合会情報セキュリティの確保に関する規程」及び「情報セキュリティ対

策基準」（以下「当会セキュリティポリシー」という。）の内容を正しく理解し、遵守すること。
なお、当会セキュリティポリシーは非公表であるが、「政府機関等のサイバーセキュリティ対策のための統一基準（令和５年度版）」（令和５年７月４日サイバーセキュリティ戦略本部）に準拠しているので、必要に応じ参照すること。当会セキュリティポリシーの開示については、契約締結後、受託者が当会に守秘義務の誓約書を提出した際に開示する。

9.1.2 受託者は、本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、行政機関の保有する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。

9.2 情報セキュリティ管理

9.2.1 受託者は、以下を含む情報セキュリティ対策を実施すること。

9.2.2 当会から提供する情報の目的外利用を禁止すること。

9.2.3 本業務の実施にあたり、受託者又はその従業員、本調達の役務内容の一部を再委託する先、若しくはその他の者による意図せざる不正な変更が情報システムのハードウェアやソフトウェア等に加えられないための管理体制が整備されていること。

9.2.4 受託者の資本関係・役員等の情報、本業務の実施場所、本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供を行うこと。

9.2.5 情報セキュリティインシデントへの対処方法が確立されていること。

9.2.6 情報セキュリティ対策その他の契約の履行状況を定期的に確認し、当会へ報告すること。

9.2.7 情報セキュリティ対策の履行が不十分である場合、速やかに改善策を提出し、当会の承認を受けた上で実施すること。

9.2.8 当会が求めた場合に、速やかに情報セキュリティ監査を受入れること。

9.2.9 本調達の役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるように措置の実施を担保すること。

9.2.10 当会から要保護情報を受領する場合は、情報セキュリティに配慮した受領方法にて行うこと。

9.2.11 当会から受領した要保護情報が不要になった場合は、これを確実に返却、または抹消すること。

9.2.12 本業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに当会に報告すること。

9.2.13 当会が履行状況の確認にあたり必要があると判断したときは、受託者が直近に実施した情報セキュリティ監査結果を提示するか又は立ち入り監査に対応すること。

10 その他

10.1 当会では現在使用中の固定資産管理システムの更改作業を実施する予定である。本業務の受託者はシステム更改作業受託者からの要請に基づき、当会の承認を得たうえで、現行システムに関する必要情報を取りまとめ、提供すること。また、データ移行作業等、システム切替時はシステム更改業務受託者と連携し作業を実施すること。

10.2 本仕様書に記載されていない事項で疑義が生じた場合は、遅滞なく当会と協議の上、業務を遂行すること。

10.3 その他、本業務の遂行にあたっては、当会の指示に従うこと。

（担当：経理部契約課）