

【公表】

整理番号	104
契約番号	5農振財契第1031号
件名	財団ネットワークシステム構築・運用保守・支援業務委託
入札方法	電子入札システム「ビジネスチャンス・ナビ」上で実施
納入場所	東京都立川市富士見町三丁目8番1号 公益財団法人東京都農林水産振興財団 立川庁舎外10か所
概要	詳細は別紙仕様書のとおり
契約期間	令和6年4月1日から令和7年3月31日
契約方式	希望制指名競争入札
希望申出要件	別紙仕様書に記載のとおり
格付	問わない
仕様説明会	実施しない
開札予定日時	令和6年1月31日(水) 午前10時00分(入札期間は指名通知時に連絡)
希望申出期間	令和6年1月11日(木)午前10時から令和6年1月18日(木)午後4時まで
希望申出方法	電子入札システム「ビジネスチャンス・ナビ」を通じて受け付けます。
希望申出時の提出書類	以下の(1)から(3)までの書類を「ビジネスチャンス・ナビ」上に添付してください。 (1) 希望票〔様式あり〕(必要事項を記入) (2) 会社概要・実績一覧表〔様式あり〕(必要事項を記入) (3) 資格要件に対応する以下の <b>全て</b> の書類(書式は任意、写しで可) ①財団又は官公庁、大手企業等において本案件と同様の業務について契約実績を有することを証明するもの(契約書・請書の写しなど) ②プライバシーマーク(JIS Q 15001)、又は、ISMS(ISO27001)の認証を受けていることが分かるもの。 ③マイクロソフト社の以下の認定ソリューションパートナーであることが分かるもの。 「Infrastructure(Azure)」、「Data & AI(Azure)」、「Digital & App Innovation(Azure)」、「Modern Work」、「Security」の認定を受けていることが望ましい。 又は、今回導入するMS365 Business Premiumについて、上記認定資格保有者と同等以上のレベルのスキルを保有した社員にて、同規模以上の販売・構築・保守を行った実績が分かるもの。
備考	(1) 指名停止等業者については、東京都に準じて取り扱うものとしします。 (2) 指名業者の選定については、当財団指名業者選定基準によるものとしします。 (3) 希望票の提出があっても、必ずしも指名されるとは限りません。 (4) 指名通知は、指名した方のみに対して開札予定日の5日前までに行う予定です。 (5) 申込書類に不備がある場合、失格になることがあります。 (6) 関係する会社に該当する場合(親会社と子会社の関係にある場合、親会社を同じくする子会社同士の関係にある場合、役員の兼任等がある場合)には、同一入札に参加することができません。 (7) 入札結果(落札業者名、落札金額等)については後日公表します。予めご了承ください。
入札に関する問い合わせ先	公益財団法人東京都農林水産振興財団 管理課 契約担当 住所 東京都立川市富士見町3-8-1 電話 042-528-0721
仕様内容に関する問い合わせ先	公益財団法人東京都農林水産振興財団 管理課 企画係 住所 東京都立川市富士見町3-8-1 電話 042-528-0722

# 仕 様 書

## 1 件名

財団ネットワークシステム構築・運用保守・支援業務委託

## 2 目的

公益財団法人東京都農林水産振興財団（以下、「財団」という。）では、令和5年度、業務の効率化を図るため、Microsoft 365 Business Basicを導入しTeams及びOneDriveの活用を開始している。令和6年度においては、更なる効率化を図るため、Business Premiumへグレードアップし、メールやスケジューラ、ミーティング、チャット、ドキュメント管理、社内ポータル、個人用ストレージ、端末管理、ユーザー管理、など、インターネット環境があればどのデバイスからでもアクセスし、各種クラウド業務システムとも連携しながら、業務を進めることができる統合的なシステム基盤を構築する。合わせてIT資産管理システム（不許可端末機能及びアプライアンス端末付き）及びクラウド型総合セキュリティシステムと端末の挙動監視を行うEDRを導入し、セキュリティ機能を強化し、安定的な業務用のコミュニケーション基盤の導入により、業務の効率化を図ることを目的とする。

## 3 契約期間

令和6年4月1日から令和7年3月31日まで

## 4 契約の更新について

年度末に、システム構築完了後のシステム運用管理状況及びユーザー運用支援状況等を見て、財団が良好と判断した場合は、初期構築部分を除く、サブスクリプションサービス等で提供されるライセンス及び運用管理、運用保守、運用支援等に係わる部分については、次年度以降も継続して契約更新するものとする。尚、大幅な物価上昇の発生など協議が必要な場合を除き、本調達の費用と同額で提供すること。具体的な項目については、別紙1「次年度（令和7年度以降）契約更新内容」で提示する。尚、次年度、端末の一斉更新等が発生する場合は、契約更新については行わない場合もある。

## 5 履行場所

東京都立川市富士見町3-8-1

公益財団法人東京都農林水産振興財団外10か所

## 6 履行内容

別紙2「特記仕様書」のとおり

## 7 受託者の資格要件

本業務を実施する者は、以下の要件を満たしているものとする。

受託者は以下の要件を満たすことを示す証明書類等（書式は任意、写しで可）を提出すること。

- (1) 財団又は官公庁、大手企業等において本案件と同様の業務について契約実績を有すること。
- (2) プライバシーマーク（JIS Q 15001）、又は、ISMS（ISO27001）の認証を受けていること。
- (3) マイクロソフト社の認定ソリューションパートナーであること。  
「Infrastructure(Azure)」、「Data & AI(Azure)」、「Digital & App Innovation(Azure)」、「Modern Work」、「Security」の認定を受けていることが望ましい。  
又は、今回導入する MS365 Business Premium について、上記認定資格保有者と同等以上のレベルのスキルを保有した社員にて、同規模以上の販売・構築・運用・保守実績があること。

## 8 支払方法

- (1) 設計構築費  
全てのシステムの設計構築履行完了後、適法な請求書を受理した日から 30 日以内に一括して支払う。
- (2) ライセンス費・運用保守・運用支援費  
運用保守・運用支援開始月、ライセンス利用開始月より、毎月、適法な請求書を受理した日から 30 日以内に支払う。

## 9 著作権等の取扱い

この契約により作成される納入物の著作権等の取扱いは、以下に定めるところによる。

- (1) 受託者は、納入物のうち本業務の実施に伴い新たに作成したものについて、著作権法昭和 45 年法律第 48 号）第 2 章第 3 節第 2 款に規定する権利（以下「著作者人格権」という。）を有する場合においてもこれを行使しないものとする。ただし、あらかじめ財団の承諾を得た場合はこの限りでない。
- (2) 上記(1)の規定は、受託者の従業員、本業務の一部を再委託した場合の再委託先又はそれらの従業員に著作者人格権が帰属する場合にも適用する。
- (3) 上記(1)及び(2)の規定については、財団が必要と判断する限りにおいて、この契約終了後も継続する。
- (4) 受託者は、納入物に係る著作権法第 2 章第 3 節第 3 款に規定する権利（以下「著作権」という。）を、財団に無償で譲渡するものとする。ただし、納入物に使用又は包括されている著作物で受託者がこの契約締結以前から有していたか、又は受託者が本業務以外の目的で作成した汎用性のある著作物に関する著作権は、受託者に留保され、その使用权、改変権を財団に許諾するものとし、財団は、これを本業務の納入物

の運用その他の利用のために必要な範囲で使用、改変できるものとする。また、納入物に使用又は包括されている著作物で第三者が著作権を有する著作物の著作権は、当該第三者に留保され、かかる著作物に使用許諾条件が定められている場合は、財団はその条件の適用につき協議に応ずるものとする。

- (5) 上記(4)は、著作権法第27条及び第28条に規定する権利の譲渡も含む。
- (6) 本業務の実施に伴い、特許権等の産業財産権を伴う発明等が行われた場合、その取扱は別途協議の上定める。
- (7) 納入物に関し、第三者から著作権、特許権、その他知的財産権の侵害の申立てを受けた場合、財団の帰責事由による場合を除き、受託者の責任と費用をもって処理するものとする。

## 10 環境により良い自動車利用

本契約の履行に当たって自動車を使用し、又は利用する場合は、次の事項を遵守すること。

- (1) 都民の健康と安全を確保する環境に関する条例（平成12年東京都条例第215号）第37条のディーゼル車規制に適合する自動車であること。
- (2) 自動車から排出される窒素酸化物及び粒子状物質の特定地域における総量の削減等に関する特別措置法（平成4年法律第70号）の対策地域内で登録可能な自動車であること。

なお、当該自動車の自動車検査証（車検証）、粒子状物質減少装置装着証明書等の提示又は写の提出を求められた場合には、速やかに提示し、又は提出すること。

## 11 その他

- (1) 契約決定後、速やかに本契約に係る費用明細（設計構築費、運用保守費、運用支援費ライセンス費等）を記載した内訳書及び年間を通した月別の支払内訳書を作成し提出すること。尚、ライセンス費、運用保守費、運用支援費については、次年度以降の契約更新に係わる費用であるため、項目ごとに、数量、単位、提供単価、提供合計、備考等を分かりやすく明記すること。
- (2) 業者決定後、財団が令和5年度より利用しているMicrosoft365関連のライセンスに関しては、令和6年3月31日に現在の業者との契約が終了するため、令和6年4月1日以降も間断なく継続して、財団がその既に構築されたMicrosoft365のテナントが利用できるように、速やかにマイクロソフト社のCSP契約に係わる追加手続き処理等必要な手続きを行うこと。又、必要がある場合は現在の業者と連携を図り手続きを進めること。

現在利用しているライセンスと令和6年4月1日以降の流れは以下の通りである。

- ・Microsoft 365 Business Basic ×300 → 令和6年4月1日以降も継続利用
- ・Office 365 E1 ライセンス ×30 → 令和6年3月31日で利用終了
- ⇒ Business Standardへ切替 ×30 → 令和6年4月1日より新規利用開始

- ⇒Business Standard×50 に増量 → 令和6年4月1日より新規利用開始
- ・Enterprise Mobility + Security E3×30 → 令和6年4月1日以降も継続利用
- ⇒Enterprise Mobility + Security E3×50 に増量
- ・Azure AD Premium P1 ×300 → 令和6年4月1日以降も継続利用

尚、上記、令和6年4月1日以降の利用ライセンスについても、契約期間中に下記の通り変更するので必要な手続きを行うこと。

- ・Microsoft 365 Business Basic ⇒ Business Premium へグレードアップ
- ・上記に合わせて、Azure AD Premium P1 は不要となるため解約

- (3) 本業務の履行に係る一切の費用は、すべて契約金額に含むものとする。
- (4) 本件で調達するマイクロソフトライセンスに係る製品の活用促進について、提案や相談対応を行うこと。また、提案や相談対応を行える技術力と体制を有すること。
- (5) マイクロソフトクラウド製品の構築実績のある人員を体制に含むこと。
- (6) マイクロソフト社の Fast Track Ready パートナーである場合は、それが分かるものを提出すること。又、その場合は下記を実施すること。  
 契約期間中に、クラウド製品の利用状況レポートを提供すること。  
 契約期間中に、Microsoft 365 に関するワークショップを提供すること。  
 Entra ID、SharePoint、Azure Open AI いずれかのワークショップを無償で提供すること。内容については財団と協議して決めるものとする。
- (7) 受託者は、契約の履行に関して知り得た機密情報を第三者に漏らし、又は他の用途に利用してはならない。契約期間の終了後においても同様とする。
- (8) 本仕様書に定めのない事項については、別紙3「電子情報処理委託に係る標準特記仕様書」を遵守すること。
- (9) 個人情報の取扱については、別紙4「個人情報に関する特記事項」のほか関係法令等を遵守すること。
- (10) 別紙5「東京都グリーン購入推進方針」に配慮すること。
- (11) 受託者は、業務の履行にあたり、その業務の一部を再委託する場合、事前に財団の承認を得ること。
- (12) 本契約において適用される準拠法は日本法とし、あらゆる紛争に関する第一審裁判所は東京地方裁判所とする。また、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。
- (13) 暴力団等排除に関する特約条項については、別に定めるところによる。
- (14) 本仕様書の解釈に疑義を生じた場合は財団と協議して処理するものとする。

## 1.2 担 当

公益財団法人東京都農林水産振興財団 管理課 企画係 システム担当  
 〒190-0013 東京都立川市富士見町3-8-1  
 (TEL) 042-528-0722 (E-mail) kanri-it@tdfaff.com

## 次年度（令和 7 年度以降）契約更新内容

次年度以降も契約更新するライセンス及び運用支援業務等は以下の通りとする。

### 1) ライセンス関係

- ①Microsoft 365 Business Premium
- ②Microsoft 365 Business Standard
- ③Enterprise Mobility + Security E3
- ④Trend Micro ウイルスバスター ビジネスセキュリティサービス
- ⑤Trend micro Email Security
- ⑤Trellix HX (EDR)
- ⑥Azure サーバー (SKYSEA サーバー用)
- ⑦SKYSEA ClientView Professional Edition(ガバメント) サーバーライセンス
- ⑧SKYSEA ClientView Professional Edition(ガバメント) クライアントライセンス

### 2) 運用管理及び運用保守

- ・上記 1) に係わる運用管理及び運用保守業務も全て含むものとする。

### 3) 運用支援関係

- ①システム運用支援 (サーバー及び端末に関する各種問い合わせ対応)
- ②システム運用支援 (定例会実施)
- ③システム運用支援 (年度末人事異動サーバーデータ変更対応)
- ④システム運用支援 (サーバパッチ適用対応)
- ⑤システム運用支援 (端末 OS リカバリ等対応)
- ⑥システム運用支援 (端末 Windows 大型アップデート対応) ※令和 7 年度より実施

## 特記仕様書

### 1 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、IP-VPN 網を通じてインターネットへの接続を行っていたが、ゲートウェイのセキュリティ対策製品のサポート終了に伴い、令和5年度にクラウド型セキュアインターネットゲートウェイサービス「Cisco Umbrella SIG Advantage」（以下、「SIG」という。）を導入し、各拠点からブレイクアウトさせる構成に変更した。また、同時にクラウド認証基盤「Microsoft Entra ID Premium P1 相当」（以下、「IdP」という。）を導入することで、認証のセキュリティの見直しを図り、クラウド型コミュニケーション基盤の一部機能(Teams、OneDrive)をリリースしたところである。本調達では、クラウド型コミュニケーション基盤への全面的な移行 (Microsoft365 Business Premium へのグレードアップ) 及び、各種セキュリティ対策の強化とクラウド移行を行うことで、運用負荷の軽減を図り、安定的な運用に資するとともに、フルクラウド/ゼロトラスト環境による、場所を問わない働き方で、業務の効率化を図ることを目的とする。

#### (2) 委託業務内容

IdP 及びクラウド型コミュニケーション基盤の追加設計・動作確認及び運用・保守サポート、各種セキュリティ対策の導入設計・構築・移行、動作確認及び本番稼働後のシステム運用・保守サポート、システム運用支援、メールシステム移行支援等を行う。

#### (3) スケジュール

各工程に要する期間については以下を想定しているが、本番稼働時期等を考慮して、適切なスケジュールを提示し財団の承認を得ること。

スケジュール（案）

項目	令和6年度											
	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
クラウド認証基盤追加設計	→											
クラウド認証基盤設定変更		→										
コミュニケーション基盤追加設計、設計変更			→									
コミュニケーション基盤 新設定、既存設定変更					→							
メール移行※							→					
新基盤利用開始 運用保守、運用支援								展開	→			

※受託者はメール移行の支援を行うこと。

#### (4) 現行環境について

現行のネットワーク構成及び導入後のネットワーク構成に関する情報については、希望票を提出した業者に別途開示するものとする。尚、開示した情報については関係者以外には共有せず秘密保持を万全に図ること。

## 2 システム要件

### (1) クラウド認証基盤

クラウド認証基盤（以下、「Idp」という。）は、以下の要件を満たすクラウドサービスであること。令和5年度に導入している以下のサービス及びソフトウェアを、令和6年4月1日からも継続して利用できるようにすること。

- ・Microsoft Entra ID Premium P1（旧 Azure AD Premium P1）相当機能

#### <基本機能>

- ①SAML2.0に対応し、財団が別途利用中の各種クラウドサービスにSSO可能なこと。
- ②Windows, Mac, iOS, Android 等様々な OS に対応し、特定のデバイスに依存しない認証サービスを利用できること。
- ③主要な機能をブラウザで管理できること。また、特殊な機能の設定や一括処理をする際には PowerShell や APIを使ったプログラム等からの管理ができること。
- ③オンプレミスのWindows Server で動作しているActive Directory と同期する機能を有し、将来的にはクラウドサービスとオンプレミス双方に対して共通のIDでアクセスできる構成が可能なこと。
- ④パスワードの有効期間を設定可能なこと。
- ⑤定期的なパスワード変更を利用者に促す機能を有していること。
- ⑥携帯電話回線のショートメッセージやスマートフォン用アプリケーション、音声通話等をつかった多要素認証が利用できること。
- ⑦接続元ネットワークのグローバルIPアドレスに応じてサービスの利用を制御できること。
- ⑧利用者がパスワードを忘れてしまった場合でも自分自身でパスワードを再発行できる機能を有すること。
- ⑨理者は利用者の認証アクセス状況をレポートとして確認することが可能なこと。
- ⑩ユーザーをグループ単位で管理可能であること。また、グループごとに認証ポリシーを設定することが可能なこと。
- ⑪前に登録したグローバル IP アドレス以外からアクセスした場合や、財団が許可した端末以外からの認証を制限することが可能なこと。またこれらのポリシーはユーザーグループや SSO 先等の条件を設けて設定可能なこと。

## (2) コミュニケーション基盤

コミュニケーション基盤は、メール、スケジュール、設備予約、社内ポータル、/連絡先/ToDo管理、ビジネスチャット、共同作業スペース、Web会議、オンラインストレージの機能を有し、以下の要件を満たすクラウドサービスであること。令和5年度に導入している「Microsoft365 Business Basic」を構築期間中に「Microsoft365 Business Premium」にグレードアップし設計・構築すること。利用する主なサービス及びソフトウェアは以下とすること。

- ・ Microsoft Teams (令和5年度より利用中)
- ・ OneDrive for Business (令和5年度より利用中)
- ・ Exchange Online (新規構築)
- ・ SharePoint Online (新規構築)

外部DNSサービス及びドメイン管理サービスは、現在財団が利用しているものを利用するものとする。

### <基本機能>

- ①全ての機能は単一のプラットフォームにより提供することとし、各サービス間で連携機能を有すること。
- ②外部関係者とのコミュニケーションに使用できるツールであること。
- ③専用のクライアントアプリケーション以外に、ブラウザベースのクライアントで主要機能が利用可能なこと。
- ④場所を問わずに操作性を損なうことなく作業可能なこと。
- ⑤PCやスマートフォン、タブレット等の端末の種類を問わず、Webベースで利用可能なこと。

### <メール要件> Exchange Online/Outlook

- ①財団内外に対してメールの送受信が行えること。
- ②外部へのメール送信を制限できる機能を有すること。
- ③メールの送受信においてサーバー間の通信が暗号化可能なこと。
- ④メールへファイルの添付が可能なこと。
- ⑤メール本文に表の作成が可能なこと。
- ⑥メッセージサイズは、既定値として35MB、最大150MB送受信可能なこと。
- ⑦フィルタ機能や名前/件名/日付でのソート機能など、メールが効率的に閲覧可能なこと。
- ⑧一括配信リストの機能を有すること。

- ⑨利用者が不在通知の設定を行え、かつ送信者に不在の通知が1度だけ送信されること。
- ⑩各利用者に、50GB以上のメールボックス領域を提供可能なこと。
- ⑪利用者が任意のアドレスにメールの転送設定を行うことが可能なこと。
- ⑫制限した容量を超過した場合には、送受信不可とすること可能なこと。
- ⑬同一組織上に存在するメールに対して、未開封メールの差し替え又は削除を行うことが可能なこと。
- ⑭利用者が自分のメールボックス内に任意のフォルダを作成可能なこと。
- ⑮指定した保存期間が経過したメールに対して自動的に削除する機能を有すること。
- ⑯利用者による削除等の操作にかかわらず指定した条件のメールを一定期間保管する機能を有すること。
- ⑰30日以内であれば、削除済みメールアイテムを利用者自身の操作により回復が可能な機能を有すること。
- ⑱無料で使用できる共有のメールボックスが提供されること。
- ⑲添付ファイルについて閲覧するためにアプリケーションを起動することなく表示できるプレビュー機能を有すること。
- ⑳フォルダ単位または全フォルダに対しての全文検索可能なこと。また、Word, Excel形式の添付ファイルについても全文検索可能なこと。
- ㉑同一組織宛てに送信するメールについては、受信者がメールを開封したか否かの通知機能を有すること。
- ㉒送信メールサーバについては、現在財団が利用している、Active!GATE SSが利用できること。

#### <スケジュール/連絡先/ToDo管理要件> Outlook及びExchange Online

- ①利用者がメールを簡単な操作でスケジュール上の予定として登録し管理できる機能を有すること。
- ②利用者がメールを簡単な操作でToDoタスクとして登録し管理できる機能を有すること。
- ③利用者がそれぞれの連絡先アドレス帳を管理できる機能を有すること。また、受信したメールから簡単な操作で連絡先を登録できる機能を有すること。
- ④スケジュール登録が行え、アクセス権の設定に基づいてスケジュールの共有が可能なこと。
- ⑤複数のスケジュールを並べて表示する機能を有すること。
- ⑥他の利用者に対してメールにて会議の招集依頼が行え、依頼を受けた利用者のスケジュールに自動的に登録されること。

- ⑦スケジュールをアイテム単位で公開。非公開の設定ができること。
- ⑧会議の招集を受けた利用者は、参加、仮承諾、不参加などの応答を開催者に行えること。
- ⑨会議への出欠予定応答の状態が一覧で容易に確認可能なこと。
- ⑩会議室などの設備予約機能を有すること。また設備に対して予約できる利用者を制限可能なこと。
- ⑪会議室を予約する際、重複した場合は予約させない機能を有すること。
- ⑫繰り返し発生するスケジュールを一括で作成できる機能を有すること。
- ⑬直近の予定の時刻が近付いたとき、ポップアップなどで利用者に通知する機能を有すること。
- ⑭スケジュール予約に連動して、Teams会議の予約、及びTeams会議案内通知も可能なこと。

#### <ビジネスチャット要件> Microsoft Teams

- ①利用者間でメッセージの送受信が可能なこと。
- ②任意の利用者を設定し、複数人への同報が可能なこと。
- ③会話の相手がオフラインであっても送信可能なこと。
- ④受信した過去のメッセージを確認可能なこと。

#### <共同作業スペース要件> SharePoint Online

- ①利用者間での資料の送付、グループに紐づくファイル保存領域を有し、電子ファイルをチャットルーム内で共有可能なこと。
- ②共有されたファイルに対し、複数メンバーでのリアルタイム同時編集が可能なこと。
- ③後述するオンラインストレージ機能と連携し、ファイルの共有やOfficeファイルの共同編集機能を提供すること。
- ④ファイルのアップロードやダウンロード、閲覧、編集において可能な限りコミュニケーション基盤のアプリケーション内で操作が完結すること。

#### <社内ポータル要件> SharePoint Online

- ①掲示板（部門ごとの掲示ができるもの）、ファイル管理等ができること。
- ②財団の社内ポータルを作成すること。
- ③財団の社内ポータルを作成・変更・更新をするための参考テンプレートを提供すること。

#### <Web会議要件> Microsoft Teams

- ①Web会議に参加できる最大参加者数は250名以上であること。
- ②ライセンスを保有しない外部関係者とのWeb会議が利用可能なこと。
- ③ビデオ使用時には背景をぼかす、仮想背景を表示する等のプライバシー保護機能が使用可能なこと。
- ④日時を指定した会議予約が可能なこと。
- ⑤メールにより会議参加者を招待可能なこと。
- ⑥会議開催者が招待することで外部関係者が会議に参加可能なこと。
- ⑦会議の予約及び開催は、メール・スケジュールサービスと連携すること。
- ⑧Web 会議の録音・録画が可能なこと。
- ⑨画面共有やホワイトボード機能を活用してオンライン会議を円滑に進められること。かつ、それらが全て1つのウィンドウ内で実現され、利用者の利便性が高いこと。

#### <オンラインストレージ要件> OneDrive for Business

- ①任意に階層的にフォルダを作成可能なこと。
- ②有用ドキュメントをオフラインで利用するためのダウンロード、同期機能を有すること。
- ③フォルダやファイル単位にアクセス不可、閲覧のみ、編集可能などのアクセス権が設定可能なこと。
- ④Excel, Word, PowerPointのファイルについて、Webブラウザ内で表示・編集できる機能を有すること。
- ⑤誤って削除したファイルを職員自身の操作で復元可能なこと。
- ⑥ファイル（Word, Excel, PowerPointなど）の本文を含めた全文検索が可能なこと。
- ⑦ファイルの検索結果について可能な限り内容のプレビューが表示可能なこと。
- ⑧ファイルサイズ10GBのファイルをアップロード可能なこと。
- ⑨ファイルの編集にあたって、排他制御が可能なこと。
- ⑩組織用共用ファイル領域として「1TB+利用者数×10GB」以上の容量が利用可能なこと。
- ⑪個人用ファイル領域として、1ユーザーあたり1TB以上の容量が利用可能なこと。

### (3) メールセキュリティ対策

メールセキュリティ対策は以下の要件を満たすクラウドサービスであること。  
Exchange Online標準のメールウイルス対策機能だけでは防げない、標的型攻撃メール対策、ゼロデイ攻撃対策、メールなりすまし対策、ランサムウェア対策等

に対応し、Exchange Onlineと連携可能な以下のサービスを利用するものとする。

- Trend Micro Email Securityサービス

#### <基本機能>

- ①悪意あるメールがメールボックスに到達する前に対策が可能なこと。
- ②機械学習及びサンドボックスを用いた高度な検索で、既知・未知を問わず、不正なファイルやURLを検出可能なこと。
- ③添付ファイルにマクロが含まれる場合、マクロを自動的に除去するサニタイズ機能を設定可能なこと。
- ④パスワード付きファイルのパスワードを、メール件名や本文、別メールから推測し、パスワード付きZIPファイルについても解析を行う機能を有すること。
- ⑤不正なメールと判定された場合、該当するメールを隔離することが可能なこと。隔離したメールについては、管理者による再送、利用者による再送が可能なこと。
- ⑥送付先のメールサーバの障害を検知し、最大10日間以上の送受信メールの保存を自動的に行えること。また、障害中に保存した送受信メールの、閲覧・ダウンロード等が可能なこと。
- ⑦送受信に関する防御ポリシーはユーザーやグループごとに設定可能なこと。
- ⑧CSV形式でログのエクスポートが可能なこと。
- ⑨管理者向けのダッシュボード機能を有すること。

#### (4) エンドポイントセキュリティ対策

エンドポイントセキュリティ対策は、以下の要件を満たすクラウドサービスであること。利用を想定する主なサービス及びソフトウェアは以下のものである。

- Trend Micro ウイルスバスター ビジネスセキュリティサービス 及び Trellix HX (旧 FireEye) 相当のもの

#### <基本機能>

- ①アンチウイルス機能とEDR機能を有すること。それぞれ別の製品で実現することも可とする。
- ②財団が別途管理サーバーを用意する必要がないこと。
- ③クライアントにモジュール常駐させる等、場所を問わず対策が可能なサービスであること。
- ④Windows PC (Windows 10 Pro / Windows 11 Pro) で動作可能なサービスである

こと。

**<アンチウイルス機能要件>** Trend Micro ウイルスバスター ビジネスセキュリティサービス

- ①不正なプログラムをリアルタイムに検出し、駆除、削除、隔離等が可能なこと。
- ②AI技術による機械学習型検索を利用し、未知の不正プログラムを検出可能なこと。
- ③エンジン、パターンファイル等を各端末がインターネット経由で自動的にアップデートすることが可能なこと。
- ④不正なプログラム等を検出した場合、管理者に通知を行う機能を有すること。
- ⑤対策の適用状況などを確認できる管理者画面の機能を有すること。

**<EDR機能要件>** Trellix HX (旧FireEye) 相当のもの

- ①カーネルモードで動作し、IOC (Indicator of Compromise) を基に侵害をリアルタイムに検知可能なこと。
- ②ふるまい検知機能を有し、アプリケーションの脆弱性を突く悪意のある攻撃に使われたプロセスを終了させる機能を提供すること。
- ③AI型マルウェア検知機能を提供し、検知されたPEファイルに関して、サンドボックスによる検体解析を行う機能を有すること。
- ④EDR管理サーバーとDNSサーバー以外との通信を遮断する端末の自動隔離機能を提供すること。
- ⑤以下の機能をもつ管理ポータルを提供すること。
  - a デバイスの一覧の表示
  - b デバイスの検索・詳細表示
  - c 選択したデバイスの隔離/隔離解除、隔離除外/隔離除外解除
  - d 選択したデバイスの削除
  - e 表示中のデバイス一覧のCSVダウンロード
  - f アラート一覧の表示と検索
  - g 自動隔離設定
  - h 簡易レポート機能
- ⑥以下の運用サービスを提供すること。
  - a 脅威アラートの監視及び分析とメール通知 (24時間365日)
  - b 検知した脅威に対するSOCアナリストによるトリアージ
  - c 侵害発生時の侵入経路、システム改変有無、ファイル操作有無の調査
  - d 危険な端末の隔離と検体取得支援
  - e 作業内容報告

## (5) デバイス管理システム

デバイス管理システムは、以下の要件を満たすクラウドサービスであること。  
導入する「Microsoft365 Business Premium」の中で提供される以下のサービス機能を利用して構築すること。

・Microsoft Intune

### <基本機能>

- ①管理対象のデバイスについて、利用者自身による登録、管理者による一括登録のどちらにも対応が可能なこと。
- ②登録するデバイスについては、制限を設けることが可能なこと。
- ③デバイスを登録することで、本件で導入するIdPで、登録済みデバイス以外のアクセスをさせない設定が可能であること。
- ④登録済みデバイスに対して、セキュリティポリシーの設定、証明書、Wi-Fi設定等を配布することが可能なこと。
- ⑤登録済みでデバイスについて、デバイスやアプリのインベントリ収集が可能なこと。
- ⑥紛失したデバイスについて、遠隔でデータの消去が可能なこと。なお、BYOD端末については業務に関連するデータのみ遠隔で消去が可能なこと。
- ⑦モバイルデバイス管理が強制できない BYOD 端末などでも安全にデータを利用できるように、モバイルデバイス上のアプリケーションに対してデータを個人の領域に保存させない、コピー&ペーストを無効化する等の制限をかけることが可能なこと。
- ⑧Windows PCの展開機能を有し、Entra ID JoinedやHybrid Entra ID Joinedの設定を自動的に行う機能を有すること。

## (6) IT資産管理システム

IT資産管理システムは、以下の要件を満たす製品であること。  
以下の2つのシステムを組み合わせで構築すること。  
不許可端末遮断については、SKYSEA Client Viewの不許可端末遮断機能を利用し、MACセンサーはSKYSEAと連携可能なIntraGudian2+を利用すること。

- ・SKYSEA Client View Professional Edition (IT資産管理システム)
- ・IntraGudian2+ (不許可端末遮断システム)

### <基本要件>

- ①本入札の公示時点で出荷されている製品であること。
- ②クライアント端末のOSについては、Windows11 に対応していると共に、製造元のサポート契約期間中は、無償で最新のOSへの対応が可能なこと。

### <機能要件（資産管理）>

- ①各クライアント端末に関する各種ハードウェア情報、ソフトウェアに関するインストール状況等を資産情報として自動的に収集可能なこと。
- ②収集したハードウェアおよびソフトウェア情報を、一覧で表示できること。また、資産情報の検索の際は、インベントリ情報やWindowsOSのバージョン、ビルド番号、サービスパックなどから、同時に複数項目、複数キーワードおよび数値の範囲を指定して検索可能なこと。
- ③資産情報の検索の際には、本ソフトウェアから削除されたクライアント端末も、検索対象として指定可能なこと。
- ④本システムを導入できないデバイスの資産情報を、資産台帳へ直接アップロードするツールを提供可能なこと。また、ソフトウェアが自動的に収集することが出来ない項目については、アンケート形式で利用者に情報を入力することが可能なこと。
- ⑤クライアント端末に対して、Windows更新プログラムを配布し自動的に更新プログラムの実行を行う等のセキュリティパッチを配布可能なこと。
- ⑥電源ON/OFFを制御できる環境下にある場合、クライアント端末の電源ON/OFFが自動で行える設定が可能なこと。
- ⑦複数のクライアントに対してソフトウェアを配信する際に、サーバーからセグメントごとに自動選択されたクライアント端末にソフトウェアが配信され、その後、その自動選択されたクライアント端末から、各クライアント端末へ一斉同時配信できるマルチキャスト配布によるソフトウェアの配信を行うことが可能なこと。
- ⑧先側のクライアント端末の配信データを、自動的にキャッシングした上で中継可能なこと。また、この際に配信データのキャッシングを行うクライアント端末は、他のクライアント端末への中継を行っている時も正常にクライアント端末として動作が可能なこと。
- ⑨クライアント端末がソフトウェアの配布を受ける際、既に同じセグメント内にソフトウェア配布のために自動選択されたクライアント端末にソフトウェアがキャッシュとして存在していた場合には、そのクライアント端末からソフトウェア配布が可能なこと。また、キャッシュから配布を行う場合は、通信帯域の制限や同時に接続できるクライアントが可能なこと。

- ⑩Administrator 権限がないクライアント端末であっても実行が出来るよう、ソフトウェア等の配布方法として管理機からのプッシュおよびクライアント端末からのプルを選択可能なこと。
- ⑪セグメント内で最後に電源を切るクライアント端末に対して、セグメント内で電源が入っているプリンターなどネットワーク機器情報をポップアップで通知可能なこと。
- ⑫IPアドレスの管理台帳と、資産情報（不許可端末検知情報も含む）を照合し、競合や不正使用、使用期限切れを表示可能なこと。また表示方法は、一覧表示およびマップ表示を選択可能なこと。
- ⑬BitLockerおよび他サードパーティ製品により、ハードディスクを暗号化した際に生成される回復キーを収集、管理可能なこと。また、これらの暗号化状態をハードウェア一覧で確認でき、暗号化状態が変更された時はドライブログとして記録可能なこと。

#### <機能要件（制御・管理）>

- ①利用者がアプリケーションの実行、禁止アプリケーションの名前変更、インストールの実行、Windows システム構成変更、レジストリ変更、Windows ストアアプリの自動更新などを禁止可能なこと。
- ②使用を禁止するアプリケーションの指定は、ブラックリスト方式とホワイトリスト方式といずれかを選択可能なこと。
- ③アプリケーションごとに、起動禁止を除外できる時間設定が可能なこと。
- ④事前定義されたルールに反した際に、管理者及びその操作を行った利用者のクライアント端末のデスクトップ上にポップアップ形式で通知可能なこと。ルールに反した操作をしたクライアントコンピューターの利用者に注意を促すため、メッセージの内容はアラート操作ごとに設定可能なこと。
- ⑤アラート発生時における端末操作画面を、マウスカーソルの位置が強調された形式で表示し、不正操作及び誤操作発生時に早期の問題把握が可能なこと。
- ⑥アラート項目ごとにメールでの通知先の設定ができ、アラートの発生時には、設定された通知先にメールを自動送信できること。
- ⑦プリンターごとやユーザーごとに印刷の禁止が設定可能であること。
- ⑧画面キャプチャー（スクリーンショット）を禁止する機能を有すること。
- ⑨外部記憶媒体へのデータ書き込みや、印刷などを禁止したい特定のフォルダを監視対象として登録可能なこと。また、監視対象になったフォルダは、以下の操作をおこなった際に、自動的にメールの通知や操作そのものの禁止が可能なこと。
  - a リモート操作受信
  - b クリップボードへのコピー

- c 印刷
- d 画面キャプチャー
- e 外部記憶媒体へのデータ書き込み
- f PrintScreen

- ⑩BitLockerを使用してドライブの暗号化を行う際に、スマートカードを使用してドライブを復号する設定を禁止できること。
- ⑪あらかじめ登録されていないクライアントコンピューターが接続された場合、該当のコンピューター情報（IPアドレス、MACアドレス、ゲートウェイMACアドレス、ゲートウェイIPアドレス）を収集できること。
- ⑫あらかじめ登録されていないクライアントコンピューターが接続された場合、該当のコンピューター情報を取得し、一覧表示できること。また、接続されたことを管理機のデスクトップにポップアップ表示および、メールで通知できること。

#### <機能要件（デバイス制御）>

- ①USB外部ストレージをクライアント端末もしくは管理者のクライアントコンピューターに挿入した際、利用したUSBメモリの製品名、シリアルナンバー、ベンダーIDを自動で認識し、UI上で自動的に管理台帳を作成できること。また、シリアル番号やベンダーID、およびプロダクトIDが取得できず、個体識別が行えないUSBデバイスについては、台帳への登録を制限可能なこと。
- ②収集した情報にもとに指定したUSBメモリを使用許可/不許可/読取専用を設定可能なこと。使用許可/不許可/読取専用の設定は、管理対象端末全体および指定した部署のみ、ユーザー単位等、柔軟な設定が可能なこと。
- ③SDカード、MOディスク、DVD-RAMなど書き込み可能メディアを、登録したメディアごとに使用許可/不許可/書き込み禁止を設定可能なこと。
- ④デバイス種別やデバイス種別に対応するメディアごとに、一括で使用不可/読取り専用/使用不可能の設定が可能なこと。設定ができるデバイスの種類、メディアは以下の通りとする。
- ⑤USBデバイスの棚卸する機能を有すること。棚卸しの期限は任意で設定でき、期限を超過しても棚卸しが確認できていないUSBデバイスや利用者を表示可能なこと。また、棚卸し期間を超過したUSBデバイスの利用を制限可能なこと。
- ⑥USBデバイスが端末に接続された日時とログオンユーザー名とを利用し、USBデバイスを現在所持している可能性が高いユーザーを自動的に特定して表示可能なこと。
- ⑦USBデバイス内ファイルの日時情報を比較し、システム外で作成・編集された外部ファイルの持ち込みを自動判定可能なこと。また、そのUSBデバイスを使用禁止に設定可能なこと。
- ⑧ネットワークに接続できない環境などでクライアント端末に対しても、デバイス

管理台帳の情報をクライアント端末のエージェントに取り込むことで、デバイス管理台帳上の設定に従ったデバイス制御（使用禁止，書き込み禁止）が可能なこと。

#### <機能要件（クライアント操作ログ取得）>

- ①電源オン/オフ、ログオン/オフの日時、実行されたソフトウェアについての起動・起動期間、プリンター出力ログ、Web閲覧（ダウンロード・書込・アップロード）ログ、不許可端末情報、共有フォルダへのアクセス、ファイル操作、クリップボードにコピーされた内容、USBメモリなどの記憶媒体を利用した内容および記憶媒体のシリアル情報等を記録する機能を有すること。また、Windowsポータブルデバイスへのファイル操作（ファイル・フォルダ作成、ファイル削除、ファイル名変更）をログとして記録する機能を有すること。
- ②クライアント端末上でアプリケーションソフトウェアから印刷が実行された際に、その印刷されたドキュメント名、1回の印刷枚数、ファイルパスを記録する機能を有すること。
- ③クライアント端末からWebサイトにアクセスした内容を表示できるとともに、表示する集計期間や集計を除外するURLの設定も可能なこと。また、クライアント端末ごとおよび部署ごとの表示においては、ネットワーク全体でのアクセスが少ないURLに対するアクセスを自動的に判定し、強調表示可能なこと。
- ④収集されたファイル操作ログから、一つのファイルに対してどのような操作（コピー、ファイル名変更、新規作成、削除など）が行われたかを抽出して表示する機能を有すること。また、特定の操作ログより前後5分間の操作ログを検索・抽出可能なこと。
- ⑤クライアントコンピューターから収集したログデータをバックアップする際、ログデータを圧縮してバックアップする設定ができること。また、圧縮してバックアップした複数のログデータに対して、まとめて検索できること。
- ⑥端末側で保存するログデータは改変されないように難読化されていること。

#### <機能要件（リモート操作・管理コンソール）>

- ①特定及び複数のクライアント端末に対して、ネットワーク経由でキー及びマウスをリモートで操作可能なこと。
- ②リモート操作時はクライアント端末の操作をロック可能なこと。
- ③遠隔からの操作を受けるクライアント端末の画面を、管理者画面で拡大・縮小、全画面表示可能なこと。
- ④管理機画面をクライアント端末側に表示可能なこと。
- ⑤リモート操作時に操作機側とクライアント端末間でファイルの転送及びテキスト

データや画像データをコピー&ペーストが可能なこと。

- ⑥パスワード入力などセキュリティの観点からクライアント端末に表示したくない遠隔操作を行う場合は、クライアント端末に対して操作画面を隠しながら遠隔操作可能なこと。
- ⑦遠隔操作によってクライアント端末のメンテナンスをする際は、遠隔操作を実行するクライアント端末で行われた操作内容に応じて遠隔操作中の通信量を自動でコントロール可能なこと。
- ⑧各クライアント端末の利用状況を把握するため、クライアントコンピューターの操作画面を管理端末で表示する機能を有すること。
- ⑨クライアント端末がマイナンバー取扱端末として設定されている場合は、操作画面を表示しないこと。

#### <機能要件（不許可端末遮断）> IntraGuadian2+

- ①IT資産管理システムに登録されていないデバイスを財団ネットワークに接続した場合、ARPパケットを読み取り、自動的に検知・遮断が可能なこと。
- ②検知・遮断時にはメール等で通知が可能なこと。
- ③以下の仕様を満たす、24時間365日の稼働を前提としたハードウェアアプライアンス製品を財団各拠点のネットワーク内に設置すること。
  - a IT資産管理システムの管理サーバーに直接アクセスをして、登録情報に基づき、遮断・接続の許可を行うこと。（別途管理サーバー等が不要であること
  - b MACアドレスを40,000件まで登録可能なこと。
  - c 筐体は1辺140mm以下の省スペース型であること。
  - d 消費電力は5W以下であること。

#### <構築・実装要件> SKYSEA Client View Professional Edition

- ①IT資産管理システムの管理サーバーはクラウド上に設置すること。財団の拠点、または、データセンターに機器を設置する構成は不可とする。  
財団の既存のインターネットVPN網（NEC CloverNET）とVPN接続する構成とすること。
- ②財団が現在、別業者よりレンタル利用しているIaaS環境（Microsoft Azure）上に構築することも可とするが、構築期間中及び運用開始後のIaaS利用料については受託者が負担すること。
- ③財団が利用しているIaaS環境以外に新規構築する場合は、構築期間中及び運用開始後のIaaS利用料、VPN接続利用料、CloverNETの運用事業者による各拠点のルーターのVPN設定変更等費用については、受託者が負担すること。

(7) 本年度調達する各システムの利用者数/ライセンス数等は以下のとおりとする。

項目	数量	単位	期間	単位	備考
Microsoft 365 Business Basic ライセンス	300	User	4	月	令和6年4月～令和6年7月
Office 365 E1 ライセンス	-	User	-	月	-
Enterprise Mobility + Security E3 ライセンス	30	User	4	月	令和6年4月～令和6年7月
AzureAD Premium P1 ライセンス	300	User	4	月	令和6年4月～令和6年7月
Microsoft 365 Business Premium ライセンス	300	User	8	月	令和6年8月～令和7年3月
Microsoft 365 Business Standard ライセンス	30	User	4	月	令和6年4月～令和6年7月
Microsoft 365 Business Standard ライセンス	50	User	8	月	令和6年8月～令和7年3月
Enterprise Mobility + Security E3 ライセンス	50	User	8	月	令和6年8月～令和7年3月
SKYSEA ClientView Professional Edition (ガバメント) サーバーライセンス	1	台	1	年	令和6年8月～令和7年3月
SKYSEA ClientView Professional Edition (ガバメント) クライアントライセンス	350	台	1	年	令和6年8月～令和7年3月
IntraGuadian2+ (アプライアンスサーバー)	10	台	—	—	令和6年11月設置
SKYSEAサーバー用IaaS環境 (Azure等) VPN接続対応含む	1	台	4	月	令和6年8月～令和7年3月
Trend Micro ウイルスバスター ビジネスセキュリティサービス	350	台	8	月	令和6年8月～令和7年3月
Trellix HX	350	台	8	月	令和6年8月～令和7年3月
Trend Micro Email Security	350	台	8	月	令和6年8月～令和7年3月

### 3 設計及び導入作業

#### (1) プロジェクト管理

以下の項目のプロジェクト管理を滞りなく実施すること。

- ①進捗管理
- ②品質管理
- ③人的資源管理
- ④課題管理
- ⑤構成及び変更管理
- ⑥リスク管理
- ⑦情報セキュリティ管理

## (2) 移行計画

移行計画書を作成のうえ、事前に財団の承認を得ること。なお、令和6年度には職員用端末の更改（本調達の範囲外）を予定していることから、端末が切替わることを前提とした、効率的で負荷の少ない移行計画とすること。移行計画にはシステム切替計画のほか、テスト計画（単体テスト、結合テスト、総合テスト）を含めること。

## (3) 設 計

上記移行計画を基に各システムの導入において必要な設計を行い、各種設計書等を作成の上、財団の承認を得ること。設計書については財団職員が理解できる内容とすること。設計作業項目は以下を想定している。

- ① Entra ID Joined 導入設計
- ② Entra ID 条件付きアクセス 要件定義、導入設計
- ③ Entra ID SAML連携 導入設計
- ④ Entra ID プロビジョニング 導入設計
- ⑤ Exchange Online 導入設計、移行設計
- ⑥ SharePoint Online 要件定義、導入設計、構築（全庁ポータル）
- ⑦ メールセキュリティ 導入設計
- ⑧ エンドポイントセキュリティ アンチウイルス 導入設計、展開設計
- ⑨ エンドポイントセキュリティ EDR導入設計、展開設計
- ⑩ Intune デバイス管理 要件定義、導入設計、展開設計
- ⑪ Intune AutoPilot 要件定義、導入設計、展開設計
- ⑫ Intune アプリ配布 要件定義、導入設計、展開設計
- ⑬ IT資産管理 導入設計、移行設計、展開設計
- ⑭ IT資産管理 IaaS導入設計
- ⑮ IntraGuardian2+ 導入設計
- ⑯ テスト計画/テストシナリオ作成
- ⑰ 運用設計、運用手順書作成

## (4) 構築、テスト、本稼働判定

- ①設計で定めた内容に基づき構築を行うこと。
- ②構築に必要な機材は受託者が用意すること。ただし、財団が認めた場合には財団の機材の借用を許可するので、移行計画書に明記すること。
- ③テストシナリオ、本稼働判定計画についても受託者が作成し、財団の承認を得ること。
- ④テストシナリオに基づいて事前テストを実施すること。
- ⑤本番稼働判定計画に基づいて仮運用等を行い本稼働の判定を行うものとする。

## (5) 移行

- ①移行切替え日は財団と受託者との協議の上、決定する。
- ②メールの移行（切替え）については、新たに導入する端末の展開スケジュールを考慮し、財団の業務に支障が発生せず、新しい端末からメールが利用できるようにすること。尚、詳細については、財団と協議して決めること。
- ③クライアントPCに対する設定変更やモジュールのインストールが必要な場合は、別途財団が契約する職員用端末更改の受託者（以降、「端末展開ベンダー」という。）と相互に連携を図りながら財団の業務に支障が発生しないようにスムーズな移行を図ること。
- ④端末展開ベンダーがマスターPCを設計/構築する際に、本件に関連するクライアントアプリケーションについて、技術支援及びインストールファイル等の提供を行うこと。
- ⑤既存のサイボウズOfficeクラウドサービスで利用しているメールデータの移行については利用者の負担を極力減らすべく、受託者が一括移行できる方式が望ましい。利用者操作が必要な場合には、利用者操作手順書を作成すること。利用者操作手順書は幅広い年代の利用者が対応する前提で分かりやすい日本語で作成し、財団職員の承認を得ること。

## (6) 稼働支援

- ①システム管理者向けにマニュアルを作成すること。マニュアルの種類、内容については財団と受託者との協議の上決定する。また、そのマニュアルに基づいて財団のシステム管理者向けに、運用引継及び操作指導説明会を実施すること。
- ②移行後の翌営業日は財団立川庁舎に受託者が待機（立会い）すること。待機は8:30-12:00とする。
- ③WindowsPC展開【ヘルプデスク】MS365利用者問い合わせ対応  
WindowsPC導入展開時において、利用者からのMS365（Outlook、SharePoint、Officeソフトなど）に関する各種問い合わせに対応すること。

## 4 導入後の運用支援及びサポート

本番稼働後、以下の運用支援及びサポートを行うこと。

### (1) サーバー及び端末に関する各種問い合わせ対応

今回導入する各種サーバーの運用方法等についての問い合わせに対応すること。  
又、それに関係する端末に関する問い合わせ等についても対応すること。

### (2) 定例会議の実施

四半期に1回程度、定例会議を実施し、運用期間中に発生したシステム運用上の

各種問い合わせなどの課題項目を整理して、課題管理表等の書式で報告すること。  
これらの報告内容については、次年度の契約更新についての参考とする。

### (3) 年度末人事異動サーバーデータ変更対応

財団で年度末に発生する人事異動に対して、各種サーバーで管理しているユーザーや端末アカウント情報等について、追加、変更、削除等の対応を行うこと。

対象の異動データ等については、年度末の1週間前頃に提示する。

### (4) サーバパッチ適用対応

今回導入する各種サーバーについて、運用期間中、脆弱性やセキュリティ対応などのためにリリースされたパッチソフトがある場合は、その適用の必要性等を事前に調査判断した上で、必要なものは適用すること。尚、その適用については、事前に財団の了承を得ること。又、適用については、原則、業務に支障が発生しないように業務時間外に行うこと。

### (5) 端末OSリカバリ等対応

今回導入するMicrosoft365システムは、端末OSと密に連携して動作するシステムであるため、Windowsアップデート時の不具合、マルウェアやウイルス感染、ファイルの誤削除、アプリケーションソフト不具合、接続機器の影響等様々な要因でOSが起動しなくなった場合は、端末納入業者と連携し、障害の切り分けを行い、OSのリカバリ等の復旧対応を行うこと。尚、ハード障害の場合は、端末納入業者が対応するものとするが、修理後、工場出荷状態に戻った端末については、元の状態に戻すための必要なキッティング等について対応すること。月2回程度の発生を想定している。

### (6) システム管理者向けサポート

クラウドサービス利用におけるシステム管理者向けの電話サポートを提供すること。電話受付時間は平日9:00-17:00の対応が可能であること。

### (7) 電話サポート／オンサイト対応

電話サポートは、運用、環境、操作および障害の原因切り分けに関する問合せを受け付け、解決を図ること。電話サポートで解決できない場合には、財団が受託者にオンサイトでの対応を要求する場合があるので対応すること。

### (8) ログの収集等

受託者のサポートセンターからリモートにて、サポート上で必要なログの収集等の調査を実施できること。

### (9) ユーザー数の変更等

ユーザー数の変更、実体の変更に関しては財団と協議の上、変更できるものとする。

## 5 履行体制

### (1) プロジェクト計画書の策定

受託者は、本業務を確実に履行できる体制を確立し、体制図、工程スケジュール、作業の進め方等を記載したプロジェクト計画書を契約締結後、速やかに提出すること。

### (2) 納入物

次の納入物を印刷物及び電子媒体（CD-ROM等）で1部を提供すること。

- ①プロジェクト計画書
- ②進捗管理表
- ③課題管理表
- ④議事録
- ⑤移行計画書
- ⑥テスト計画書兼テスト結果報告書
- ⑦各種システム設計書
- ⑧各種システム設定書（パラメータシート）
- ⑨システム管理者向け運用手順書
- ⑩メールデータ移行手順書

(3) 受託者は、設計・構築期間中、財団と定期的に打合せを実施して、進捗状況等を報告すること。

(4) 財団は、本業務の履行に関して、受託者に対し説明を求め、また、補足資料の提出を要求することができる。

## 6 その他

(1) 現在利用中のMicrosoft365テナントが継続して利用可能であり、データ等が引き継がれるように必要な対応及び処置を行うこと。又、そのために現在の業者との連携が必要な場合は、打合せの実施などを自ら行うこと、尚、これらに係わる費用は全て受託費用に含むものとする。

(2) クラウドサービス提供元の仕様変更が発生した場合は、財団と受託者との協議の上、誠意をもって対応すること。なお、クラウドサービスの中断又は終了等による措置を取らざるを得ない場合、他のクラウドサービスへの円滑な移行等の対策を講じること。

(3) クラウド利用期間終了後は、全ての情報を復元が困難な状態すること。作業完了後は、消去作業完了報告書（書式は任意）を提出すること。

(4) 本仕様書の解釈について疑義が生じた場合は財団と協議して処理するものとする。

## 電子情報処理委託に係る標準特記仕様書

委託者から電子情報処理の委託を受けた受託者は、契約書及び仕様書等に定めのない事項について、この特記仕様書に定める事項に従って契約を履行しなければならない。

### 1 サイバーセキュリティポリシーを踏まえた業務の履行

受託者は、公益財団法人東京都農林水産振興財団（以下「財団」という。）サイバーセキュリティ基本方針及び財団サイバーセキュリティ対策基準の趣旨を踏まえ、以下の事項を遵守しなければならない。

### 2 業務の推進体制

- (1) 受託者は、契約締結後直ちに委託業務を履行できる体制を整えるとともに、当該業務に関する責任者、作業体制、連絡体制及び作業場所についての記載並びにこの特記仕様書を遵守し業務を推進する旨の誓約を書面にし、委託者に提出すること。
- (2) (1)の事項に変更が生じた場合、受託者は速やかに変更内容を委託者に提出すること。

### 3 業務従事者への遵守事項の周知

- (1) 受託者は、この契約の履行に関する遵守事項について、委託業務の従事者全員に対し十分に説明し周知徹底を図ること。
- (2) 受託者は、(1)の実施状況を書面にし、委託者に提出すること。

### 4 秘密の保持

受託者は、この契約の履行に関して知り得た秘密を漏らしてはならない。この契約終了後も同様とする。

### 5 目的外使用の禁止

受託者は、この契約の履行に必要な委託業務の内容を他の用途に使用してはならない。また、この契約の履行により知り得た内容を第三者に提供してはならない。

### 6 複写及び複製の禁止

受託者は、この契約に基づく業務を処理するため、委託者が貸与する原票、資料、その他貸与品等及びこれらに含まれる情報（以下「委託者からの貸与品等」という。）を、委託者の承諾なくして複写及び複製をしてはならない。

### 7 作業場所以外への持出禁止

受託者は、委託者が指示又は承認する場合を除き、委託者からの貸与品等（複写及び複製したものを含む。）について、2(1)における作業場所以外へ持ち出してはならない。

### 8 情報の保管及び管理

受託者は、委託業務に係る情報の保管及び管理に万全を期するため、委託業務の実施に当たって以下の事項を遵守しなければならない。

- (1) 全般事項
  - ア 契約履行過程

(ア) 以下の事項について安全管理上必要な措置を講じること。

- a 委託業務を処理する施設等の入退室管理
- b 委託者からの貸与品等の使用及び保管管理
- c 仕様書等で指定する物件（以下「契約目的物」という。）、契約目的物の仕掛品及び契約履行過程で発生した成果物（出力帳票及び電磁的記録物等）の作成、使用及び保管管理
- d その他、仕様書等で指定したもの

(イ) 委託者から(ア)の内容を確認するため、委託業務の安全管理体制に係る資料の提出を求められた場合は直ちに提出すること。

#### イ 契約履行完了時

(ア) 委託者からの貸与品等を、契約履行完了後速やかに委託者に返還すること。

(イ) 契約目的物の作成のために、委託業務に係る情報を記録した一切の媒体（紙及び電磁的記録媒体等一切の有形物）（以下「記録媒体」という。）については、契約履行完了後に記録媒体上に含まれる当該委託業務に係る情報を全て消去すること。

(ウ) (イ)の消去結果について、記録媒体ごとに、消去した情報項目、数量、消去方法及び消去日等を明示した書面で委託者に報告すること。

(エ) この特記仕様書の事項を遵守した旨を書面で報告すること。また、再委託を行った場合は再委託先における状況も同様に報告すること。

#### ウ 契約解除時

イの規定の「契約履行完了」を「契約解除」に読み替え、規定の全てに従うこと。

#### エ 事故発生時

契約目的物の納入前に契約目的物の仕掛品、契約履行過程で発生した成果物及び委託者からの貸与品等の紛失、滅失及び毀損等の事故が生じたときには、その事故の発生場所及び発生状況等を詳細に記載した書面をもって、遅滞なく委託者に報告し、委託者の指示に従うこと。

#### (2) アクセスを許可する情報に係る事項

受託者は、アクセスを許可する情報の種類と範囲、アクセス方法について、業務着手前に委託者から承認を得ること。

#### (3) 個人情報及び機密情報の取扱いに係る事項

委託者からの貸与品等及び契約目的物に記載された個人情報は、全て委託者の保有個人情報である（以下「個人情報」という。）。また、委託者が機密を要する旨を指定して提示した情報及び委託者からの貸与品等に含まれる情報は、全て委託者の機密情報である（以下「機密情報」という。）。ただし、委託者からの貸与品等に含まれる情報のうち、既に公知の情報、委託者から受託者に提示した後に受託者の責めによらないで公知となった情報、及び委託者と受託者による事前の合意がある情報は、機密情報に含まれないものとする。

個人情報及び機密情報の取扱いについて、受託者は、以下の事項を遵守しなければならない。

ア 個人情報及び機密情報に係る記録媒体を、施錠できる保管庫又は施錠及び入退室管理の可能な保管室に格納する等適正に管理すること。

イ アの個人情報及び機密情報の管理に当たっては、管理責任者を定めるとともに、台帳等を設け個人情報及び機密情報の管理状況を記録すること。

ウ 委託者から要求があった場合又は契約履行完了時には、イの管理記録を委託者に提出し報告すること。

エ 個人情報及び機密情報の運搬には盗難、紛失、漏えい等の事故を防ぐ十分な対策を講じること。

オ (1)イ(イ)において、個人情報及び機密情報に係る部分については、あらかじめ消去すべき情報項目、数量、消去方法及び消去予定日等を書面により委託者に申し出て、委託者の承諾を得るとともに、委託者の立会いのもとで消去を行うこと。

カ (1)エの事故が、個人情報及び機密情報の漏えい、滅失、毀損等に該当する場合は、漏えい、

滅失、毀損した個人情報及び機密情報の項目、内容、数量、事故の発生場所及び発生状況等を詳細に記載した書面をもって、遅滞なく委託者に報告し、委託者の指示に従うこと。

キ カの事故が発生した場合、受託者は二次被害の防止、類似事案の発生回避等の観点から、委託者に可能な限り情報を提供すること。

ク (1)エの事故が発生した場合、委託者は必要に応じて受託者の名称を含む当該事故に係る必要な事項の公表を行うことができる。

ケ 委託業務の従事者に対し、個人情報及び機密情報の取扱いについて必要な教育及び研修を実施すること。なお、教育及び研修の計画及び実施状況を書面にて委託者に提出すること。

コ その他、個人情報の保護に関する法律（平成15年法律第57号）に従って、本委託業務に係る個人情報を適切に扱うこと。

## 9 委託者の施設内での作業

(1) 受託者は、委託業務の実施に当たり、委託者の施設内で作業を行う必要がある場合には、委託者に作業場所、什器、備品及び通信施設等の使用を要請することができる。

(2) 委託者は、(1)の要請に対して、使用条件を付した上で、無償により貸与又は提供することができる。

(3) 受託者は、委託者の施設内で作業を行う場合は、次の事項を遵守するものとする。

ア 就業規則は、受託者の定めるものを適用すること。

イ 受託者の発行する身分証明書を携帯し、委託者の指示があった場合はこれを提示すること。

ウ 受託者の社名入りネームプレートを着用すること。

エ その他、(2)の使用に関し委託者が指示すること。

## 10 再委託の取扱い

(1) 受託者は、この契約の履行に当たり、再委託を行う場合には、あらかじめ再委託を行う旨を書面により委託者に申し出て、委託者の承諾を得なければならない。

(2) (1)の書面には、以下の事項を記載するものとする。

ア 再委託の理由

イ 再委託先の選定理由

ウ 再委託先に対する業務の管理方法

エ 再委託先の名称、代表者及び所在地

オ 再委託する業務の内容

カ 再委託する業務に含まれる情報の種類（個人情報及び機密情報については特に明記すること。）

キ 再委託先のセキュリティ管理体制（個人情報、機密情報、記録媒体の保管及び管理体制については特に明記すること。）

ク 再委託先がこの特記仕様書の1及び3から9までに定める事項を遵守する旨の誓約

ケ その他、委託者が指定する事項

(3) この特記仕様書の1及び3から9までに定める事項については、受託者と同様に、再委託先においても遵守するものとし、受託者は、再委託先がこれを遵守することに関して一切の責任を負う。

## 11 実地調査及び指示等

(1) 委託者は、必要があると認める場合には、受託者の作業場所の実地調査を含む受託者の作業状況の調査及び受託者に対する委託業務の実施に係る指示を行うことができる。

(2) 受託者は、(1)の規定に基づき、委託者から作業状況の調査の実施要求又は委託業務の実施に係る指示があった場合には、それらの要求又は指示に従わなければならない。

(3) 委託者は、(1)に定める事項を再委託先に対しても実施できるものとする。

## 12 情報の保管及び管理等に対する義務違反

- (1) 受託者又は再委託先において、この特記仕様書の3から9までに定める情報の保管及び管理等に関する義務違反又は義務を怠った場合には、委託者は、この契約を解除することができる。
- (2) (1)に規定する受託者又は再委託先の義務違反又は義務を怠ったことによって委託者が損害を被った場合には、委託者は受託者に損害賠償を請求することができる。委託者が請求する損害賠償額は、委託者が実際に被った損害額とする。

## 13 契約不適合責任

- (1) 契約目的物に、その契約の内容に適合しないものがあるときは、委託者は、受託者に対して相当の期間を定めてその修補による履行の追完又はこれに代えて若しくは併せて損害の賠償を請求することができる。
- (2) (1)の規定によるその契約の内容に適合しないものの修補による履行の追完又はこれに代えて若しくは併せて行う損害賠償の請求に伴う通知は、委託者がその不適合を知った日から1年以内に、これを行わなければならない。

## 14 著作権等の取扱い

この契約により作成される納入物の著作権等の取扱いは、以下に定めるところによる。

- (1) 受託者は、納入物のうち本委託業務の実施に伴い新たに作成したものについて、著作権法（昭和45年法律第48号）第2章第3節第2款に規定する権利（以下「著作者人格権」という。）を有する場合においてもこれを行使しないものとする。ただし、あらかじめ委託者の承諾を得た場合はこの限りでない。
- (2) (1)の規定は、受託者の従業員、この特記仕様書の10の規定により再委託された場合の再委託先又はそれらの従業員に著作者人格権が帰属する場合にも適用する。
- (3) (1)及び(2)の規定については、委託者が必要と判断する限りにおいて、この契約終了後も継続する。
- (4) 受託者は、納入物に係る著作権法第2章第3節第3款に規定する権利（以下「著作権」という。）を、委託者に無償で譲渡するものとする。ただし、納入物に使用又は包括されている著作物で受託者がこの契約締結以前から有していたか、又は受託者が本委託業務以外の目的で作成した汎用性のある著作物に関する著作権は、受託者に留保され、その使用权、改変権を委託者に許諾するものとし、委託者は、これを本委託業務の納入物の運用その他の利用のために必要な範囲で使用、改変できるものとする。また、納入物に使用又は包括されている著作物で第三者が著作権を有する著作物の著作権は、当該第三者に留保され、かかる著作物に使用許諾条件が定められている場合は、委託者はその条件の適用につき協議に応ずるものとする。
- (5) (4)は、著作権法第27条及び第28条に規定する権利の譲渡も含む。
- (6) 本委託業務の実施に伴い、特許権等の産業財産権を伴う発明等が行われた場合、取扱いは別途協議の上定める。
- (7) 納入物に関し、第三者から著作権、特許権、その他知的財産権の侵害の申立てを受けた場合、委託者の帰責事由による場合を除き、受託者の責任と費用をもって処理するものとする。

## 15 運搬責任

この契約に係る委託者からの貸与品等及び契約目的物の運搬は、別に定めるものを除くほか受託者の責任で行うものとし、その経費は受託者の負担とする。

## 個人情報に関する特記事項

### (定義)

第1 本業務において、公益財団法人東京都農林水産振興財団（以下、「財団」という。）の保有する個人情報（以下、「個人情報」という。）とは、財団が貸与する原票、資料、貸与品等に記載された個人情報及びこれらの情報から受託者が作成した個人情報並びに受託者が財団に代わって行う本業務の過程で収集した個人情報の全てをいい、受託者独自のもものと明確に区分しなければならない。

### (個人情報の保護に係る受託者の責務)

第2 受託者は、この契約の履行に当たって、個人情報を取り扱う場合は、「個人情報の保護に関する法律」（平成15年法律第57号）を遵守して取り扱う責務を負い、以下の事項を遵守し、個人情報の漏えい、滅失、き損の防止その他個人情報保護に必要な措置を講じなければならない。

### (再委託の禁止)

第3 受託者は、この契約書に基づく委託業務を第三者に委託してはならない。ただし、委託業務全体に大きな影響を及ぼさない補助的業務についてあらかじめ財団の書面による承諾を得た場合にはこの限りでない。

2 前項ただし書きに基づき財団に承諾を求める場合は、再委託の内容、そこに含まれる情報、再委託先、個人情報管理を含めた再委託先に対する管理方法等を文書で提出しなければならない。

### (秘密の保持)

第4 受託者は、第3第1項ただし書きにより財団が承認した場合を除き、委託業務の内容を第三者に漏らしてはならない。この契約終了後も同様とする。

2 第3第1項ただし書きにより、財団が承認した再委託先についても、同様の秘密保持に関する責務を課し、受託者が全責任を負って管理するものとする。

### (目的外使用の禁止)

第5 受託者は、この契約の履行に必要な委託業務の内容を他の用途に使用してはならない。また、第3第1項ただし書きにより財団が承認した部分を除き、契約の履行により知り得た内容を第三者に提供してはならない。

### (複写複製の禁止)

第6 受託者は、この契約に基づく業務を処理するため、財団から引き渡された原票、資料、貸与品等がある場合は、財団の承諾なくして複写又は複製してはならない。

### (個人情報の管理)

第7 受託者は、財団から提供された原票、資料、貸与品等のうち、個人情報に係るもの及び受託者が契約履行のために作成したそれらの記録媒体については、施錠できる保管庫又は施錠入退管理の可能な保管室に格納するなど適正に管理しなければならない。

2 受託者は、前項の個人情報の管理に当たっては、管理責任者を定めるとともに、台帳等を設け個人情報の管理状況を記録しなければならない。

3 受託者は、財団から要求があった場合には、前項の管理記録を財団に提出しなければならない。

### (受託者の安全対策と管理体制資料の提出)

第8 受託者は、委託業務の適正かつ円滑な履行を図るとともに個人情報保護に万全を期するため、

委託業務の実施に当たって使用する受託者の管理下の施設において、以下の事項について安全管理上必要な措置を講じなければならない。

- (1) 委託業務を処理する施設等の入退室管理
- (2) 財団から提供された、原票、資料、貸与品等の使用保管管理
- (3) 契約履行過程で発生した業務記録、成果物等（出力帳票及び磁気テープ、フロッピー等の磁気媒体を含む。）の作成、使用、保管管理
- (4) その他仕様等で指定したもの。

2 財団は、前項の内容を確認するため、受託者に対して、個人情報の管理を含めた受託者の安全管理体制全般に係る資料の提出を求めることができる。

#### **（財団の検査監督権）**

第9 財団は、必要があると認める場合には、受託者の作業現場の実地調査を含めた受託者の個人情報の管理状況に対する検査監督及び作業の実施に係る指示を行うことができる。

2 受託者は、財団から前項に基づく検査実施要求、作業の実施に係る指示があった場合には、それらの要求、指示に従わなければならない。

#### **（資料等の返還）**

第10 受託者は、この契約による業務を処理するため財団から引き渡された原票、資料及び貸与品等並びに受託者が収集した個人情報に係る資料等を、委託業務完了後速やかに財団に返還しなければならない。

2 前項の返還時に、個人情報に係るものについては、第7第2項に定める個人情報の管理記録を併せて提出し報告しなければならない。

#### **（記録媒体上の情報の消去）**

第11 受託者は、受託者の保有する記録媒体（磁気ディスク、紙等の媒体）上に保有する、委託処理に係る一切の情報について、委託業務終了後、全て消去しなければならない。

2 第3第1項ただし書きにより財団が承認した再委託先がある場合には、再委託先の情報の消去について受託者が全責任を負うとともに、その状況を前項の報告に含め財団に報告しなければならない。

#### **（事故発生の通知）**

第12 受託者は、委託業務の完了前に事故が生じたときには、速やかにその状況を書面をもって財団に通知しなければならない。

2 前項の事故が、個人情報の漏えい、滅失、き損等の場合には、漏えい、滅失、き損した個人情報の項目、内容、数量、事故の発生場所及び発生状況等を詳細に記載した書面をもって、速やかに財団に報告し、財団の指示に従わなければならない。

#### **（財団の解除権）**

第13 財団は、受託者の個人情報の保護に問題があると認める場合はこの契約を解除することができる。

#### **（疑義についての協議）**

第14 この取扱事項の各項目若しくは仕様書で規定する個人情報の管理方法等について疑義等が生じたとき又はこの取扱事項若しくは仕様書に定めのない事項については、両者協議の上定める。

## 東京都グリーン購入推進方針

物品等の調達に当たっては、その必要性をよく考えた上で、価格・機能・品質だけでなく、環境への負荷ができるだけ少ないものを選択して購入することとする。

その際、可能な限り、原材料の採取から製品やサービスの生産、流通、使用、廃棄に至るまでのライフサイクルにおいて環境への負荷が少ないものを選択することが必要である。

特に、脱炭素化や HTTP の推進、サーキュラーエコノミーの推進に寄与する製品やサービスを積極的に選択することで、物品等の調達を通じ、全庁をあげて環境課題に対応していくことが重要である。

そこで、調達する各製品やサービスごとに、適正な価格・機能・品質を確保しつつ、以下の観点で他の製品等と比較して、相対的に環境負荷の少ないものを選択することとする。

### <原材料の採取段階での環境配慮>

- ① 原材料の採取において資源の持続可能な利用に配慮されているもの
- ② 原材料が違法に採取されたものではないもの
- ③ 原材料の採取が保護価値の高い生態系に影響を与えていないなど、生物多様性の損失を引き起こしていないもの
- ④ 原材料の採取において環境汚染及び多量の温室効果ガスの排出を伴わないもの

### <製造段階での環境配慮>

- ⑤ 再生材料（再生紙、再生樹脂等）を使用したもの
- ⑥ 余材、廃材（間伐材、小径材等）を使用したもの
- ⑦ 再生しやすい材料を使用したもの

### <使用段階での環境配慮>

- ⑧ 使用時の資源やエネルギーの消費が少ないもの
- ⑨ 修繕や部品の交換・詰め替えが可能なもの
- ⑩ 梱包・包装が簡易なもの、又は梱包・包装材に環境に配慮した材料を使用したもの

### <廃棄・リサイクル段階での環境配慮>

- ⑪ 分別廃棄やリサイクルがしやすい（単一素材、分離可能等）もの
- ⑫ 回収・リサイクルシステムが確立しているもの
- ⑬ 耐久性が高く、長期使用が可能なもの

### <その他の環境配慮>

- ⑭ 製造・使用・廃棄等の各段階で、有害物質を使用又は排出しないもの
- ⑮ 製造・使用・廃棄等の各段階で、環境への負荷が大きい物質（温室効果ガス等）の使用、排出が少ないもの
- ⑯ 製造・使用・廃棄等の各段階で、生物多様性の損失を引き起こさないもの