

仕 様 書

1 件 名

業務用コンピュータ機器等の賃貸借

2 納入・設置場所及び数量

納入・設置 場所	住 所	パーソナルコンピュータ種別・数量（台）		
		デスクトップ型	ノート型	計
緑化管理部 経営企画課	中区基町 4 番 4 1 号 中央公園ファミリープール内	2	2	4
安佐動物公園 管理課	安佐北区安佐町 大字動物園	4	3	7
安佐動物公園 飼育・展示課		—	1 5	1 5
植物公園 管理課	佐伯区倉重 三丁目 4 9 5 番地	3	4	7
植物公園 栽培・展示課		1	1	2
昆虫館	東区福田町字 藤ヶ丸 1 7 3 番地 森林公園内	1	1	2
合 計		1 1	2 6	3 7

3 賃貸借物件（パーソナルコンピュータ（以下「パソコン」という。）、周辺機器及びソフトウェア）

- (1) 別紙「機器等仕様書」の条件を満たすこと。
- (2) 賃貸借期間中における修理部品の供給が可能であること。

4 納入、設置、接続・設定

- (1) 各パソコンがインターネットに接続できるよう設定を行うとともに、設定内容を記載した書類を発注者に提出すること。
また、発注者は平成 2 6 年 3 月から新たに LAN システムを利用する予定としており、導入の際において、インターネットに接続できるよう再度設定を行うとともに、設定内容を記載した書類を発注者に提出すること。
- (2) e メールがすぐに利用ができるよう、各パソコンにアカウントの設定やアドレス帳の移行を行うこと。
- (3) 各パソコンに、利用可能なプリンタの設定を行うこと。
- (4) 基本ソフト (Windows) 及びウイルス対策ソフト (シマンテック Symantec Endpoint Protection)

のアップデートを自動実行できるように設定すること。

- (5) 発注者が平成25年9月30日まで利用するパソコン（以下「旧パソコン」という。）のデータを納入、設置するパソコンに移行すること。（旧パソコンごとに作成した「移行用フォルダ」の移行）
- (6) ソフトウェアは、インストール等を済ませ、動作確認を行うとともに、必要なユーザー登録を行うこと。
- (7) 平成26年3月からLANシステムの利用を開始することに伴うウイルス対策等のセキュリティについては、LANシステム一式の賃貸借契約書、仕様書の「別紙3 セキュリティ対策等」を考慮するとともに、必要に応じてLANシステム事業者の確認の上、設定等を行うこと。
- (8) 納入、設置、接続・設定を行う日程は、発注者と協議すること。

5 パソコン及び周辺機器の管理

受注者は、善良な管理者の注意をもってパソコン及び周辺機器（以下「機器」という。）を管理し、個々のパソコンに識別票（賃貸業者名、賃貸借期間、管理番号、IPアドレス、デフォルトゲートウェイ、故障時の連絡先等）を貼付すること。

6 納入期限

平成25年9月30日

7 賃貸借期間

平成25年10月1日から平成30年9月30日まで（60か月）

8 検査受領

接続・設定後、速やかに発注者の検査職員に報告し、検査職員立会いのうえ、検査を受けること。

9 保守内容及び保守体制

- (1) 受注者は、賃貸借期間中、機器及びソフトウェア（以下「機器等」という。）が正常に動作するよう必要な保守（修繕・交換等を含む。以下同じ。）を行うこと。
- (2) 受注者は保守に関する受付窓口を設けるものとする。受付時間は9時から17時まで（土曜日、日曜日及び祝日を含み、年末年始を除く。）とする。
- (3) 機器等に障害が発生し、復旧や修理等の依頼を受けたときは、直ちに専門技術者を派遣し、復旧や修理等の作業に着手し障害の切り分けを行うこと。

また、ネットワークの不具合に起因すると考えられる障害に対しても原因確認に努め、ネットワーク事業者と連絡を取り合うなどして復旧対応を行うこと。

なお、発注者が簡単な操作等を行うことにより復旧が可能であると、発注者又は受注者が判断できる場合には、電話対応によることができるものとする。

- (4) 復旧や修理等が必要となった場合、受注者は迅速に各種対応（機器等の設定、部品の交換・修理等）を行い、受付当日に復旧や修理等を行うものとする。（訪問修理を含む。）ただし、土曜日、日曜日及び祝日は、保守に関する受付のみとし、復旧や修理等を翌営業日に行うことができるものとする。また、やむを得ない事情により受付当日に復旧や修理が困難な場合は、速やかに発注者と協議を行い、発注者の指示に従うものとする。

- (5) 機器等に障害が発生し、復旧や修理等に日数を要し発注者の業務に支障が生じるときは、その期間中代替機を設置すること。
- (6) 次に掲げる事項を除き、保守に関する一切の経費（部品代、出張費及び技術料を含む。）は、受注者の負担とする。
 - ア 機器の清掃
 - イ バッテリーパックの交換
 - ウ 発注者の瑕疵により生じたことが明らかな障害の対応
- (7) 交換して不要となった部品等については、受注者が適正に廃棄処分するものとする。

10 機器等の撤去

- (1) 賃貸借期間満了後、受注者は、発注者と日程等を協議し、機器等を撤去するものとする。
- (2) 撤去する機器等に記録しているデータは、復元できないよう、発注者と協議の上、専用ソフトを利用するなど確実な方法で完全に消去するものとする。
- (3) 機器等の撤去の際、データを復元できないよう削除したことが確認できる書類を提出するものとする。
- (4) (1)から(3)の実施に係る一切の経費は、受注者が負担するものとする。

11 リース取引の会計処理に関する書類の提出

発注者が、公益法人会計基準（平成 20 年 4 月 11 日内閣府公益認定等委員会）による「財務諸表に対する注記」を作成するために必要となる内容を記載した書類を提出するものとする。

12 その他

本件に関する疑義が生じた場合、又は定めのない事項については、発注者と受注者が協議して定めるものとする。また、協議後に、受注者は協議録を作成し、発注者に提出するものとする。

機 器 等 仕 様 書

1 パソコン及び周辺機器の仕様

(1) パソコン（デスクトップ型） 11台

項 目	仕 様
①OS	Microsoft Windows 7 Professional（日本語 32bit） SP 1
②CPU	インテル Celeron プロセッサ-G1610 (2.60GHz) 相当以上であること。
③メモリ	2GB 以上であること。
④HDD	250GB 以上（内蔵型）であること。
⑤光学ドライブ	DVD-ROM ドライブ（内蔵型）を有すること。
⑥LAN ボード	1000BASE-T/100BASE-TX 対応(内蔵型)であること。
⑦インターフェース	USB2.0×4 以上 LAN (RJ-45) ×1 アナログ RGB (ミニ D-SUB 15 ピン) ×1
⑧キーボード	日本語キーボード(109A キー、JIS 配列準拠)であること。
⑨マウス	光学式ホイールマウス (USB 接続) であること。
⑩その他	リカバリデータディスクを添付すること。

(2) ディスプレイ 11台

項 目	仕 様
①パネルタイプ	17 型 (TFT カラー液晶) 以上であること。
②画素数	1280×1024 ドット以上であること。
③映像入力端子	アナログ RGB(ミニ D-Sub 15 ピン)

(3) パソコン (A4 ノート型) 26 台

項 目	仕 様
①OS	Microsoft Windows 7 Professional (日本語 32bit) SP 1
②CPU	インテル Celeron プロセッサ B830 (1.80GHz) 相当以上であること。
③メモリ	2GB 以上であること。
④HDD	250GB 以上 (内蔵型) であること。
⑤光学ドライブ	DVD-ROM ドライブ (内蔵型) を有すること。
⑥ディスプレイ・画素数	15 型以上、1,366×768 ドット 以上であること。
⑦LAN ボード	1000BASE-T/100BASE-TX 対応(内蔵型)であること。
⑧インターフェース	USB2.0×4 以上 LAN (RJ-45) ×1 アナログ RGB (ミニ D-SUB 15 ピン) ×1
⑨キーボード	日本語キーボード(86 キー、JIS 配列準拠)であること。
⑩マウス	光学式ホイールマウス (USB 接続) であること。
⑪その他	リカバリデータディスクを添付すること。

2 ソフトウェア

(1) アプリケーションソフト

次のアプリケーションソフトのインストールを行うこと。

- ・ Microsoft Office Personal 2013

(2) ウイルス対策ソフト

次のウイルス対策ソフトのインストールを行うこと。

- ・ シマンテック SymantecEndpointProtection (5年間の更新を含む)

別紙3 セキュリティ対策等

1 クライアントパソコンのウィルス対策管理

(1) ~~仮想サーバ仕様~~

~~ウィルス対策サーバの仕様のとおり~~

(2) ソフトウェア仕様

- ア 世界規模で展開されたウィルス解析機関を有し、ウィルス定義ファイルを1日1回以上更新する事が可能な環境及び機能を有していること。
- イ リアルタイムスキャン機能、スケジュールスキャン機能を有すること。スケジュールスキャンの設定を「日」、「週」、「月」単位で設定することが可能であること。
- ウ ヒューリスティック技術を搭載し、新種・亜種等の未知のウィルスも検出する機能を有すること。
- エ メモリ上に存在するウィルスに対しても検出する事が可能な機能を有すること。
- オ 定義ファイルで検知しないウィルスの場合、振る舞い挙動検知により、トロイの木馬、キローガーや未知のマルウェアの検出機能を有すること。
- カ 特定のアプリケーションの起動制御や外部デバイスの利用制限機能を有すること。
- キ ウィルス対策サーバから対象デバイスへ最新の定義ファイルを配信する機能を有すること。
- ク ダウンロードファイルに関するレピュテーション(評価)機能を有しており、評価によってダウンロードの可能/不可能を決定する事が出来ること。
- ケ シングルコンソール(統一管理ツール)で管理が可能なこと。
- コ ダウンロードをするファイルのマルウェアを検知し、世界規模で展開しているセキュリティ解析機関にて管理をしている脅威情報と同期を取り、感染を防止させる機能を有していること。
- サ ウィルス検出時、管理者宛てにメールで通知する機能を有すること。
- シ アンチウィルスの定義ファイルを更新する機能があり、インターネットを通じて入手する事が可能なこと。
- ス ウィルススキャンの状況、パソコン/サーバのウィルス定義ファイルの状態が、把握出来る機能を有すること。

2 スпам対策、ウィルス対策、URLフィルタリング対策

(1) ~~ハードウェア仕様~~

~~ファイアウォールの仕様のとおり~~

(2) 機能仕様(ウィルス対策)

- ア メール、Webアクセストラフィックへのウィルスチェック機能を有すること。
- イ ウィルスチェックのためのデータベースを持ち、自動更新がされること。

(3) 機能仕様(スパムメール対策)

- ア IPアドレスチェック、E-mailアドレスチェックやリバースDNSルックアップなど複数のアンチスパムフィルタを装備し、スパムの可能性があるメールをブロックする機能を有すること。

イ スпам検索するデータベースを有し、自動更新がされること。

(4) 機能仕様 (URL フィルタリング)

ア Web アクセス時の URL フィルタリング機能を有すること。

イ URL/IP レベルでリサーチされた Web コンテンツカテゴリーによる分類がなされ、フィルタリングできること。

ウ Web コンテンツカテゴリーの自動更新機能を有すること。

3 既知／未知の脅威への対応 (2台)【アプライアンスサーバ】

(1) ハードウェア仕様

ア CPU はインテル®Xeon®X3450(2.66GHz)相当以上のものを1個以上搭載した機能相当以上であること。

イ 8GB以上のメモリを搭載していること。

ウ ハードディスクは300GB以上を有すること。

(2) ソフトウェア仕様

ア 一定以上の期間/人数で評価を行った検知対象ファイルの評価に基づいた、疑わしいファイル/アプリケーションを検知出来る機能・振る舞い検知の機能を有すること。

イ 標的型攻撃対策として、定義ファイルで検知されず侵入してきたマルウェアに対して、ネットワーク的な観点でマルウェアを見つけ出すことができる機能を有すること (ボット、スパイウェアなど)。

ウ マルウェアとインターネット指令サイトとの通信を検知、ブロック可能であること。

エ 標的型攻撃の防御のために未知のマルウェアを含め、ウィルス/スパイウェアに感染しているパソコンをIPアドレスで特定し、その通信を監視、ボット通信の検知を行う機能を有していること。

オ 複数の通信ログを相関的に分析し検知が可能なエンジンを有していること。

カ 外部のマルウェアサイト及びインターネット指令サイトの情報を随時アップデートし通信を監視できること。

キ 悪意あるWebサイトの閲覧を検知し、ブロックする機能を有すること。

ク 外部Webサイトへのファイルのアップロードの監視が可能であること。

ケ P2P通信の検知が可能であること。

コ レポート機能を有し、各種インシデントを可視化出来る機能を有すること。

サ Spanポートに接続し、ネットワークのパフォーマンスに影響なく設置、運用が可能なこと。

シ ボットと疑われる通信が発生した際、問題解決に向けたサービスが提供されること。

4. クライアントパソコンのセキュリティ状況管理

(1) 基本要件

ア サービスの開発元は国内企業とし、国内で開発されたシステムで日本語化対応であること。

イ クラウドサービス (SaaS) による提供を行うこと。

ウ 管理者によるポリシー (設定情報) の配付、セキュリティ診断結果及び資産管理情報の収集が可能で、毎月の保守報告と合わせて、各共同利用団体に収集した情報の概要等について報告すること。

エ クライアントライセンスをクライアントパソコンの台数分準備すること。

オ クライアントパソコンの動作環境を確認し、動作環境が不十分な場合は、共同利用団体に対して必要な助言を行うこと。ただし、メモリーの増設等クライアントパソコンの動作環境に係る経費は、本契約に含まれない。

(2) 管理者機能

ア 日々の全体把握を管理者及び各共同利用団体が即座にできるよう、Web 上のワンビュー（1画面）で、セキュリティアラート情報、セキュリティポリシー遵守状況、棚卸し実施状況、機器稼働状況、ソフトウェアライセンス管理状況、電力使用容量、印刷状況が確認できる機能を有すること。

イ セキュリティ違反のクライアントは、ドリルダウン方式にてクライアント一覧と個別のクライアント状況が表示される機能を有すること。

ウ 管理者パソコンから各共同利用団体の拠点施設単位もしくは全クライアントに対し、一斉にポリシーの適用ができる機能を有すること。

(3) セキュリティ関連機能

ア ウィルス対策ソフトウェアのパターンファイルのチェックを行い、古い場合はクライアントにメッセージを表示し、最新化へ誘導する機能を有すること。

イ ウィルス対策ソフトウェアの最終スキャン日時をチェックし、管理者が指定した一定期間以上スキャンを実行していない場合は、警告を出す機能を有すること。

ウ Windows のパッチ適用のチェックを行い、古い場合はクライアントにメッセージを表示し、最新化へ誘導する機能を有すること。

エ Adobe Flash Player、Adobe Reader、Java Runtime Plugin のバージョンのチェックを行い、古い場合はクライアントにメッセージを表示し、最新化へ誘導する機能を有すること。

オ クライアントパソコンのログオンパスワード、スクリーンセーバーパスワード、ハードディスクパスワード、BIOS パスワードをチェックする機能を有し、スクリーンセーバ起動時間のチェックについても可能なこと。

カ 管理者が指定した利用禁止アプリケーションがクライアントにインストールされていないかどうかをチェックし、インストールしている場合は警告を出す機能を有すること。なお、利用禁止アプリケーションについては、受注者から履行期間までに利用禁止として指定するアプリケーション案を共同利用団体に提示すること。

キ 端末においてセキュリティ診断結果を表示することができ、違反項目を解決するためのガイドンスが表示されること。

(4) 利用制限

ア 管理者が許可していない USB メモリ等の USB 媒体の使用を禁止する機能を有すること。違反者には警告メッセージを表示し、管理者側にも通知できること。

(5) 資産管理

ア ハードウェア資産情報を自動的に収集する機能を有すること。自動収集の項目は以下のとおりとする。

- ・ CPU 関連（種別、クロック）

- ・ メモリ関連（物理、仮想）
- ・ パソコン関連（種別、型名、メーカー、製造番号）
- ・ ネットワーク関連（アダプタ名、IP アドレス、MAC アドレス、サブネットマスク、デフォルトゲートウェイ）
- ・ ハードディスク関連（全体容量、空き容量）

イ ソフトウェア資産情報を自動的に収集する機能を有すること。自動収集の項目は以下のとおりとする。

- ・ OS 名
- ・ サービスパック名
- ・ ウィルス対策ソフトウェア名
- ・ インストールソフトウェア名

ウ 資産管理情報を手動で追加できる機能を有すること。追加項目は、機器管理番号、登録日、導入責任者、購入形式、購入日、購入先、購入金額、リースまたはレンタル情報（開始日、終了日、取引先、経費、管理番号、契約番号）、管理部署、担当職員、使用部署、使用者、設置場所及び備考とする。

エ ソフトウェア情報と管理者が入力したソフトウェア(保有ライセンス) 情報を比較し、ソフトウェアライセンス数の利用状況を確認し、ライセンス違反をチェックする機能を有すること。

オ 任意のクライアントに対して、棚卸し指示を依頼することができ、棚卸し指示を受けたクライアントにおいて登録した棚卸し情報を管理者が確認できること。クライアントで登録が可能な情報には、「管理部門名」「担当職員」「棚卸し実施者名」「設置場所」「利用状況」が含まれること。