

テレワーク用パーソナルコンピュータの購入253式 仕様書

I 調達案件の概要に関する事項

東北農政局では、本省を中心にテレワークの取組を拡大しているところであり、政府機関の働き方改革の推進を踏まえモバイルワークの実現を図るため、持ち運びが容易な軽量のノート型の端末を選定することとする。

II 調達案件及び関連調達案件の調達単位、調達の方式等に関する事項

東北農政局が実施する本調達については以下のとおりである。

東北農政局テレワーク用端末購入

【一般競争入札（最低価格落札方式）】

職員がテレワークで利用するための端末を調達するもの。

III 導入作業等

1 調達物品

ノート型端末（電源アダプタ等の付属品を含む。） 253式

2 納入場所及び期限

（1）納入場所

宮城県仙台市青葉区本町3-3-1 仙台合同庁舎A棟
東北農政局

（2）納入期限

令和3年3月29日（月）

3 端末の基本要件

本業務で調達する端末については、下記4の（1）、（2）に掲げる要件を満たすもの、又はこれと同等以上の性能等を有するものとし、「環境物品等の調達の推進に関する基本方針」（令和2年2月7日変更閣議決定）に対応していること。

また、ハードウェア及びOSが一体として運用できるものであり、かつ、農林水産省行政情報システムと接続した場合にも、起動後良好な運用ができる操作性の良い端末とし、東北農政局の職員が業務で支障なく使用できるものとする。

4 機能等

（1）ハードウェア

項目	要件
形状等	ノート型であり同一機種未使用品であること。
キーボード	JIS 配列準拠。原則としてキーピッチは 18mm 以上で、タッチパッドを内蔵すること。
CPU 種別	第 7 世代以降の Intel Core i3 プロセッサ同等以上
メインメモリ	8 GB 以上
ストレージ (HDD/SSD)	HDD 又は SSD を内蔵すること。 HDD の場合は 500GB 以上とし、C ドライブに 200GB を割り当て、残りを D ドライブとする。 SSD の場合は 250GB 以上とし、C ドライブに 150GB を割り当て、残りを D ドライブとする。 TPM を使用して保存領域を暗号化できること。
液晶パネル	13.0 型以上 15.6 型以下で、解像度 1366×768 以上の液晶パネル (TFT カラー) とすること。
外部映像出力	解像度 1920×1080 ドットの出力が可能な HDMI (標準サイズ) 出力端子又は VGA (D-Sub15 ピン) 出力端子を備えること。 なお、外付けドック等で対応することを可とする。
有線 LAN	1000BASE-T/100BASE-TX/10BASE-T 準拠の LAN 接続端子 (RJ-45) を備えること。 なお、外付けドック等で対応することを可とする。
無線 LAN	IEEE802.11a/b/g/n/ac 及び Wi-Fi に準拠している無線 LAN 機能を備えること。
内蔵カメラ	Web カメラが備わっていること。
音声入出力	マイク入力及びヘッドフォン出力を備えること。 なお、共用端子 (オーディオコンボジャック) で対応することも可とする。
USB ポート	USB2.0 以降に対応した Type-A のポートを 2 つ以上備えること。うち少なくとも 1 ポートは 3.0 又は 3.1 に対応していること。 なお、LAN 接続端子 (RJ-45) や外部映像出力を外付けドック等で対応する場合、それらを接続しても上述のポート数の空きが確保されること。
電源バッテリー	JEITA バッテリー動作時間測定法 Ver. 2.0 で 7 時間以上稼働可能なバッテリーを内蔵すること。

項目	要件
マウス	全機毎に USB 光学式ホイール付きマウス又はレーザー式ホイール付きマウスを装備すること。
その他	盗難防止用ロック取り付け穴を備えること。
電源	AC アダプタ及び電源ケーブルを添付すること。電圧は AC100V～240V に対応していること。

(2) ソフトウェア

項目	要件
OS	Windows 10 Pro (64bit・日本語)
インターネットブラウザ	Microsoft Internet Explorer 11
SSL-VPN クライアントソフト	発注者が用意する SSL-VPN クライアントソフトウェアをインストールすること。

(3) ソフトウェアライセンス

本業務においてソフトウェアライセンスを調達する場合は、より安価となるよう以下を踏まえて調達すること。

① Microsoft Windows OS

OEMライセンス（プリインストール）又はMicrosoft Open License for Governmentで調達すること。

② トレンドマイクロ ウイルスバスター

トレンドマイクロ社のウイルスバスターのライセンス253式について、農林水産省大臣官房広報評価課情報管理室で現行保有している以下のライセンスを追加する形で調達すること。

- ・製品名：TRSL C/S Suite Premium ガバメント
- ・ライセンスID：54515
- ・期間：2020/4/1～2021/3/31

なお、ウイルスバスターのインストール作業は、発注者側で行うためインストール作業は必要ない。

5 導入・設定作業

受注者は、以下のとおり設定作業等を行い、納品すること。

(1) 初期端末及びリカバリ用メディアの作成

- ① 上記4の要件を満たす端末（以下「初期端末」という。）を受注者が用意する施設において作成すること。なお、端末の設定に必要な設定情報については発注者から提示する。

- ② 端末のストレージに対して4の(2)のソフトウェアを全てインストールし設定を終えた状態へ復元する「リカバリ用メディア」(USBフラッシュメモリ又はCD-R又はDVD-R(ドライブが付属されている場合))及びリカバリの手順を記した「リカバリマニュアル」を作成し、端末の納入期限までに3式納品すること。
- ③ 初期端末において、発注者から設定内容等の確認を得た上で他の端末への展開を行うこと。

(2) 端末の設定作業等

設定作業の詳細は以下のとおり。

- ① 設定作業の実施場所
設定作業は受注者が用意する施設において行うこと。
- ② コンピュータ名の設定
端末のコンピュータ名を発注者から提示された名称に設定すること。
なお、コンピュータ名を決定するために必要な情報として、端末のシリアル番号一覧を発注者に提出することとし、一覧の提出期限については発注者と協議すること。

(3) 端末等の納品

端末の納入期限までに「設定作業が完了した端末」を納品すること。詳細は以下のとおり。

- ① 納入については、運搬日時、配布手順等について十分に打合せを行い、拠点の業務に支障のないようにすること。
- ② 端末の運搬に当たっては、紛失、破損等の事故が起きないように十分に注意し、運搬に必要な資材等は受注者の負担で準備すること。

(4) ラベルの貼付

本調達で納品された端末、ACアダプタ及びマウスについて、コンピュータ名を記したラベルを端末に貼付すること。

(5) その他

端末の配布作業が全て終了した後5日(行政機関の休日を含まない。)以内に、作業終了日、作業内容等を記した「作業完了報告書」を発注者へ提出すること。

6 成果物の提出

成果物(納品物に含まれる書類)は、全て日本語で作成すること。

用字・用語・記述符号の表記については、「公用文作成の要領(昭和27年4月4日内閣閣令第16号内閣官房長官依命通知)」を参考にすること。
情報処理に関する用語の表記については、日本産業規格(JIS)の規定を参考にすること。

成果物は紙媒体及び電磁的記録媒体により作成し、納品すること。

紙媒体による納品について、用紙のサイズは、原則として日本産業規格 A 列 4 番とするが、必要に応じて日本産業規格 A 列 3 番を使用すること。

電磁的記録媒体による納品について、原則としてMicrosoft Office形式及びPDF形式の双方を収録することとし、Office形式で作成されていない既存の製品マニュアル等についてはPDF形式のみの収録を可とする。

なお、原則として、納品物は納入場所において引渡しを行うこと。ただし、発注者が納品場所を別途指示する場合はこの限りではない。

(1) 成果物

納品物名	数量	納入期限
「リカバリ用メディア」	3	端末の納入期限まで
「リカバリマニュアル」	3 (紙媒体) 1 (電磁的記録媒体)	端末の納入期限まで
導入作業に係る「作業完了報告書」	1 (紙媒体)	作業終了後 5 日以内

7 保守に関する事項

受注者は、端末の納入期限から 1 年間について以下の対応が可能であること。

(1) 問合せ対応

開庁日の 9 時から 17 時までの間、発注者からの修理依頼等の電話受付を実施すること。

(2) 不具合対応

納入後 1 年以内に、納入したハードウェアの不具合が明らかとなり、修理、交換等の必要が生じた場合には、発注者と協議の上で受注者の責任において不具合の解消のために必要な作業を実施すること。

VI 作業の実施に当たっての遵守事項

1 責任の所在

納品した端末等については、製造者の如何に関わらず、受注者が最終的に責任を負うこと。

(1) 発注者は検収完了後、納入物についてシステム仕様書との不一致(バグも含む。

以下「契約不適合」という。)が発見された場合、受注者に対して当該契約不適合の修正等の履行の追完(以下「追完」という。)を請求することができ、受注者は、当該追完を行うものとする。但し、発注者に不相当な負担を課するものでないときは、受注者は発注者が請求した方法と異なる方法による追完を行うことができること。

(2) 前項にかかわらず、当該契約不適合によっても個別契約の目的を達することができる場合であって、追完に過分の費用を要する場合、受注者は前項所定の追完

義務を負わないものとする。

- (3) 発注者は、当該契約不適合（受注者の責めに帰すべき事由により生じたものに限る。）により損害を被った場合、受注者に対して損害賠償を請求することができること。
- (4) 当該契約不適合について、追完の請求にもかかわらず相当期間内に追完がなされない場合又は追完の見込みがない場合で、当該契約不適合により個別契約の目的を達することができないときは、発注者は本契約及び個別契約の全部又は一部を解除することができること。
- (5) 受注者が本項に定める責任その他の契約不適合責任を負うのは、検収完了後1年以内に発注者から当該契約不適合を通知された場合に限るものとする。但し、検収完了時において受注者が当該契約不適合を知り若しくは重過失により知らなかった場合、又は当該契約不適合が受注者の故意若しくは重過失に起因する場合にはこの限りでない。
- (6) 前各項の要件は、契約不適合が発注者の提供した資料等又は発注者の与えた指示によって生じたときは適用しないこと。但し、受注者がその資料等又は指示が不相当であることを知りながら告げなかったときはこの限りでない。

2 情報セキュリティの確保

- (1) 受注者は本契約の遂行に当たり、別紙1「情報セキュリティの確保に関する共通基本仕様」（以下「セキュリティ共通仕様」という。）の内容について、本業務に係る事項について遵守すること。
- (2) 納入候補となる機器について、11月9日（月）正午までに、発注者へ機器等リスト（区分（ノートPC等）、製造業者名、製造業者の法人番号、製品名及び型番を記載したリスト）を提出することとし、発注者においてサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、速やかに発注者に確認した上で、代替品の選定等、納入候補となる機器を見直すこと。

V その他特記事項

詳細な事項及び本仕様書等に定めのない事項で必要と認められる作業は、発注者と協議し決定すること。

別紙1

情報セキュリティの確保に関する共通基本仕様

I 情報セキュリティポリシーの遵守

- 1 受託者は、担当部署から農林水産省における情報セキュリティの確保に関する規則（平成27年農林水産省訓令第4号。以下「規則」という。）等の説明を受けるとともに、本業務に係る情報セキュリティ要件を遵守すること。

なお、規則は、政府機関等の情報セキュリティ対策のための統一基準群（以下「統一基準群」という。）に準拠することとされていることから、受託者は、統一基準群の改定を踏まえて規則が改正された場合には、本業務に関する影響分析を行うこと。

- 2 受託者は、規則と同等の情報セキュリティ管理体制を整備していること。
- 3 受託者は、本業務の従事者に対して、規則と同等の情報セキュリティ対策の教育を実施していること。

II 受託者及び業務実施体制に関する情報の提供

- 1 受託者は、受託者の資本関係・役員等の情報、本業務の実施場所、本業務の従事者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）の所属・専門性（保有資格、研修受講実績等）・実績（業務実績、経験年数等）及び国籍に関する情報を記載した資料を提出すること。

なお、本業務に従事する全ての要員に関する情報を記載することが困難な場合は、本業務に従事する主要な要員に関する情報を記載するとともに、本業務に従事する部門等における従事者に関する情報（〇〇国籍の者が△名（又は□%）等）を記載すること。また、この場合であっても、担当部署からの要求に応じて、可能な限り要員に関する情報を提供すること。

- 2 受託者は、本業務を実施する部署、体制等の情報セキュリティ水準を証明する以下のいずれかの証明書等の写しを提出すること。（提出時点で有効期限が切れていないこと。）

- (1) ISO/IEC27001等の国際規格とそれに基づく認証の証明書等
- (2) プライバシーマーク又はそれと同等の認証の証明書等
- (3) IPAが公開する「情報セキュリティ対策ベンチマーク」を利用した自己評価を行い、その評価結果において、全項目に係る平均値が4に達し、かつ各評価項目の成熟度が2以上であることが確認できる確認書
- (4) MS 認証信頼性向上イニシアティブに参画し、不祥事への対応や透明性確保に係る取組を実施している実績

III 業務の実施における情報セキュリティの確保

- 1 受託者は、本業務の実施に当たって、以下の措置を講じること。また、以下の措置を講じる

ことを証明する資料を提出すること。

- (1) 本業務上知り得た情報(公知の情報を除く。)については、契約期間中はもとより契約終了後においても第三者に開示及び本業務以外の目的で利用しないこと。
 - (2) 本業務に従事した要員が異動、退職等をした後においても有効な守秘義務契約を締結すること。
 - (3) 本業務の各工程において、農林水産省の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること(例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図、第三者機関による品質保証体制を証明する書類等を提出すること。)
 - (4) 本業務において、農林水産省の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入調査等、農林水産省と連携して原因を調査し、排除するための手順及び体制(例えば、システムの操作ログや作業履歴等を記録し、担当部署から要求された場合には提出するなど)を整備していること。
 - (5) 本業務において、個人情報又は農林水産省における要機密情報を取り扱う場合は、当該情報(複製を含む。以下同じ。)を国内において取り扱うものとし、当該情報の国外への送信・保存や当該情報への国外からのアクセスを行わないこと。
 - (6) 本業務における情報セキュリティ対策の履行状況を定期的に報告すること。
 - (7) 農林水産省が情報セキュリティ監査の実施を必要と判断した場合は、農林水産省又は農林水産省が選定した事業者による立入調査等の情報セキュリティ監査(サイバーセキュリティ基本法(平成26年法律第104号)第25条第1項第2号に基づく監査等を含む。以下同じ。)を受け入れること。また、担当部署からの要求があった場合は、受託者が自ら実施した内部監査及び外部監査の結果を報告すること。
 - (8) 本業務において、要安定情報を取り扱うなど、担当部署が可用性を確保する必要があると認めた場合は、サービスレベルの保証を行うこと。
 - (9) 本業務において、第三者に情報が漏えいするなどの情報セキュリティインシデントが発生した場合は、担当部署に対し、速やかに電話、口頭等で報告するとともに、報告書を提出すること。また、農林水産省の指示に従い、事態の收拾、被害の拡大防止、復旧、再発防止等に全力を挙げる。なお、これらに要する費用の全ては受託者が負担すること。
 - (10) 情報セキュリティ対策の履行が不十分な場合、農林水産省と協議の上、必要な改善策を立案し、速やかに実施するなど、適切に対処すること。
- 2 受託者は、私物(本業務の従事者個人の所有物等、受託者管理外のものをいう。)の機器等を本業務に用いないこと。
 - 3 受託者は、成果物等を電磁的記録媒体により納品する場合には、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処するとともに、確認結果(確認日時、不正プログラム対策ソフトウェアの製品名、定義ファイルのバージョン等)を成果物等に記載又は添付すること。

- 4 受託者は、本業務において取り扱われた情報を、担当部署の指示に従い、本業務上不要となったとき若しくは本業務の終了までに返却又は復元できないよう抹消し、その結果を担当部署に書面で報告すること。

IV 情報システムの各工程における情報セキュリティの確保

- 1 受託者は、本業務において情報システムの運用管理機能又は設計・開発に係る企画・要件定義を行う場合には、以下の措置を実施すること。

- (1) 情報システム運用時のセキュリティ監視等の運用管理機能を明確化し、本業務の成果物へ適切に反映するために、以下を含む措置を実施すること。

ア 情報システム運用時に情報セキュリティ確保のために必要となる管理機能を本業務の成果物に明記すること。

イ 情報セキュリティインシデントの発生を監視する必要がある場合、監視のために必要な機能について、以下を例とする機能を本業務の成果物に明記すること。

(ア) 農林水産省外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能

(イ) 不正プログラム感染や踏み台に利用されること等による農林水産省外への不正な通信を監視する機能

(ウ) 農林水産省内通信回線への端末の接続を監視する機能

(エ) 端末への外部電磁的記録媒体の挿入を監視する機能

(オ) サーバ装置等の機器の動作を監視する機能

- (2) 開発する情報システムに関連する脆(ぜい)弱性への対策が実施されるよう、以下を含む対策を本業務の成果物に明記すること。

ア 既知の脆(ぜい)弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。

イ 開発時に情報システムに脆(ぜい)弱性が混入されることを防ぐためのセキュリティ実装方針を定めること。

ウ セキュリティ侵害につながる脆(ぜい)弱性が情報システムに存在することが発覚した場合に修正が施されること。

エ ソフトウェアのサポート期間又はサポート打ち切り計画に関する情報を提供すること。

- 2 受託者は、本業務において情報システムの設計・開発を行う場合には、以下の事項を含む措置を適切に実施すること。

- (1) 情報システムのセキュリティ要件の適切な実装

- (2) 情報セキュリティの観点に基づく試験の実施

ア ソフトウェアの開発及び試験を行う場合は、運用中の情報システムと分離して実施すること。

イ 試験項目及び試験方法を定め、これに基づいて試験を実施すること。

- ウ 試験の実施記録を作成し保存すること。
- (3) 情報システムの開発環境及び開発工程における情報セキュリティ対策
 - ア ソースコードが不正に変更されることを防止するため、ソースコードの変更管理、アクセス制御及びバックアップの取得について適切に管理すること。
 - イ 調達仕様書等に規定されたセキュリティ実装方針に従うこと。
 - ウ セキュリティ機能の適切な実装、セキュリティ実装方針に従った実装が行われていることを確認するために、情報システムの設計及びソースコードを精査する範囲及び方法を定め実施すること。
 - エ オフショア開発を実施する場合、試験データとして実データを使用しないこと。
- 3 受託者は、情報セキュリティの観点から調達仕様書で求める要件以外に必要となる措置がある場合には、担当部署に報告し、協議の上、対策を講ずること。
- 4 受託者は、本業務において情報システムの運用・保守を行う場合には、情報システムに実装されたセキュリティ機能が適切に運用されるよう、以下の事項を適切に実施すること。
 - (1) 情報システムの運用環境に課せられるべき条件の整備
 - (2) 情報システムのセキュリティ監視を行う場合の監視手順や連絡方法
 - (3) 情報システムの保守における情報セキュリティ対策
 - (4) 運用中の情報システムに脆(ぜい)弱性が存在することが判明した場合の情報セキュリティ対策
 - (5) 利用するソフトウェアのサポート期限等の定期的な情報収集及び報告
 - (6) 「デジタル・ガバメント推進標準ガイドライン」(平成 30 年 3 月 30 日各府省情報化統括責任者(CIO)連絡会議決定)の別紙 3 に基づく ODB に情報を登録又は更新するために必要な事項を記載した情報システム資産管理用シートの提出
 - (7) 情報システムの利用者に使用を求めるソフトウェアのバージョンのサポート終了時における、サポート継続中のバージョンでの動作検証及び当該バージョンで正常に動作させるための情報システムの改修等
- 5 受託者は、本業務において情報システムの運用・保守を行う場合には、運用保守段階へ移行する前に、移行手順及び移行環境に関して、以下を含む情報セキュリティ対策を行うこと。
 - (1) 情報セキュリティに関わる運用保守体制の整備
 - (2) 運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施
 - (3) 情報セキュリティインシデント(可能性がある事象を含む。以下同じ。)を認知した際の対処方法の確立
- 6 受託者は、本業務において情報システムのセキュリティ監視を行う場合には、以下の内容を含む監視手順を定め、適切に監視運用すること。
 - (1) 監視するイベントの種類
 - (2) 監視体制

(3)監視状況の報告手順

(4)情報セキュリティインシデントの可能性のある事象を認知した場合の報告手順

(5)監視運用における情報の取扱い(機密性の確保)

7 受託者は、本業務において運用中の情報システムに脆(ぜい)弱性が存在することを発見した場合には、速やかに担当部署に報告し、本業務における運用・保守要件に従って脆(ぜい)弱性の対策を行うこと。

8 受託者は、本業務において本業務の調達範囲外の情報システムを基盤とした情報システムを運用する場合は、運用管理する府省庁等との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。

9 受託者は、本業務において情報システムの運用・保守を行う場合には、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。

10 受託者は、本業務において情報システムの更改又は廃棄を行う場合には、当該情報システムに保存されている情報について、以下の措置を適切に講ずること。

(1)情報システム更改時の情報の移行作業における情報セキュリティ対策

(2)情報システム廃棄時の不要な情報の抹消

V クラウドサービスに関する情報セキュリティの確保

受託者は、本業務において、クラウドサービスを活用する場合には、以下の措置を講じること。また、当該クラウドサービスの活用が本業務の再委託に該当する場合は、当該クラウドサービスに対して、Ⅷの措置を講じること。

1 ISO/IEC27001 又はそれに基づく認証を取得しているクラウドサービスを採用すること。また、当該認証の証明書等の写しを提出すること。(提出時点で有効期限が切れていないこと。)

2 クラウドサービスの情報セキュリティ水準を証明する以下のいずれかの証明書等の写しを提出すること。(提出時点で有効期限が切れていないこと。)

(1)ISO/IEC 27017 又は ISMS クラウドセキュリティ認証制度に基づく認証

(2)セキュリティに係る内部統制の保証報告書(SOC 報告書(Service Organization Control Report))

(3)情報セキュリティ監査により対策の有効性が適切であることを証明する報告書(クラウド情報セキュリティ監査制度に基づくCS マークが付されたCS 言明書等)

3 クラウドサービスにおいて個人情報又は農林水産省における要機密情報が取り扱われる場合には、当該クラウドサービスのデータセンター(バックアップセンターを含む。)は国内に限ること。

4 クラウドサービスの廃止、サービス内容の変更等に伴い契約を終了する場合は、他のクラウドサービス等に円滑に移行できるよう、十分な期間をもって事前(サービス廃止等の1年

以上前が望ましい。)に担当部署へ通知すること。

- 5 クラウドサービスの契約を終了する場合、クラウドサービス上に保存された農林水産省のデータについて、汎用性のあるデータ形式に変換して提供するとともに、クラウドサービス上において復元できないよう抹消し、その結果を担当部署に書面で報告すること。
- 6 クラウドサービスに係るアクセスログ等の証跡を保存し、担当部署からの要求があった場合は提供すること。なお、証跡は1年間以上保存することが望ましい。
- 7 インターネット回線とクラウド基盤との接続点の通信を監視すること。
- 8 クラウドサービスに係る業務の一部がクラウドサービス事業者以外の事業者へ外部委託されている場合は、当該クラウドサービス事業者以外の事業者へⅧの措置を講ずること。
- 9 クラウドサービスにおける脆(ぜい)弱性対策の実施内容を担当部署が確認できること。
- 10 クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切替等の対策が講じられていること。また、クラウドサービスに障害が発生した場合の復旧時点目標(RPO)等の指標を提示すること。

なお、農林水産省の要安定情報を取り扱う場合は、データセンターを地理的に離れた複数の地域に設置するなどの災害対策が講じられていること。

- 11 クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。
- 12 クラウドサービスの利用者が、自らの意思によりクラウドサービス上で取り扱う情報を確実に抹消できること。
- 13 本業務において、農林水産省に開示することとしているクラウドサービスに係る情報について、業務開始時に開示項目や範囲を明記した資料を提出すること。
- 14 農林水産省に対して、クラウドサービスに係る機密性の高い情報を開示する場合は、農林水産省において、当該情報を審査又は本業務以外の目的で利用しないよう適切に取り扱うため、必要に応じて当該情報に取扱制限を明記するなどの措置を講じること。

VI 機器等に関する情報セキュリティの確保

受託者は、本業務において、農林水産省にサーバ装置、端末、通信回線装置、複合機、特定用途機器、外部電磁的記録媒体、ソフトウェア等(以下「機器等」という。)を納品、賃貸借等をする場合には、以下の措置を講じること。

- 1 納入する機器等の製造工程において、農林水産省が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。
- 2 機器等に対して不正な変更があった場合に識別できる構成管理体制を確立していること。また、不正な変更が発見された場合に、農林水産省と受託者が連携して原因を調査・排除できる体制を整備していること。
- 3 機器等の設置時や保守時に、情報セキュリティの確保に必要なサポートを行うこと。

- 4 利用マニュアル・ガイドンスが適切に整備された機器等を採用すること。
- 5 脆(ぜい)弱性検査等のテストが実施されている機器等を採用し、そのテストの結果が確認できること。
- 6 ISO/IEC 15408 に基づく認証を取得している機器等を採用することが望ましい。なお、当該認証を取得している場合は、証明書等の写しを提出すること。(提出時点で有効期限が切れていないこと。)
- 7 情報システムを構成するソフトウェアについては、運用中にサポートが終了しないよう、サポート期間が十分に確保されたものを選定し、可能な限り最新版を採用するとともに、ソフトウェアの種類、バージョン及びサポート期限について報告すること。なお、サポート期限が事前に公表されていない場合は、情報システムのライフサイクルを踏まえ、販売からの経過年数や後継ソフトウェアの有無等を考慮して選定すること。
- 8 機器等の納品時に、以下の事項を書面で報告すること。
 - (1) 調達仕様書に指定されているセキュリティ要件の実装状況(セキュリティ要件に係る試験の実施手順及び結果)
 - (2) 機器等に不正プログラムが混入していないこと(最新の定義ファイル等を適用した不正プログラム対策ソフトウェア等によるスキャン結果、内部監査等により不正な変更が加えられていないことを確認した結果等)

VII 管轄裁判所及び準拠法

- 1 本業務に係る全ての契約(クラウドサービスを含む。以下同じ。)に関して訴訟の必要が生じた場合の管轄裁判所は、国内の裁判所とすること。
- 2 本業務に係る全ての契約の成立、効力、履行及び解釈に関する準拠法は、日本法とすること。

VIII 業務の再委託における情報セキュリティの確保

- 1 受託者は、本業務の一部を再委託(再委託先の事業者が受託した事業の一部を別の事業者へ委託する再々委託等、多段階の委託を含む。以下同じ。)する場合には、受託者が上記Ⅱの1、Ⅱの2及びⅢの1において提出することとしている資料等と同等の再委託先に関する資料等並びに再委託対象とする業務の範囲及び再委託の必要性を記載した申請書を提出し、農林水産省の許可を得ること。
- 2 受託者は、本業務に係る再委託先の行為について全責任を負うものとする。また、再委託先に対して、受託者と同等の義務を負わせるものとし、再委託先との契約においてその旨を定めること。なお、情報セキュリティ監査については、受託者による再委託先への監査のほか、農林水産省又は農林水産省が選定した事業者による再委託先への立入調査等の監査を受け入れるものとする。
- 3 受託者は、担当部署からの要求があった場合は、再委託先における情報セキュリティ対策

の履行状況を報告すること。

IX 資料等の提出

上記Ⅱの1、Ⅱの2、Ⅲの1、Ⅴの1、Ⅴの2、Ⅵの1及びⅥの6において提出することとしている資料等については、最低価格落札方式にあつては入札公告及び入札説明書に定める証明書等の提出場所及び提出期限に従つて提出し、総合評価落札方式にあつては提案書等の総合評価のための書類に添付して提出すること。

X 変更手続

受託者は、上記Ⅱ、Ⅲ、Ⅴ、Ⅵ及びⅧに関して、農林水産省に提示した内容を変更しようとする場合には、変更する事項、理由等を記載した申請書を提出し、農林水産省の許可を得ること。