別紙１

特　記　仕　様　書

１　作業概要

（１）目的

東京都農林水産振興財団（以下、「財団」という。）では、グループウェアサーバ、ウイルス対策サーバ、ファイルサーバ等を財団内に設置し、基本 OS Microsoft Windows7 のクライアント端末を利用し、運用を行ってきた。

しかし、2020 年 1 月 Windows7 のサポート終了、資産管理ソフトや外部デバイス制御機能の未導入による情報セキュリティ対策の脆弱性、オンプレミス運用によるサーバダウンリスク等の課題を抱えている。

2019 年 11 月末に現行サーバ・PC 端末等、賃借機器の借入期間が終了することに伴い、これらの課題を解決するため、最適な OS 環境に移行し、情報セキュリティ対策を強化するとともに、IT 資産管理リスクや運用負荷の軽減を図る。

（２）業務内容

主な業務内容は以下のとおり。

・サーバ及び接続するクライアント端末を財団が指定する場所に設置して、新システムを稼動させるための各種設定作業を行う。
・クライアント端末の OS バージョンは、Microsoft Windows10 とする。機能アップデート等更新プログラムの配信、適用を制御するため、WSUS を導入して通信回線の圧迫を回避する。
・ウイルス対策サーバ等を最新のクラウドシステムへ移行し、サーバの運用リスクを軽減する。
・資産管理ソフトを導入し、各端末の台帳管理や外部デバイスの制御等セキュリティの強化を図る。
・新システムを安定的に稼働させるとともに、万が一の障害等に対する予防策及びその際の早期復旧のための運用保守等を適切に実施する。

表１　業務内容と役割分担

【凡例】◎：主担当、〇：支援

委託業務	内容	役割分担		
		財団	受託者	ネットワーク運用委託業者
プロジェクト管理	本プロジェクトの進捗管理、課題管理等		◎	
	定期的な報告会議の開催、議事録の作成等		◎	
	連携する他システムとの接続に係わる調整等		◎	〇
要件定義	要件定義書等の作成		◎	
影響調査	システム改修等における業務、システムへの影響調査		◎	〇

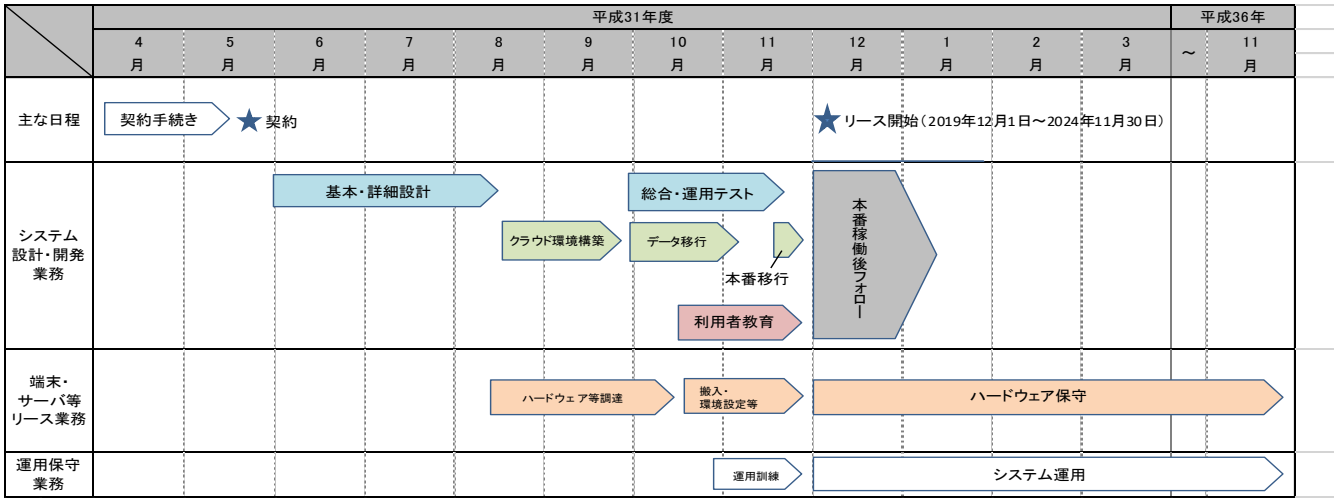
設計開発	現行システムに係る情報（設計書等）の提供		◎		
	基本設計、詳細設計			◎	
	開発（製造）			◎	
テスト	単体テスト、結合テスト			◎	
	総合テスト	機能、性能、障害要件等テスト		◎	○
		他システム連携テスト		◎	○
	受入テスト	受入テスト準備	◎	○	
		機能等の確認テスト	◎	○	○
	開発、テスト環境の構築			◎	
ハードウェア導入（ソフトウェア導入含む）	ハードウェア等（サーバ機器、OS、ミドルウェア等）構成案の作成			◎	
	導入するハードウェア等の設置（ソフトウェアインストール等含む）、各種設定			◎	
	導入機器等の動作確認			◎	
移行	移行設計、移行手順の作成等			◎	
	現行システムからのデータ抽出作業		◎	○	
	データ移行（サーバー等）			◎	
	データ移行（クライアントＰＣ）		◎	○	
	移行リハーサルの実施			◎	
	移行（新システムへの切り替え）			◎	
	移行確認テスト		◎	○	
教育訓練	研修実施計画等の策定			◎	
	関係者との調整		◎		
	研修実施、操作説明（システム管理者、IT リーダー等）			◎	

（３）スケジュール

各工程に要する期間について、ハードウェア調達や本番稼働時期等を考慮して、適切なスケジュールを提案すること。

なお、導入する機器等の借入期間は、平成 31 年（2019 年）12 月 1 日から平成 36 年（2024 年）11 月 30 日までとする。

図１　開発スケジュール



２　作業要件

（１）プロジェクト計画書の策定

業務全体のプロジェクト管理方法、体制、計画（作業ごとの詳細スケジュール含む）等を記載したプロジェクト計画書を契約締結後１週間以内に作成及び提出し、財団の承認を得ること。

（２）プロジェクト管理

１）進捗管理

各タスクの状況把握及びスケジュール管理を行うため、次の要件を満たす進捗管理を実施すること。

①作業工程ごとに必要な成果物、作業タスクを明確にすること。

②プロジェクトの進捗状況を管理する進捗管理表及び各作業タスクの進捗状況等を定量的に分析した報告書を定期的（月２回程度）に作成及び提出し、財団の承認を得ること。

③計画から遅れが生じた場合は、原因を調査し、要員追加や担当者変更等の体制見直しも考慮した改善策を提示し、財団の承認を得た上で、実施すること。

２）課題管理

プロジェクト遂行中に発生した各種課題を一元的に管理するため、次の要件を満たす課題管理を実施すること。

①課題の内容、発生日、優先度、解決予定日、担当者、対応状況、対応策、対応結果及び解決日等の情報を一元的に管理すること。

②定期的（月２回程度）に対応状況を確認及び報告し、課題の経過状況を財団と共有することで、迅速な解決に取り組むこと。

３）コミュニケーション管理

プロジェクトに係る全ての参画者が円滑かつ効率的なコミュニケーションを可能とするため、次の要件を満たすコミュニケーション管理を実施すること。

①作業工程ごとにおける各種作業に関する打合せ、成果物等のレビューのほか、進捗・課題等に関する報告を定期的に行う会議を開催すること。

②会議及び報告会等については、会議の内容、対象者及び開催頻度等を明確にすること。なお、会議の開催頻度等は、各作業工程の状況等を鑑みて、財団と協議の上、必要に応じて変更すること。

③会議及び報告会等が開催される都度、原則 3 営業日以内に議事録を提示し、財団の承認を得ること。

４）体制・要員管理

プロジェクト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ため、次の要件を満たす体制・要員管理を実施すること。

①適切に履行するための体制づくりと要員の確保を行うこと。

②作業工程ごと及び作業タスクごとに必要となるスキルに応じて、適切な知識及び経験を有した要員を配置すること。

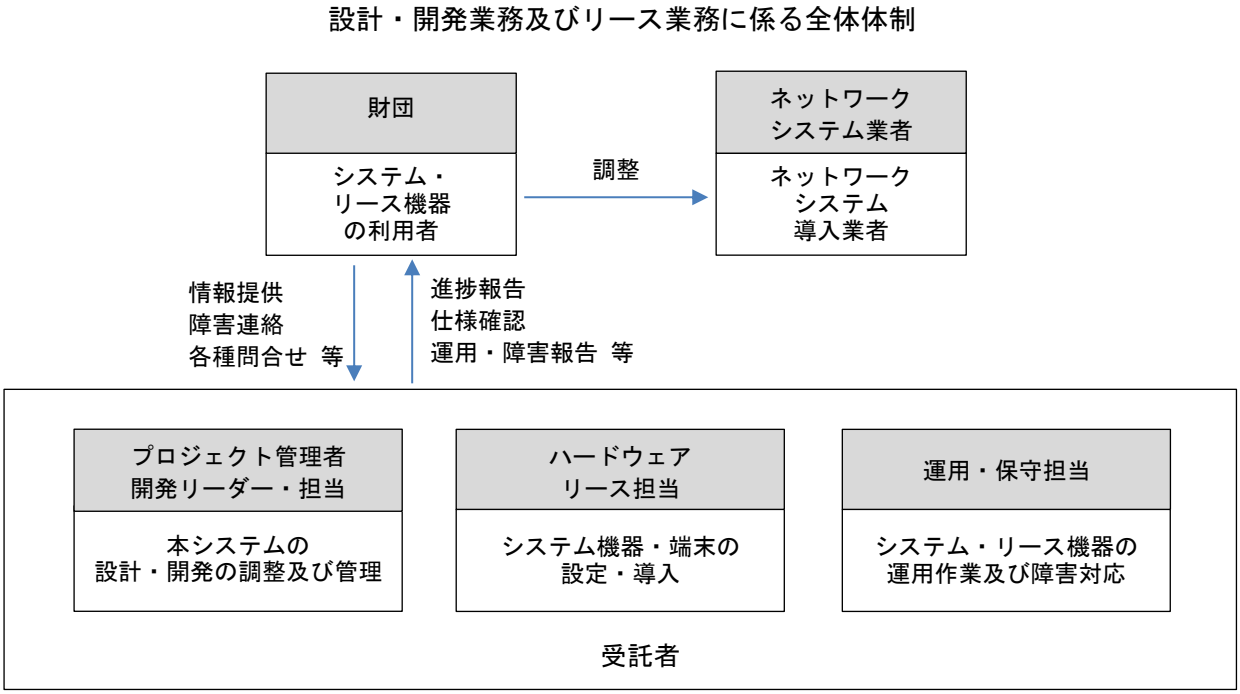
上記の中で、 成果物に相当すると考えられるドキュメントについては、財団と協議の上納入物件

一覧に加え、成果物とすること。

（３）作業体制

１）作業体制図

財団、受託者、及び新システムに係る関連事業者との関係は下図のとおり。



２）主要担当者に求める要件

①プロジェクト管理者の資格要件

プロジェクト管理者とは、プロジェクト全ての運営管理に係る責任を持つ者である。なお、プロジェクト管理者に求める要件として、次のいずれかを満たすこと。

ア　プロジェクト管理の実務経験を５年以上有すること。

イ　情報処理技術者試験のプロジェクトマネージャー、又はPMI（米国プロジェクトマネジメント協会）が認定するPMP（Project Management Professional）の資格、又はこれと同等の能力があること。

②開発リーダーの資格要件

開発リーダーとは、システムの設計・開発業務において、主体となって財団担当者と調整する者である。なお、開発リーダーに求める要件として、次のいずれかを満たすこと。

ア　設計・開発の実務経験を５年以上有すること。

イ　情報処理技術者試験の高度情報処理技術者（システムアーキテクト、ITサービスマネージャ、ネットワークスペシャリスト及びデータベーススペシャリストのいずれか）の資格、又はこれと同等の能力があること。

ウ　VMwareの資格（VCP以上）を取得済み、又はこれと同等の能力があること。

3　規模・システム利用環境

（1）利用者数

1）職員数　　約 320 名

2）クライアント端末数　　236 台

（2）全体構成

別紙２「システム全体構成図」のとおり

（3）各拠点の機器等導入

別紙３「機器等導入一覧」のとおり

（4）クラウド環境の構築（IaaS 環境）

現在、サーバ機器を立川庁舎内に設置しているが、サーバ運用管理コスト削減及び拡張性・安全性の強化を図るため、外部サーバ上にクラウド（IaaS）環境を構築する。主な IaaS サービス基盤要件は、以下のとおり。

1）IaaS 上に構築するサーバは以下のとおりとする。可能な場合は、複数のサーバ機能を一つのサーバに統合する構成でも可とし、ソフトウェアの動作に必要なスペック要件を満たしたサーバ環境を構築すること。

①ウイルス統合管理サーバ

②Active Directory サーバ（副）

③資産管理サーバ

④バックアップサーバ

2）システム要件に合わせて、仮想マシンのスペックを選択できること。また、オーバーコミット機能の有無を選択できること。

3）システムデータ用ディスクとして SSD を提供できること。また、柔軟に拡張できること。

4）1000 社以上の導入実績を有していること。

5）VMware を基盤としたクラウドサービスであること。

6）実績として月間 99.99%以上の稼働率であることとし、物理機器障害時には自動でフェイルオーバーするクラウドサービスであること。

7）クラウド上の SQL Server のライセンスを、コアライセンスまたはユーザライセンスより選択できること。

8）クラウド利用料の支払いは日本円とし、月額定額払いが可能であること。

9）自社グループのデータセンターで提供されるクラウドサービスであり、日本国内で運用され、首都圏データセンターのほか、DR サイトを首都圏から 600km 以上離れた場所にて運用していること。

10）24 時間 365 日の受付窓口やリモートメンテナンスによる障害原因特定など、OS 運用・復旧支援サービスが含まれること。

（５）ネットワーク環境

財団の閉域ネットワークは、回線事業者である NEC ネクサソリューションズの Clovernet を使用しており、各拠点のルータから Clovernet を介して、直接、IaaS 基盤へ VPN 接続する。各拠点の変更作業は、NEC ネクサソリューションズが行うものとする。

回線引き込み作業及びルータ・終端装置等については別途財団が手配するが、引き込みのためのデータセンター現地調査及び回線工事やルータ等機材の設置の際の立会等ができること。また、データセンターは複数回線、複数ルータによる冗長化ができるようにすることとし、ルータ及び終端装置を設置するためのラック内スペース、電源を用意すること。

想定する回線、装置等は以下のとおり。

１）回線

①光ネクスト　ファミリー　ギガラインタイプ

②光アクセス(UCOM)

２）ルータ及び終端装置

①UNIVERGE IX2016　２台　【19 インチラック取付棚(1U サイズ)上に 2 台横置き可】

筐体サイズ　135 ㎜（W）×196 ㎜（D）×36 ㎜（H）

電源容量　14VA(7W)

電源コンセント　１個

②終端装置(ONU)　１台　光ネクスト　ファミリー　ギガラインタイプ（NTT）

③終端装置(ONU)　１台　光アクセス(UCOM)

４　借入物品（端末）に係る要求仕様

（１）クライアント端末（ノート型）　　103 台

機　器	詳細
筐体（本体） （注：突起部含まず）	ノート型（A4 サイズ相当） 380 ㎜（W）×260 ㎜（D）×35 ㎜（H）以内
質量（本体）	2.5kg 以下
対応 OS	Microsoft Windows 10 Professional 64bit（正規版）
CPU	Core i3-7300 以上　第８世代でも可
メモリ	4GB 以上実装（4GB×１） 本体機器で動作保証のある製品であること。
表示装置	液晶フル HD　TFT カラー　15.6 インチ
解像度	1920×1080（フル HD）ドット以上
表示色数	1,677 万色　以上
ストレージ	SSD　128GB 以上
光学ドライブ	DVD が読み書きできること（内蔵）。
ポインティングデバイス	フラットポイントであること。

USB	3.0 以上準拠３ポート以上とする。 Type-C は１ポートまでとする。
インターフェース（USB を除く）	外部ディスプレイ端子×1 ポート以上（うち１ポートは HDMI 準拠）、LAN(RJ-45)×1、 ヘッドホン・ラインアウト端子×1、 マイク・ラインイン端子×1 （ヘッドホンとマイク端子はコンボジャック×１でも可）
通信	1000BASE-T/100BASE-TX/10BASE-T Wake On LAN 対応
オーディオ	スピーカー内蔵
電源	電源ケーブル及び AC アダプタ
消費電力	最大約 45W 以下であること。
マウス	USB 接続、光学式、ホイール機能付き 本体機器メーカー製の純正品とすること。 標準サイズであること。
キーボード	JIS 配列準拠日本語キーボード（内蔵）
テンキーボード	本体に内蔵されていること。 デスクトップ PC に近い 4 列テンキーであること。
バッテリー	本体に内蔵されていること バッテリーのみで約 9 時間以上駆動可能なこと（JEITA2.0 測定法準拠）。
盗難防止用ロック 取り付け穴	盗難防止用ロックと取り付け穴があること。
BIOS	パスワード保護が可能であること。

（２）クライアント端末（デスクトップ型）　　133 台

項　目	仕　様
筐体（本体）	省スペースデスクトップ（液晶一体型または一体化できること。） 65 ㎜（W）×200 ㎜（D）×200 ㎜（H）以内 （液晶一体型の場合、490 ㎜（W）×210 ㎜（D）×475 ㎜（H）以内）
質量（本体＋表示装置）	7.0kg 以下
対応 OS	Microsoft Windows 10　Pro　(64bit)　（日本語版）
ＣＰＵ	Core i3-7300 以上　第８世代でも可
メモリ	4GB 以上実装（4GB×１） 本体機器で動作保証のある製品であること。

表示装置	液晶フル HD　TFT カラー　21.5 型ワイド以上
解像度	1920×1080（フル HD）ドット以上
表示色数	1,677 万色以上
ストレージ	SSD　128GB 以上
光学ドライブ	DVD が読み書きできること（内蔵または一体化）。
ＵＳＢ	3.0 以上準拠４ポート以上とする。
インターフェース（ＵＳＢを除く）	DisplayPort(音声出力対応)×１ LAN(RJ-45)×1、 ヘッドホン・ラインアウト端子×1、 マイク・ラインイン端子×1 （ヘッドホンとマイク端子はコンボジャック×１でも可）
通信	1000BASE-T/100BASE-TX/10BASE-T Wake On LAN 対応
オーディオ	スピーカー内蔵
電源	内蔵電源
消費電力	約 20W 以下
マウス	USB 接続、光学式、ホイール機能付き 本体機器メーカー製の純正品とすること。 標準サイズであること。
キーボード	JIS 配列準拠日本語キーボード（テンキー付き） 原則として、本体機器メーカー製の純正品とすること。
キーボードケーブル	添付
盗難防止用ロック取り付け穴	あり
ＢＩＯＳ	パスワード保護が可能であること。

（3）クライアント端末（ノート型、デスクトップ型共通）

機　器	仕　様	数　量
統合オフィスソフト	Microsoft Office Standard 2016 (Government License)	177
	Microsoft Office ProPlus 2016 (Government License)	59
	統合オフィスソフトは、最新のサービスパックおよび最新のセキュリティ修正プログラムを適用し、インストールすること。 原則としてインストールした状態での納入とする	-

	が、別途財団が指定する端末については、プレインストールせずに納入すること。	
ウイルス対策ソフト	財団より別途提供するものを使用し、インストールすること。 ※財団所有端末（49 台相当）に対して、資産管理ソフトを用いて、ウイルス対策ソフトのインストール状況を確認し、アンインストール及びクラウド版への設定変更を行うこと。	－

（4）添付品

機　器	仕　様	数　量
セキュリティワイヤー	長さ：２m以内、太さ 4.0㎜ 以内	236
マスターキー	個別キーとは別にマスターキーを納品すること。	5
キーボードカバー	防水及び防塵に有効であること。 装着した状態でキー入力が可能であること。 原則として本体機器の専用製品であり、各キーの凹凸に沿った成形がされていること。 ただし、クライアント端末自体に防滴構造が採用されている場合はその限りではない。	

5　各端末に係る基本要件

（1）各機器は全て新品であること。ノート型端末とデスクトップ型端末（本体とディスプレイ）のメーカーは同一とし、機種は統一すること。

（2）国際エネルギースタープログラムの適合製品であること。

（3）JEITA「PC グリーンラベル制度」の審査基準を満たしていること。

（4）「グリーン購入法」（国等による環境物品等の調達の推進等に関する法律）に基づき定められている「環境物品等の調達の推進に関する基本方針」に記載されている判断の基準を満たしていること。

（5）ソフトウェア仕様で示すソフトウェアをインストールした状態で、正常に動作するものであること。ただし別に示す場合を除く。

（6）無線 LAN 装置、メモリーカードスロット、カメラ機能その他財団が不要と判断する機器及び機能については、未装着又は使用不可状態になっていること。

（7）付属する取扱説明書類は、設定時に電子データで端末本体に格納し、物品による納品は行わないこと。付属するメディア類については、システム管理者が必要とする最小限の枚数を納入すること。詳細については、契約締結後、財団担当者と協議すること。

（8）電源ケーブルその他必要なケーブル類を添付すること。

（9）デスクトップ PC はディスプレイとパソコン本体の電源が連動できること。

(10) デスクトップ PC とディスプレイを一体化した状態で、容易に電源を入れることができること。

また、容易に光学ドライブの取り出しが可能なこと。

(11) デスクトップ PC 本体とディスプレイを一体化した状態で USB 機器を容易に接続できること。USB ポートが背面のみの場合、USB 延長ケーブルなどで対応すること。

6　各端末に導入するソフトウェアに係る基本要件

（1）各ソフトウェアは、基本 OS　Windows10 に対応するものであること。

（2）ソフトウェアは原則としてライセンス調達を行うこと。その際、インストールメディアを添付すること。

（3）ライセンス登録を行う際に、販売店情報などの登録が可能な場合は、受託者の会社名・担当者名・電話番号等を登録すること。

（4）サイボウズ及びファイルサーバのショートカットアイコンを各端末のデスクトップ上に作成すること。

7　借入物品（サーバ）に係る要求仕様

（1）Active Directory サーバ

1）Active Directory 機能

現在、クライアント端末は Work Group での運用を行っているため、ユーザアカウント管理やソフトウェア一括インストールなどの管理を行うことができず、管理者の運用負荷となっている。そのため、本調達にて Active Directory サーバを新規導入し、ユーザアカウント管理を Active Directory にて行うこととする。

2）バックアップソフトウェア

①IaaS 上のバックアップ用ディスク領域にフルバックアップが取得できること。

②スケジュールによるバックアップが可能であること。

③ログ情報を１年以上保存すること。

3）正副の 2 台構成とすること。1 台（正）はオンプレミス運用で財団立川庁舎に設置し、もう 1 台（副）はクラウド基盤上のゲスト OS に構築すること。

4）ドメインを新規構築し、本調達にて導入するクライアント端末及び既存クライアント端末を構築したドメインの配下に置くこと。内訳は、【別紙 3】機器導入一覧を参照のこと。

5）Active Directory サーバのうち１台（正）については、以下の仕様を満たす物理サーバとすること。

機　器	詳細
筐体（本体）	EIA 規格　19 インチサーバラックに搭載できること。 ラック占有スペースは 1U 以内であること。
対応 OS	Microsoft Windows Server 2016、もしくは 2019 に対応すること。 導入バージョンは財団との協議の上、選択できること。
CPU	Xeon Silver 4110 2.1GHz 1P8C 以上であること。
メモリ	16GB 以上を搭載すること。
ハードディスク	SAS ディスクを搭載し、RAID１構成＋ホットスペア 1 個となるよう設定

	すること。 実効容量は 300GB 程度が使えること。 ディスク装置はホットスワップに対応すること。 ディスクドライブベイは 8 個以上を有し、必要に応じて空きベイにディスク装置を追加できること。
光学ドライブ	9.5mm SATA DVD-ROM ドライブを内蔵で有すること。
ネットワークインタフェース	ネットワークインタフェースは 1000BASE-T×4 ポート以上有すること。 管理用ポートは上記インタフェースとは別に 1 ポート以上有すること。
管理ポートおよび管理機能	サーバ管理専用のネットワークポートを 1 ポート以上備えること。 サーバ管理用ポートを経由して、グラフィック表示ができること。 リモートで電源の投入・遮断等の管理ができること。 サーバ管理機能はサーバ本体の CPU とは独立したチップセットで構成されていること、および OS とは独立して稼働すること。
外部インタフェース	モニター×2（背面 VGA×1、前面 Display Port×1 が望ましい） USB 2.0 準拠×1（前面 1 が望ましい） USB 3.0 準拠×5（背面 2、前面 1、内部 2 が望ましい）
異常検知機能	サーバ内の異常個所（メモリ・プロセッサ・ファン・LAN ポート）を本体外側の LED 等で表示し、直観的に目視できること。 本体内部を開けなくとも、外面から故障個所がわかるよう表示されることが望ましい。 障害及び障害予兆に対して、メール等でシステム管理者に通知する機能を有すること。 障害及び障害予兆に対して、サーバ管理機能により画面で通知・確認する機能を有すること。
電源	国際エネルギースタープログラム（ENERGY STAR）の認定を受けていること（80Plus が望ましい）。 100V 電源が利用でき、電源コードのプラグは NEMA 5-15P であること。 消費電力は 500W 以内であること。 電源ユニットは冗長化されており、無停止で稼働中に交換できること。
無停電電源装置	停電時に安全にシャットダウンできる容量の無停電電源装置を含むこと。 停電時には自動的に検知してサーバ機器に通知し、安全にシャットダウンできる機能を有すること。 無停電電源装置とサーバ機器はネットワーク経由で通信できること。 無停電電源装置は 100V/15A の商用電源が利用できること。 無停電電源装置の電源プラグ形状は NEMA 5-15P であること。 無停電電源装置は 1U 以内のラックマウント型であること。

（２）WSUS サーバ

１）WSUS(Windows Server Update Services)機能

①本調達にて導入するクライアント端末の Windows セキュリティ更新や推奨パッチの適用、サービスパックの導入を実施できること。

②各クライアント端末のパッチ適用状況を確認できること。

③資産管理ソフトと連携し、更新プログラムの管理スケジュールを設計・設定すること。

２）バックアップソフトウェア

①IaaS 上のバックアップ用ディスク領域にフルバックアップが取得できること。
ただし、配信されるパッチ部分は取らなくてもよい。

②スケジュールによるバックアップが可能であること。

③ログ情報を１年以上保存すること。

３）オンプレミス運用で財団立川庁舎に設置すること。

４）WSUS サーバについては、７（１）５）の Active Directory サーバ仕様を満たす物理サーバとすること。

ただし、ハードディスクについては以下の仕様とする。

・SAS ディスクを搭載し、RAID５構成＋ホットスペア１個となるよう設定すること。

・実効容量は 2400GB 程度が使えること。

・ディスク装置はホットスワップに対応すること。

・ディスクドライブベイは８個以上を有し、必要に応じて空きベイにディスク装置を追加できること。

（３）ウイルス対策統合管理サーバ

１）ウイルス対策統合管理ソフトウェア

①財団が提供する「ウイルスバスター　コーポレートエディション　Plus」を導入すること。

②バージョンは導入時点での最新版を導入すること。

２）バックアップソフトウェア

①IaaS 上のバックアップ用ディスク領域にフルバックアップが取得できること。

②スケジュールによるバックアップが可能であること。

３）クラウド基盤上のゲスト OS に構築すること。

４）財団が提供するウイルス対策統合ソフトウェアを用いて、ウイルス対策統合管理サーバ及び新規に導入するクライアント端末 236 台のインストール・設定を行うこと。また、財団所有端末（49 台相当（設置拠点は、【別紙 3】機器導入一覧を参照のこと。））に対して、資産管理ソフトを用いてウイルス対策統合管理ソフトウェアのインストール状況を確認し、アンインストール及び今回のウイルス対策統合管理サーバへの設定変更を行うこと。

（４）資産管理サーバ

１）資産管理ソフトウェア

IT 資産管理ソフトについては、参考機種として SKYSEA Client View Government License

Professional Edition 同等品以上の製品を選定し、必要なライセンス数（301 台を想定（内訳は、【別紙 3】機器導入一覧を参照のこと。））を受託者にて用意の上、システムを構築して、各端末にインストール、設定を行うこと。必要な機能は以下のとおりとする。

①IT セキュリティ対策強化

・アラート情報を syslog として他社製品へ送信できること。
・UTM と連携し、サイバー攻撃を早期把握できること。
・ウイルスを検知したクライアント端末をネットワーク遮断できること。
・特定（共有）フォルダへのアクセスを制限できること。
・ログから起動元プロセスを特定できること。

②ログ管理

・クライアント端末の操作ログを記録し、必要なデータを素早く抽出して確認できること。
・ネットワーク非接続のクライアント端末のログを収集できること。
・組織内のクライアント端末の外部との通信状況を把握できること。

③セキュリティ管理

・WSUS と連携し、更新プログラムを管理できること。
・Windows10 の自動アップデートを制御できること。
・クライアント端末の異常を検知して、管理者に通知できること。

④不許可端末の検知・遮断

・未登録の持ち込みクライアント端末からのアクセスを 24 時間遮断するハードウェア型の不許可端末検知・遮断アプライアンスを設置すること。アプライアンスは必要な VLAN ごとに設置すること。なお、VLAN 数は 10 とする。
・不正端末検知・遮断アプライアンスで取得した機器情報と資産管理ソフトの登録情報をそれぞれ反映し、管理画面での運用が可能なこと。
・自動連携が出来ない場合は、受託者にて資産管理ソフトの機器情報データベースと整合性が取れるよう、 定期的(週 1 回程度）および財団から依頼があった場合は手動にてデータベースのメンテナンスを行うこと。
・センサー動作時の許容周辺温度は 50℃まで対応可能であること。
・MAC アドレス登録以外（許可、ブロック）に、IP アドレス/MAC アドレス(頭 6 桁)/ベンダー名称に対して、許可、ブロックが出来ること。

⑤デバイス管理

・USB デバイス、メディアを台帳管理（使用制限、棚卸も可能）できること。
・紛失したデバイスの保存データをログ追跡できること。
・持ち込みデータを含むデバイスを接続禁止にできること。
・取り扱いファイルを暗号化できること。

⑥レポート

・ログデータをもとに、ログ解析レポート、資産レポート、傾向分析／注意表示レポート、経費節減レポート、資産・ログ利活用レポートライブラリを出力できること。

⑦資産管理

・クライアント端末ごとのハードウェア、ソフトウェア情報を自動収集して管理台帳を作成し、管理できること。
・資産管理ソフト未導入のクライアント端末情報も検出・管理できること。
・プリンター等の IT 機器情報を定期的に収集できること。
・WSUS と連携し、ソフトウェアを一斉配布、自動インストールできること。

⑧メンテナンス
・離れた場所にあるクライアント端末を、管理機からリモート操作できること。
・複数のクライアント端末へ管理機の操作を一斉転送できること。
・クライアント端末を遠隔制御（資料配布、電源制御等）できること。

2）バックアップソフトウェア
①IaaS 上のバックアップ用ディスク領域にフルバックアップが取得できること。
②スケジュールによるバックアップが可能であること。
③サーバ機器および IT 資産管理システムが収集するログ情報を１年以上保存すること。

3）クラウド基盤上のゲスト OS に構築すること。なお、他のソフトと共存させないこと。

（5）バックアップサーバ

1）バックアップソフトウェア（管理機能）
上記（2）～（4）のサーバについて、以下のバックアップを取得できること。
①各バックアップはシステムイメージを含めクラウド上のバックアップサーバで取得する。システムバックアップ用のオプションを入れること。
②クラウド上のサーバのシステムバックアップについては、バックアップサーバで定期的に取得すること。
③フルバックアップの取得タイミングは、納品前、システム構成変更時等とすること。
④データバックアップの取得タイミングは、基本的に毎日とし、詳細は設計時に決定すること。

2）クラウド基盤上のゲスト OS に構築すること。

8　サーバに係る設計及び設定

各サーバ（ウイルス統合管理、Active Directory（正・副）、資産管理、WSUS、バックアップ）に係る設計及び設定は以下のとおりとする。

（1）導入時の最新のセキュリティパッチを適用すること。
（2）設計書を作成し、財団に提出すること。
（3）設計書に基づき、サーバの設定、ソフトウェアのインストール・設定等を行うこと。
（4）クラウド環境については、（PING 結果／サーバステータス（停止）／CPU 使用率／メモリ使用率／ディスク使用率を監視し、予め設定した閾値を超過した場合はアラートメールを送信できること。
（5）サーバの定期バックアップに係る設計を行うこと。バックアップ失敗の際にはメールなどによる通知を行うこと。また、手動でのバックアップ及びリストア作業の手順書を作成すること。
（6）実施した設定について、設定値の確認と動作確認を行うための試験仕様書を作成し、試験を行う

こと。

（7）ウイルス対策ソフト（クライアント機能）等により、サーバのウイルス対策を講じること。

9　クライアント端末に係る設計および設定・試験

（1）ノート型・デスクトップ型それぞれ統合オフィスソフトごとに全４種類マスタ PC を作成すること。

（2）導入時、最新のセキュリティパッチを適用すること。

（3）設計書を作成し、財団に提出すること。

（4）グループウェア、ファイルサーバ、統合オフィスソフト、その他財団が別途指示するソフトウェアを導入すること。また、これらがクライアント端末で問題なく動作するよう構築すること。

（6）マスタ PC の動作について、試験を行うこと。特にインストールするソフトウェアとハードウ　ェアとの間で競合等の不具合が発生しないことを確認すること。また、試験結果報告書を作成し、財団に提出すること。

（7）マスタ PC の試験合格後、マスタディスクを作成すること。マスタディスク作成において、クライアント端末ごとに特定の値を取らなければならない IP アドレス・ホスト名などの項目を踏まえて実施すること。

（8）マスタディスクを元にリカバリディスクを作成し、リカバリ用マニュアルとあわせて財団に提出すること。また、リカバリディスクから実際にリカバリが行えることを確認するためのリカバリ試験を実施すること。

（9）リカバリ用マニュアルおよび設定用マニュアルは平易に実施可能なものとすること。

(10) 財団のネットワークに接続して作業を行う場合、必ず事前に財団担当者に報告し、作業の了承を得ること。

(11) 財団が保有するネットワークプリンタより印刷が行えるよう設定すること。なお、設定するプリンタの機種等については別途指示する。

10　クライアント端末のデータ移行

（1）現行クライアント端末から移行するデータは以下のものとする。

１）利用者作成データ

２）Internet Explorer のお気に入り

（2）上記（1）のデータ移行は財団の各職員にて行う。各職員がデータ移行を容易に行えるよう、下記の移行作業手順書を作成すること。

１）Windows 7 端末→Windows10 端末へのデータ移行

２）Windows10 端末→Windows10 端末へのデータ移行

（3）受託者は、データ移行作業がスムーズに行えるように移行前後のサポートを十分に行うこと。

11　設置

（1）サーバ、クライアント端末等を設置する日程について財団担当者と協議し、設定・設置等にかかる作業計画書を作成すること。

（２）機器の搬入・据付において、財団の施設及び設備に対して損害を与えることのないよう必要な措置を講じること。万一、損害を与えた場合は、受託者の負担で原状回復を行うこと。
なお、機器の撤去時においても同様の措置を講じること。
（３）機器等搬入時に生じる梱包資材等は、受託者の責任において持ち帰り処分すること。
（４）各拠点への搬入の際に、納品物の数量について現地担当職員の確認を得ること。
（５）調達するすべてのクライアント端末について、設定インストール作業を行い、PC・キーボード・マウスが正常に動作することを確認すること。また、インターネット・各サーバとの接続確認を実施すること。
（６）現行端末からクライアント端末への移行後、移行されたデータについて問題がないことを職員に確認すること。
（７）設置の完了後、設置完了報告書を作成し、財団に提出すること。

12　研修

（１）財団のシステム管理者、IT リーダー等を対象として、新システム（クラウド環境、Windows10、資産管理ソフトの導入等）に係る操作説明研修を実施し、導入支援を行うこと。研修スケジュール、研修内容等について、研修実施計画書を作成及び提出し、財団の承認を得ること。
（２）新システムの操作手順を示した操作マニュアル及び障害対応マニュアルを作成し、財団の承認を得ること。また、新システムの運用管理及び障害発生時の一次切り分け等を円滑に実施するための運用手順を示した運用マニュアルを作成及び提出し、財団の承認を得ること。
（３）研修の規模について、システム管理者は 10 名程度（1 回）、IT リーダーは約 20 名×2 回開催＝40 名程度とし、研修会場は財団立川庁舎とする。実施方法は講義形式とし、実施に必要なプロジェクター、講師用 PC 等の研修用機器は、財団で用意する。
なお、研修資料（操作説明マニュアル等）は、受託者で用意すること（A4 カラー両面、50 部）。

13　運用保守

（１）オンサイト対応時間
9:00～17:30（土日祝日、年末年始を除く）
上記の時間外においても、電話、E-Mail 等による受付を行うこと（24 時間 365 日）。
（２）保守内容
１）クライアント端末ハードウェア保守
①5 年間の保守契約が可能であること。
②SSD 障害が発生した場合、受託者により、OS、統合オフィスソフト、ウイルス対策ソフト、資産管理ソフト等がインストールされた初期納入時の状態まで復旧を行うこと。また、部品交換が必要と判断された場合、受託者にて部品交換を行うこと。クライアント端末の復旧については、下記 14（2）の定期メンテナンス時に行うものとし、財団固有のアプリケーションの復旧は含まない。
③島しょの拠点については例外としてセンドバック対応を可とするが、その場合、必要な設定及び動作確認をすべて行った上で返送し、職員はネットワークケーブルを接続するだけで利用

が再開できるようにすること。

2）財団庁舎オンプレミス運用のサーバハードウェア保守

①5 年間の保守契約が可能であること。

②サーバ機器本体の保守に、無停電電源装置の保守を含むこと。

3）財団庁舎オンプレミス運用のサーバ運用保守

①5 年間の保守契約が可能であること。

②運用、環境、操作、障害対応および障害原因切り分けに関する問合わせについて、電話、E-Mail 等で対応すること。サーバハードウェア障害である場合には、メーカー保守窓口に連絡を代行すること。

③運用に関する問い合わせの対象範囲は以下のとおりとする。

・サーバ OS に関する対応

・Active Directory におけるユーザー管理のドメインサービスに関する対応

・バックアップソフトウェアに関する対応

4）オンプレミスサーバの監視・通報

①システムの運用にあたり、下記項目の監視を行うこと。エラーやアラートを検知した場合、その内容を解析し、受託者が対応を必要と判断した場合は、財団に電話、E-Mail 等で通報するとともに、必要な措置を講じること。

ア　ハードウェア監視

メーカーが提供するサーバ監視エージェントでエラーを検知し、監視ソフトウェアに出力されることによるハードウェア監視

イ　バックアップ監視

バックアップの実行結果とバックアップソフトの Windows サービス状態の監視

ウ　死活監視

対象のサーバの死活監視ができること。

②通報に必要なソフトウェア等は、受託者の負担で用意すること。また、システムの監視・通報について、特別な回線の契約やネットワーク機器の導入を必要としないこと。

③システムの運用状況や監視・通報サービスについて、四半期に１回、運用保守レポートを提出すること（様式任意）。

5）リモートサービス

①財団の求めに応じ、リモートでの障害切り分け・復旧支援の対応を行うこと。

②リモート対応は財団のインターネット利用用のインフラを利用し、HTTPS プロトコルを用いて行うこと。また、特別な回線の契約やネットワーク機器の導入が不要であること。

③リモート対応の内容は以下のとおりとする。

ア　サポート上必要となった場合、任意のコマンド実行、また、対象のサーバにインストールしたツールを用い、リモート接続による運用支援サービスを提供すること。

イ　財団の求めに応じ、サーバ再起動を実施すること。

ウ　財団の求めに応じ、サーバハードウェアリセットを実施すること。

エ　財団の求めに応じ、システムの設定変更を行うこと。
オ　財団の求めに応じ、修正プログラムの適用を行うこと。
カ　財団の求めに応じ、ファームウェアアップデートを行うこと。
キ　財団の求めに応じ、又は受託者が必要と判断した場合に各種ログの収集を実施すること。
④リモートサービスに必要なソフトウェアの導入は、受託者の負担で実施すること。
⑤リモートサービスによるサーバ停止が発生する際は、財団担当者に連絡すること。
⑥リモートサービスで障害が復旧しない場合は、必要に応じてオンサイト対応を実施して、OS 及びネットワーク設定の復旧を行うこと。

6）オンサイトサービス
①リモートサービスで障害が復旧しなかった場合は、必要に応じてオンサイト対応を実施すること。
②オンサイト対応では、設定仕様書の記載どおりに OS およびネットワーク設定の復旧を行うこと。ただし、データ復旧、財団が用意するアプリケーションソフトの復旧は含まない。

7）クラウドサービス
①クラウドサーバ基盤要件
ア　クラウドサーバ運用データセンター要件
・データセンターの入退館およびサーバルームへの入退室は、IC カードもしくは生体認証による認証を備えていること。
・震度 7 相当に耐えられる建物構造と防災対策が施されていること。
・複数の変電所からの２系統以上の受電設備を備えていること。
・Ｎ＋１構成の冗長構成 UPS 又は CVCF を備えていること。
・自家発電装置により最低 40 時間連続稼働できること。また燃料優先供給契約を締結していること。
・空調は空冷式 n+1 の冗長構成であること。
・装置・人体に無害な窒素ガス消火設備（超高感度煙探知機）を備えていること。
・データセンターには、財団が別途契約する回線（閉域網）を引き込むことができること。
イ　クラウドサービス提供基盤要件
・他の契約者とは論理的に分離された環境で、安全なパブリッククラウド環境を提供すること。
・クラウド基盤は冗長化されており、ホスト障害の際にも仮想マシンのダウンタイムを最小限に抑えることができること。
・クラウド基盤のハードウェア、ネットワーク装置はサービス提供事業者の責任で保守・監視・運用を実施すること。
・自社グループのデータセンターで提供されるサービスであり、日本国内で運用され、国内法が適用されること。また所轄裁判所は東京地方裁判所とすること。
・いかなる理由や目的であっても、データが二次利用されることが無いこと。

②クラウドサービス提供条件

ア　1年間単位の契約とし、5年間の自動更新が可能であること。

イ　クラウドサービス提供時間：24時間365日対応とすること。

ウ　定期的にシステムイメージバックアップの取得を行うこと。

エ　ゲストOSの作成、リソース割当変更、イメージバックアップ/リストア、電源操作など、必要に応じて操作・運用を代行すること。

オ　必要に応じてセットアップメディア等のマウントを実施すること。

カ　データセンター監視による、サーバ機器のハードウェア監視、ゲストOSの死活監視・リソース監視を行うこと。

キ　イベントログ監視・バックアップジョブ監視を行うこと。

ク　リモートメンテナンスによる障害原因の切り分け、および障害復旧支援を行うこと。

ケ　利用するWindowsサーバOSのライセンスはクラウドサービスの提供費用に含まれていること。

コ　各クラウドサーバは、CPU・メモリ・ディスク容量などが選択できること。また契約変更によりリソースの増減が可能なこと。

サ　各クラウドサーバに割り当てられるディスクは、SSD・SAS・SATAディスクもしくは同等のNAS機能を持ったサービスから選択できること。

シ　運用、環境、操作、障害対応および障害原因切り分けに関する問い合わせを、電話、E-Mail等で対応すること。

ス　運用に関する問い合わせの対象範囲は以下のとおりとすること。

・サーバOSに関する対応

・バックアップソフトウェアに関する対応

14　その他運用要件

（1）本案件にて導入したシステムの運用について、財団からの以下の相談に対応すること。

1）立川設置のサーバ群の操作方法、庁舎停電時の事前対応、セキュリティ対策

2）資産管理ソフト管理画面の操作方法、クライアント端末へのインストール方法

3）Windows10アップデートに係る操作・運用方法

4）その他、本案件にて導入したシステムの運用管理に関すること

（2）以下の定期メンテナンスを実施すること。

1）立川設置のサーバ群に対するパッチ対応・ファームウェア対応

2）クライアント端末に対するメンテナンス（財団依頼分、工数は半日程度まで）

3）定期メンテナンスは四半期に1回、半日程度実施すること。SSD障害が起きたクライアント端末の復旧等もここで行うものとする。

（3）データセンターのクラウドサーバ群に対し、以下のメンテナンスを実施すること。

1）パッチ対応（四半期1回程度）※ただし適用するパッチについては都度財団と協議すること。

2）必要に応じてリモートメンテナンスを実施すること。

（4）以下の支援を実施すること。

１）人事異動処理として新入職員、退職者アカウント追加削除（年１回想定）

２）資産管理ソフト導入後の資産情報の整理

３）Windows アップデートに係る WSUS スケジュール設定の変更（年１回想定）

４）クライアント端末の問い合わせに対する支援

①WindowsOS、ブラウザー、Microsoft Office製品等について、電話、E-Mail等で質問に対応すること。

②電話、E-Mail等で可能な範囲での一般的なソフト操作説明、及び障害切り分けと障害復旧支援を行うこと。

③対応時間は、9:00～17:30（土日祝日、年末年始を除く）とし、問い合わせ回数の上限はないこと。

④問い合わせ実施対象者は、システム管理者及び財団が指定する10名以内のITリーダー等とし、一般職員からの問い合わせは行わないこととする。

15　期間満了時の取扱い

（１）契約期間満了時においては、受託者の負担により、物理的破壊またはデータ消去によりデータが漏洩しないよう情報セキュリティ対策を講じること。実施にあたっては、事前に財団担当者と実施方法やスケジュールを調整するとともに、完了後はデータ消去完了証明書（書式は任意）を提出すること。なお、クラウドサーバについては、財団データの削除報告書を提出すること。
なお、機器の撤去後にデータの消去を行う場合は、事前調整において、データ消去までの期間における情報セキュリティ対策を示した上で、厳重に管理すること。

（２）付属品、添付品等の返却については、財団と協議の上、決定すること。

（３）搬出及び機器の撤去に係る一切の経費は、受託者の負担とする。