行政情報システム用パーソナルコンピュータ賃貸借及び保守等業務仕様書

Ⅰ　目　的

農林水産省では、各拠点において職員１人に対し、農林水産省行政情報システム（以下「ＬＡＮシステム」という。）に接続される１台のパーソナルコンピュータ（以下「ＰＣ」という。） を整備しているところであり、水産庁漁業調整事務所における、その一部の機器について、賃貸借期間の終了等を迎えることから、その更新のため本仕様書に示すＰＣ（ノート型）の賃貸借及び保守契約を行うものである。

Ⅱ　調達範囲及び入札参加要件

本調達においては、契約締結後、賃貸借期間が開始するまでの間のＰＣ導入作業の一切、賃貸借期間中の運用・保守の一切、賃貸借期間満了後の措置の一切及びこれらに関する全てのドキュメントの納品を調達範囲とする。

また、ＰＣを配付する拠点は別紙１「拠点別配付一覧」のとおりとし、別紙１の拠点に納入する。

本業務の確実な履行の確保の観点から、受注者は官公庁におけるパソコンリース実績を過去５年以内に有することを入札参加要件とする。

Ⅲ　作業期間等

１　ＰＣ導入作業期間
　契約締結日から令和２年 11 月 10 日まで

２　ＰＣ納品期限
　令和２年 11 月 20 日まで

３　賃貸借期間
　令和２年 12 月１日から令和６年 11 月 30 日まで

４　データ消去履行期限
　令和７年３月 31 日まで

Ⅳ　賃貸借数量

44 式（ノート型）

Ⅴ　業務実施要領の策定

受注者は、本業務におけるコミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理及び情報セキュリティ対策（以下「業務管理等」という。）を記した「業務実施要領」を作成し、契約締結後７日（行政機関の休日（行政機関の休日に関する法律（昭和 63 年法律第 91 号）第１条第１項各号に掲げる日をいう。以下同じ。）を含まない。）以内に水産庁漁政部漁政課経理班（以下「担当部署」という。）の承認を得ること。

本業務の実施期間中、業務実施要領に基づき業務管理等を行うこと。

また、受注者は、農林水産省が業務実施要領を作成するに当たり、具体的な作業内容や実施時間、実施サイクル等に関する資料作成等の支援を行うこと。

Ⅵ　賃貸借機器の仕様及び機能

１　端末の基本要件

本業務で調達する端末については、下表に掲げる要件又はこれと同等以上の性能等を有するものとし、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（以下「LAN システム」という。）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、水産庁の職員が業務で支障なく使用できるものとすること。ただし、納入候補となる機器について、証明書等の提出期限までに、担当部署へ機器リスト（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、農林水産省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、速やかに担当部署に確認した上で、代替品の選定等、納入候補となる機器の見直しを図ること。

また、同一機種未使用品に限定するとともに、開発工程、製造工程等において、①から⑦の情報セキュリティ要件を満たすこと。

① 開発工程において信頼できる品質保証体制が確立されていること。

② 利用マニュアル・ガイダンスが整備された製品であること。

③ 脆（ぜい）弱性検査等のテストの実施が確認できること。

④ 製造工程における不正行為の有無について、定期的な監査が行われていること。

⑤ 製造者が不正な変更を加えないよう、サプライチェーン全体が適切に管理されていること。

⑥ 不正な変更が発見された場合に、当省と受注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。

⑦ ISO/IEC15408 に基づく認証を取得する等、第三者による情報セキュリティ機能の客観的な評価を得た製品であることが望ましい。なお、「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。

番号	区分	項目	要件
1	本体の要件	形状等	持ち運びが容易なノート型であり、1.3kg 以下であること。
2		入力デバイス	キーボード（JIS 配列準拠。原則としてキーピッチは 18mm 以上。）及びタッチパッドを内蔵すること。

番号	区分	項目	要件
3		OS	Windows 10 Pro（64bit・日本語）
4		CPU 種別	Intel Core i5、Core m5 のいずれか又は同等以上
5		CPU クロック周波数	１コア当たり最大動作周波数が 1.7GHz 以上かつ２コア以上搭載していること。
6		メインメモリ	８GB 以上
7		ストレージ	SSD 又はフラッシュメモリ型のストレージを 100GB 以上内蔵すること。 TPM を使用して保存領域を暗号化すること。 C ドライブと D ドライブの配分割合については担当部署の指示に従うこと。
8		導入するソフトウェア	ストレージに OS 及び担当部署が別途用意するソフトウェア等（以下のソフトウェアを含む。）を導入し設定すること。 ・担当部署が指示する SSL-VPN クライアント ・担当部署が指示するウイルス対策ソフトウェア （ウイルスバスターコーポレートエディションを予定。） ・担当部署が指示する端末管理ソフトウェア （SKYSEA Client View を予定。） ・担当部署が指示する以下のソフトウェア InforCage FileShell Office 365　Pro Plus（Teams を除く） Skype for Business 一太郎 ７ZIP Google Chrome Adobe Acrobat Reader DC
9		対応プロトコル	TCP/IP（IPv4）に対応していること。 受注後に担当部署が指示する必要最小限の通信先 IP アドレスを除き、Windows Firewall 等で通信をブロックする設定を行うこと。
10		液晶パネル	12.5 型以上 15.6 型以下で、解像度 1920×1080、1920×1200 又は 1920×1280 ドットの液晶パネルを内蔵していること。 18bit 以上でフルカラー表示が可能であること。

番号	区分	項目	要件
11		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。
12		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。
13		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。
14		内蔵カメラ	有効画素数約90万画素以上のウェブ会議用のフロントカメラを備えること。
15		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。
16		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以上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。
17		電源バッテリ	JEITAバッテリ動作時間測定法 Ver.2.0で７時間以上稼働可能なバッテリを内蔵すること。
18		その他	盗難防止用ロック取り付け穴を備えること。
19	本体添付品の要件	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。
20		外部映像出力	端末本体にHDMI（標準サイズ）出力端子を備えていない場合にはHDMI（標準サイズ）出力に変換するコネクタを、VGA出力端子を備えていない場合にはVGA出力に変換するコネクタを添付すること。 なお、外付けドック等で対応することを可とする。
21	本体に有する	本体重量等	可能な限り軽量であることが望ましい。 堅牢性について外部機関で検証していること又は米軍調達基準（MIL-STD-810G)を満たしていることが望ましい。

番号	区分	項目	要件
22	ことが望ましい要件	防水･耐水	キーボード等について防水・耐水性能を有することが望ましい。
23		タッチパネル	内蔵ディスプレイについてタッチパネルであることが望ましい。
24		カメラのカバー	内蔵カメラのレンズ部分に開け閉めが容易にできるカバーを有することが望ましい。
25		覗き見防止	内蔵ディスプレイについて覗き見防止機能を有することが望ましい。
26	ソフトウェア設定等の要件	利用者による変更を許容するOS設定	本体の利用者が以下のような変更を行えるよう設定を行うこと。設定内容について担当部署に説明し承認を得た上で設定を実施すること。また、運用開始後に担当部署等が設定の変更を行うことができるようマニュアルを作成し、仕様書Ⅳ２(4)に記載の「管理者用マニュアル」に含めること。 【許可の例】 ・ 液晶パネルと外部映像出力の２画面表示の際、画面複製又は画面拡張を選択できること。 ・ 外部映像出力について、縦長画面表示に変更できること。 ・ 利用者が画面の解像度を変更できること。 ・ 無線LAN（WiFi）の設定の変更及び保存ができること。 ・ 音量設定が保存できること。 ・ 画面の輝度設定が保存できること。 ・ 画面の電源とスリープの設定が保存できること。
27		利用者による変更を制限するOS設定	本体の利用者が以下のような変更を行えないよう設定を行うこと。設定内容について担当部署に説明し承認を得た上で設定を実施すること。また、運用開始後に担当部署等が設定の変更を行うことができるようマニュアルを作成し、仕様書Ⅳ２(4)に記載の「管理者用マニュアル」に含めること。 【制限の例】 ・ OSのシステム設定等の変更 ・ OSへのデバイスドライバ、ソフトウェア等のインストール・アンインストールの実施
28		バッチファイル･ショ	本業務で調達する端末について、担当部署が提示するプロキシサーバの設定を切り替えるためのバッチファイルを配置し、デスクトップにショートカットを設置すること。こ

番号	区分	項目	要件
		ートカットの設置	のほか、担当部署が指示するショートカットをデスクトップに配置すること。
29		USB機器等の接続制御	USB機器について、ClassID、VenderID、ProductIDの指定等による接続制限を行うこと。また、以下のようなデバイスについては、利用が可能であること。また、要件に定めのないメモリカードデバイス等が本体に備わっている場合、そのデバイスについて本体の利用者が利用できないよう設定が可能であること。 【有効とするデバイスの例】 キーボード、マウス、マイク、スピーカー、ウェブカメラ、担当部署が指示するUSBメモリ
30		端末の一元管理	本業務で調達する端末全てについて、本体のOSパッチの配信・適用、OSの設定変更、ソフトウェア等のインストール、遠隔操作、端末の情報の収集等について、担当部署やLANシステムのサービスデスクの担当者が管理画面にアクセスすることにより、一元管理を行える仕組みを端末に導入すること。（当省が保有するSKYSEA Client View（Light Edition）を使用して本機能を実現することを原則とする。）
31		ログイン認証	指紋認証デバイスを内蔵することが望ましく、 認証については指紋認証またはそれ以外の方法で設置を行うこと。 原則として当省で構築済みのActive Directoryのユーザアカウントを使用可能とすること。 オフライン時においても、端末本体のローカル環境へログインできること。 非常時等の際に他の職員の端末へのログインが可能であること。

２　機能要件

（１）機能に関する事項

本機能の実現においては、農林水産省が保有する端末管理ソフト（SKYSEA Client View（Light Edition）。サーバも含め構築済み。）、WSUS（Windows Server Update Services）サーバを利用することを原則とする。

①　LANシステム接続機能

本業務で調達する端末について、Word、Excel、PowerPoint等による文書作成、Outlookによるメール送受信等、Internet Explorerによるウェブサイトの閲覧（動

画閲覧を含む。)、業務システムの利用、ウェブ会議システムの利用等を行えること。

この際、以下に注意して設定を行うこと。

ア　ウェブ会議システムにおいて映像･音声出力だけでなく映像･音声入力　が利用できるよう端末を設定すること。

イ　庁舎外からLANシステムに接続するためにVPNソフトウェアが動作可能であること。

なお、端末の利用者が以下のような変更を行えるよう設定を行うこと。設定内容について担当部署に説明し承認を得た上で設定を実施すること。

【許可の例】

・ 液晶パネルと外部映像出力の２画面表示の際、画面複製又は画面拡張を選択できること。

・ 外部映像出力について、縦長画面表示に変更できること。

・ 利用者が画面の解像度を変更できること。

・ 無線LAN（WiFi）設定を変更できること。

また、端末の利用者が以下のような変更を行えないよう設定を行うこと。設定内容について担当部署に説明し承認を得た上で設定を実施すること。

【制限の例】

・ OSのシステム設定等の変更

・ OSへのデバイスドライバ、ソフトウェア等のインストール・アンインストールの実施

② 端末の一元管理機能

本業務で調達する端末全てについて、本体のOSパッチの配信・適用、OSの設定変更、ソフトウェア等のインストール、遠隔操作、端末の情報の収集等について､担当部署やLANシステムのサービスデスクの担当者が管理画面にアクセスすることにより、一元管理を行えること。

（２）画面に関する事項

・端末の一元管理機能

本業務で調達する端末について、一元管理機能の画面上から端末の各種設定情報について、一覧を確認できること。

また、端末のOSパッチ配信や設定変更について、操作が画面上で実施できること。

（３）帳票に関する事項

・端末の一元管理機能

本業務で調達する端末について、一元管理機能の画面上から端末の各種設定情報について、一覧を出力できること。

（４）情報・データに関する事項

① LANシステム接続機能

本業務で調達する端末について、データを保存するストレージを暗号化する

こと。

② 端末の一元管理機能

本業務で調達する端末について、一元管理機能の画面上で端末のOSパッチや設定情報について、管理が可能であること。

（５）外部インターフェース

・LANシステム接続機能

USB機器について、ClassID、VenderID、ProductIDの指定等による接続制限を行うこと。なお、以下のようなデバイスについては、利用が可能であること。

また、要件に定めのないメモリカードデバイス等が本体に備わっている場合、そのデバイスについて本体の利用者が利用できないよう設定が可能であること。設定内容について担当部署に説明し承認を得た上で設定を実施すること。

【有効とするデバイスの例】

キーボード、マウス、マイク、スピーカー、ウェブカメラ、担当部署が指示するUSBメモリ

３ 非機能要件の定義

（１）ユーザビリティ及びアクセシビリティに関する事項

・LANシステム接続機能

本業務で調達する端末の利用者が、LANシステムに接続する際、可能な限り少ない操作で接続できるよう、利用者の利便性を考慮した画面構成とすること。

（２）システム方式に関する事項

・LANシステム接続機能

本業務で調達する端末について、Word、Excel、PowerPoint等による文書作成、Outlookによるメール送受信等、Internet Explorerによるウェブサイトの閲覧（動画閲覧を含む。）、業務システムの利用、ウェブ会議システムの利用等を行えること。

（３）規模に関する事項

・端末の一元管理機能

本業務で調達する端末全てについて、一元管理ができること。

（４）性能に関する事項

１に示す性能を満たしていること。

（５）上位互換性に関する事項

・LANシステム接続機能

端末に導入したOSについて、当省において上位OSへのアップグレード等を実施する場合がある。

（６）中立性に関する事項

トータルコスト削減に資するよう、ベンダーロックインとならない製品選定を行うこと。

（７）継続性に関する事項

障害、災害等による情報システムの問題発生時の対応については、別途調達しているLANシステムにおいて対応を行う。

（８）情報システム稼働環境に関する事項

本業務で調達する端末について、農林水産省の庁舎内においては敷設済みの有線 LAN 及び無線 LAN を利用し、広域ネットワーク（農林水産省統合ネットワーク）を経由してデータセンタ内の LAN システムに接続可能であり、自宅、出張先等の庁舎外においては、インターネット（SSL-VPN）を経由してデータセンタ内の LAN システムに接続可能である。（システム構成については、以下の図を参照。）

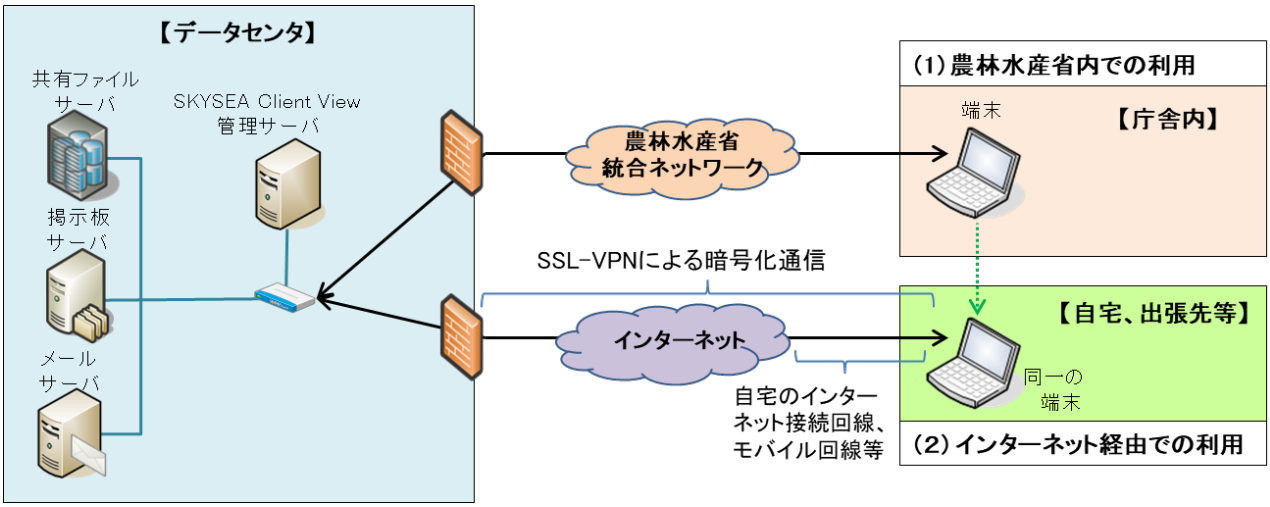


図　システム構成

Ⅶ　保証等

納入するハードウェア及びソフトウェアについては、その保証については以下の要件とする。

１　納入したハードウェアの無償保証期間は、賃貸借契約開始後１年間とするが、２年目以降について保証期間の延長の提案があった場合は、この限りでない。

２　ハードウェアに係る無償保証対象は、機器本体すべての部品及び付属品（ＡＣアダプター及び電源コード）とする。

ただし、以下の場合については、有償による対応とするが、無償保証の提案があった場合はこの限りではない。

（１）職員の過失（水などの液体こぼれ、落下、水没、誤接続等）による破損、故障。

（２）天災、異物による破損、故障。

（３）バッテリーパック、乾電池の自然消耗。

（４）キーボードの文字の擦れ。

３　故障内容により、機器本体を交換した場合についても、当初の無償保証期間内は無償保証とすること。２年目以降について保証期間の延長の提案があった場合についても、同様の対応とすること。

Ⅷ　導入作業

受注者は以下に従いＰＣの設定作業等を行い、対象拠点に納品すること。

１　作業計画書及び作業実施者名簿の作成

本調達で実施する作業に係る「作業計画書」及び「作業実施者名簿」を作成し、契約締結後 20 日（行政機関の休日を含まない。） 以内に各拠点においてＰＣ等の管理・運用を担当する職員（以下「システム担当者」という。）の承認を得ること。なお、システム担当者の所属部署、連絡先等は契約締結後に担当部署から受注者に開示する。

また、ＸＶの要件等を踏まえて本調達の全般に係る情報セキュリティ対策を記した「方針書」を作成し、担当部署の承認を得ること。

２　初期ＰＣ及びリカバリメディアの作成

（１）Ⅵの要件を満たすＰＣ（以下「初期ＰＣ」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、初期ＰＣの作成に必要な設定情報等については担当部署に確認すること。

（２）ＨＤＤをⅥの１の表８のソフトウェア等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」（CD-R、DVD-R 又はＵＳＢメモリ）を担当部署及び各拠点毎に１ 組ずつ作成し､リカバリに必要なライセンスを含めて賃貸借期間の開始までに納品すること。

また、リカバリ手順を記した「リカバリマニュアル」１部を各メディアに添付して納品すること。

３　ソフトウェア（LAN 共通機能）の設定作業

初期ＰＣを基に、ＬＡＮシステムに接続するための設定、必要なソフトウェアのインストール等の作業（以下「設定作業」という。）を実施することとし、詳細は以下のとおり。

（１）設定作業の実施場所

設定作業は、原則として農林水産省本省庁舎内で実施することとし、担当部署の指示に従い初期ＰＣを搬入すること。

また、担当部署から作業実施場所の説明を受け、作業スペースを踏まえた効率的な設定作業を実施できるように１の作業計画書を作成すること。

本業務の作業場所及び作業に当たり必要となる設備、備品及び消耗品等については、受注者の責任において用意すること。また、必要に応じて担当職員が現地確認を実施することができるものとする。

（２）ＬＡＮシステムへの接続

初期ＰＣをＬＡＮシステムに接続するに当たっては、契約締結後に提示する手順に従いドメイン参加等の設定を行うこと。

なお、ドメイン登録に必要な情報として、担当部署と協議の上、コンピュータ名、MAC アドレス、シリアル番号等を整理したものから随時提出することとし、これらを取りまとめた「一覧表」については賃貸借期間の開始までに提出すること。

（３）ソフトウェアのインストール等

ＬＡＮシステムの共通機能を利用するための複数のソフトウェア等を当省が保有するライセンスを使用してそれぞれインストールし、設定作業を行うこと。

なお、対象となるソフトウェア等は、ウイルス対策ソフト、統合管理ソフト等

であり、ソフトウェア等の仕様（ソフト名・バージョン等）については担当部署から提示する。

（４）作業資材等

設定作業に必要となる電源タップ、ＬＡＮケーブル、スイッチングハブ等の資材については、受注者の負担で準備すること。

（５）ソフトウェアのインストールの不備等、設定作業を終えたＰＣに不具合があった場合には、受注者の負担において再度設定作業を行うこと。

４　ＰＣ等の納品

賃貸借期間の開始までに別紙１に示す各拠点に「設定作業が完了したＰＣ」を納品することとし、詳細は以下のとおり。

（１）拠点建物内の具体的な配付場所については、契約締結後にシステム担当者から提示するので、運搬日時、配付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）ＰＣの運搬に当たっては、紛失、破損等の事故が起きないよう十分に注意し、運搬に必要な資材等は受注者の負担で準備すること。

特に設定作業場所から各拠点へ運搬する際は、車両等による輸送中のセキュリティ対策に万全を図ること。

（３）ＰＣの詳細な操作方法、設定方法、トラブルシューティング等を記した「管理者用マニュアル」を納品すること。

また、取扱説明書、ユーザマニュアル等の「既存の添付資料」を納品すること。

なお、納品部数は担当部署に一組ずつ、及び別紙１の拠点毎にそれぞれ１組ずつとし、それ以外の資料の余分については受注者の責任で廃棄すること。

（４）その他

ア　ラベルの貼付

賃貸借期間中のＰＣ等の管理のために（ア）及び（イ）のラベルを貼付すること。

なお、使用するラベルの色、貼付位置等の詳細は担当部署と協議の上で決定すること。

（ア）本調達で納品されたＰＣが賃貸借物件であることが明確に判別できるよう、所有者名、賃貸借期間等を記したラベルをＰＣに貼付すること。

（イ）納品するＰＣ及びＡＣアダプタに、一連番号及びコンピュータ名等を記したラベルを貼付すること。

イ　ＰＣの配付間違いを防ぐため、ＰＣを梱包した箱にコンピュータ名、システム担当者から示された配付部署名等を記したラベルを貼付する等の事前準備を行うこと。

ウ　ＰＣ配付後の空箱等の梱包材について、システム担当者が指示する場所で回収し、受注者が責任を持って撤去すること。その際、イで貼付したラベルを裁断等の方法で確実に処分すること。

５　その他

（１）搬入時のエレベータ等への養生については、システム担当者と打合せを行い必

要に応じて対処すること。

（２）導入作業に当たっては、マスター機を作成して展開する等、効率的な方法により作業を実施することとし、詳細について事前に担当部署と協議すること。

（３）賃貸借期間終了後のＰＣ回収確認作業等の簡便化を講じた措置を行うこと。

（４）Ⅷに規定する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、各組織別に作業終了日、作業内容等を記した「作業完了報告書」を担当部署へ提出すること。

Ⅸ　保守等

対応に当たっては、システム担当者からの連絡・質問等の受付先、対応者、作業フロー等を記載した「体制図」を作成し、賃貸借期間の開始前までにシステム担当者へ提出し、承認を得ること。

１　ＰＣのハードウェアを常に良好な状態に保つためにカスタマエンジニアを確保し、十分な保守対応を実施できる体制を整備すること。

２　別紙２「拠点別受付時間一覧」のとおり、システム担当者からの連絡・質問等の電話受付を実施すること。

３　納入したＰＣの障害連絡について、初期切り分け及び障害対応日の調整を受付後２時間以内に行うこと。

また、障害対応については、障害受付日を含め３開庁日（ 行政機関の休日を含まない。）以内に行うこと。

ただし、システム担当者と協議の上で、障害対応期日を定めたものについてはその限りではない。

なお、障害対応作業は原則として各拠点の庁舎建物内で実施することとし、庁舎建物内で作業ができない場合は、事前にシステム担当者と協議し、作業場所について承認を得ること。

４　原因の如何に関わらず、ＰＣに障害が発生した場合又は障害の発生が疑われる場合は、システム担当者からの依頼に基づき、当該ＰＣの修理又は交換を行うこと。また、付属品についても同様に対応すること。

なお、修理又は交換に係る費用負担については、Ⅶに示す要件によるものとする。

５　納入したハードウェア及びⅥの２のソフト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、システム担当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。また、メモリ、ＨＤＤ等、ＰＣの構成部品の初期不良等による不具合が発生し、ハードウェア本体の交換、部品の交換を行う場合は、受注者の責任において設定作業、動作確認等を行うこと。

特に初期納入時の場合は、賃貸借開始期日までに再度良品を納入すること。

６　ＰＣの修理又は交換においてＨＤＤを交換する場合は、リカバリ作業は含まないものとする。また、元のＨＤＤについては、３で規定した作業場所において、米国国家安全保障局（NSA） 方式（３回書込み）又は米国国防総省規格（DoD5220／22-M)により、ソフトウェアを使用したデータ消去を実施すること。

なお、ソフトウェアを使用してデータ消去できない場合は、物理破壊でのデータ

消去を認めることとし、その他の方法による場合は、システム担当者と協議の上、方法等を決めること。

７　賃貸借期間中、以下に示す毎月の保守状況を、当月分を翌月 15 日（行政機関の休日の場合は、その翌開庁日。）までに担当部署に書面で報告すること。

（１）ＰＣの障害の発生・対応状況（障害の原因、修理状況等）

（２）納入したハードウェア及びソフトウェアに関する重要な情報（脆弱性、緊急サポート、リコール、サポート期限の到来等）

（３）６の作業を実施した場合のデータ消去証明書

８　「デジタル・ガバメント推進標準ガイドライン　別紙２　調達仕様書に盛り込むべき ODB 登録用シートの提出に関する作業内容」に基づき、情報システム資産管理用シートを提出するとともに、担当部署の指示に基づき、情報システム資産管理データと毎年 10 月１日時点での現況との突合・確認作業を支援すること。

９　本業務の遂行に当たっては、「デジタル・ガバメント推進標準ガイドライン」、に基づき、作業を行うこと。具体的な作業内容及び手順等については、「デジタル・ガバメント推進標準ガイドライン解説書（内閣官房情報通信技術（ＩＴ）総合戦略室）」（以下「解説書」）を参考とすること。なお、「標準ガイドライン」及び「解説書」が改定された場合は、最新のものを参照し、その内容に従うこと。

Ｘ　賃貸借期間満了後の措置

賃貸借期間満了後、令和７年３月 31 日までに受注者はＰＣのデータ消去をするとともに、データ消去証明書をシステム担当者に提出し、データ消去の確認を得た上でＰＣを引き取ることとし、詳細は以下のとおり。

１　作業実施場所

データ消去作業は原則として庁舎外で実施することとし、システム担当者と協議の上、作業実施場所を決定すること。その際、作業実施場所のセキュリティ要件を証明する書類を提出すること。

作業実施場所に係る要件は以下のとおり。なお、協議の結果、庁舎内で作業を実施する場合にはその限りではない。

（１）ＰＣの輸送中におけるＰＣの紛失及び情報漏えいを防止するため、必要な措置を講じた上で作業を行うこと。

（２）関係者以外立ち入ることのできない、セキュリティを完備し、ＩＣ錠等で作業者の入退室管理を講じている建物内で行うこと。

２　作業計画書及び作業実施者名簿の作成

以下の３から６の作業に係る「作業計画書」及び「作業実施者名簿」を賃貸借期間満了前までに作成し、システム担当者の承認を得ること。

３　ＰＣ等の回収

機器を設置している各拠点の事務室等から、庁舎内の回収場所に機器の回収を行うとともに、回収した機器、付属品等の数量、状態、残留媒体の有無の確認等を行うこと。

回収作業については、農林水産省が別途調達する後継ＰＣの導入と平行して実施

する前提で、作業期間等を事前にシステム担当者と協議して作業計画を作成すること。

なお、回収に必要な資材（コンテナ等）については、受注者の負担において用意することとし、ＰＣが破損しないよう適切な措置を行うこと。

４　搬出

ＰＣを各拠点から作業実施場所へ搬出する際の要件は以下のとおり。

（１）搬出日時、搬出手順等についてシステム担当者と十分に打合せを行い、作業計画を作成すること。

（２）ＰＣの搬出に当たっては、紛失、破損等の事故が起きないよう十分に注意し、搬出に必要な資材等は受注者の負担で準備すること。

（３）各拠点から作業実施場所への車両等による輸送中のセキュリティ対策に万全を図ること。

５　データ消去

（１）受注者は、データ消去に係るＰＣの引取後、速やかにＰＣ内のデータ消去を行うこと。

なお、消去方法は、米国国家安全保障局（NSA）方式（３回書込み）又は米国国防総省規格（DoD5220／22-M）とすること。

（２）データ消去作業は、ＨＤＤが正常に動作する場合はデータ消去ソフトウェアを使用して、全ての情報の復元が不可能な状態となる段階までデータ消去を行うこと。

ただし、ＨＤＤが正常に動作しない等、データ消去ソフトウェアの使用が困難な場合は、事前にシステム担当者に連絡の上、データ消去装置の利用、磁気的な破壊又は物理的な破壊などの方法を用いて、全ての情報の復元が不可能な状態となる段階まで行うこと。

また、データ消去後に、データ消去の作業実施者以外の者がデータ消去の確認を行うこと。

（３）データ消去作業の終了後、速やかに「作業完了報告書」を作成し、ＨＤＤ単位に以下の項目を網羅した一覧表を添付した「データ消去証明書」とともにシステム担当者に提出すること。

ア　コンピュータ名及びシリアル番号(内蔵されているＨＤＤ固有のシ リアル番号)

イ　データ消去処理方法、作業日時、作業実施者、データ消去確認者

ウ　ＨＤＤの物理的な破壊によりデータ消去した場合は、破壊した状態が分かるように作業前後のＨＤＤを撮影した写真

（４）受注者はデータ消去作業の進捗状況を適切に管理し、システム担当者から状況報告を求められた場合には、速やかに応じることができるようにすること。

（５）データ消去の未実施又は未完了により情報が漏えいした場合には、該当するＰＣの回収先のシステム担当者に報告を行い、直接又は間接的に被る損害の全てについて責任を負い、賠償を行うこと。

（６）３のＰＣ等の回収後に明らかとなったＰＣの部品故障及び破壊したＨＤＤの交

換費用等については受注者が負担することとし、本調達に含めてはならない。

６　返却

（１）データ消去作業が終了した後５日（行政機関の休日を含まない。）以内に、システム担当者と受注者で賃貸借機器のデータが消去されたことを確認し、両者が合意した上で返却を行うものとし､当庁が返却したＰＣを受領した証として､「賃貸借物品受領書」を担当部署へ提出すること。

（２）返却したＰＣについて、Ⅷの４の（４）のアで貼付したラベルを剥がすこと。また、剥がしたラベルは裁断等の方法で確実に処分すること。

７　上記１から６までの作業終了後５日（行政機関の休日を含まない。）以内に、「業務完了報告書」を作成し、担当部署へ提出すること。

Ⅺ　納品物

納品物は、特に定めのない限り、紙媒体１部と電子媒体２部をシステム担当者に納品することとし、電子媒体については、ウイルスチェックを行った上で、ウイルスチェックに関する情報（ウイルス対策ソフト名、定義ファイルのバージョン、チェック年月日等）を記載したラベルを貼付すること。

また、電子媒体に収録するファイルについては、原則として MicrosoftOffice 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、本業務の受注者は、成果物等について、納品期日までに農林水産省に内容の説明を実施して検収を受けることとし、検収の結果、納品物に不備が認められる場合には、指定された日時までに再度納品すること。

納品物名：提出期限

１　Ⅴの業務実施要領の策定に係る納品物

「業務実施要領」：契約締結後 20 日※

２　Ⅷの導入作業に係る納品物

（１）「作業計画書」及び「作業実施者名簿」（Ⅷの１）：契約締結後 20 日※

（２）情報セキュリティ対策を記した「方針書」（Ⅷの１）：契約締結後 20 日※

（３）「リカバリ用メディア」（ライセンスを含む）及び「マニュアル」（Ⅷの２の（２））：令和２年 11 月 20 日

（４）コンピュータ名、MAC アドレス、シリアル番号等を記載した「一覧表」（Ⅷの３の（２））：令和２年 11 月 20 日

（５）設定作業が完了したＰＣ（Ⅷの４）：令和２年 11 月 20 日

（６）「管理者用マニュアル」及び「既存の添付資料」（Ⅷの４の（３））：令和２年 11 月 20 日

（７）導入作業に係る「作業完了報告書」（Ⅷの５の（４））：作業終了後５日※

３　Ⅸの運用及び保守等に係る納品物

（１）運用・保守等を実施するための「体制図」（Ⅸ）：令和２年 11 月 20 日

（２）毎月の「保守状況報告」（Ⅸの７）：毎月 15 日

４　Ｘの賃貸借期間満了後の措置に係る納品物

（１）「作業計画書」及び「作業実施者名簿」（Ｘの２）：令和６年 11 月 30 日

（２）データ消去作業に係る「作業完了報告書」及び回収したＰＣの「データ消去証明書」（Ｘの５の（３））：令和７年３月 31 日

（３）賃貸借物品受領書（Ｘの６の（１））：作業終了後 10 日※

（４）本業務に係る「業務完了報告書」（Ｘの７）：作業終了後 10 日※

注）※印は行政機関の休日を含まない。

Ⅻ　責任の所在

納品したＰＣ等の責任の所在については、次のとおりとする。

１　水産庁は検収完了後、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こと。但し、水産庁に不相当な負担を課するものでないときは、受注者は水産庁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とする。

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　水産庁は、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。

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、水産庁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。

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年以内に水産庁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こと。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、契約不適合が水産庁の提供した資料等又は水産庁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適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。

ⅩⅢ　成果物の権利帰属

この契約により作成される成果物の著作権等の取扱いは､次に定めるところによる。

１　受注者は、著作権法（昭和 45 年法律第 48 号）第 21 条（複製権）、第 26 条の３

（貸与権）、第 27 条（翻訳権・翻案権等）及び第 28 条（二次的著作物の利用に関する原著作者の権利）に規定する権利を、発注者に無償で譲渡する。

２　発注者は、著作権法第 20 条（同一性保持権）第２項第３号又は第４号に該当しない場合においても、その使用のために当該成果物を改変し、また、任意の著作者名で任意に公表することができるものとする。

３　受注者は、発注者の書面による事前の同意を得なければ、著作権法第 18 条（公表権）及び第 19 条（氏名表示権）を行使できないものとする。

４　第三者が権利を有する著作物（以下「既存著作物」という。）を使用して成果物を作成する場合は、発注者が特に使用を指示した場合を除いて、受注者が必要な費用の負担及び使用許諾契約に係る一切の手続きを行うこと。この場合、受注者はその手続きの内容について事前に発注者の承認を得ることとし、発注者は既存著作物についてその許諾要件の範囲内で使用するものとする。

なお、業務の実施に関し、第三者との間に著作権に係る権利侵害の紛争が生じた場合は、その原因が専ら発注者の責めに帰す場合を除き、受注者の責任及び負担において一切を処理すること。この場合、発注者は係る紛争等の事実を知ったときは、受注者に通知し、必要な範囲で訴訟上の防衛を受注者に委ねる等の協力措置を講じるものとする。

５　使用する画像、デザイン、表現等に関して他者の著作権を侵害する行為に十分配慮し、これを行わないこと。

ⅩⅣ 個人情報の取扱い

１　本業務において、個人情報（生存する個人に関する情報であって、当該契約に含まれる氏名、生年月日、その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。以下同じ。）の取扱いが必要な場合には、その取扱いに係る事項について、システム担当者と協議の上決定し、書面にて提出すること。

なお、その際、以下の事項を記載すること。

（１）個人情報保護取扱責任者の所属・氏名等を記載した管理体制

（２）個人情報の管理状況の検査に関する事項（検査時期、検査項目、検査結果において問題があった場合の対応等）

２　本業務の作業を派遣労働者に行わせる場合は、労働者派遣契約書に秘密保持義務など個人情報の適正な取扱いに関する事項を明記し、システム担当者の承認を得た上で実施すること。また、作業実施前に教育を実施し、認識を徹底させること。

３　個人情報を複製する際には、事前にシステム担当者の許可を得ること。なお、複製の実施は必要最小限とし、複製が不要となり次第、その内容が絶対に復元できないように破棄・消去すること。

４　受注者は、本業務を履行する上で個人情報の漏えい等安全確保の上で問題となる事案を把握した場合には、直ちに被害の拡大防止等のため必要な措置を講ずるとともに、システム担当者に事案が発生した旨、被害状況、復旧等の措置及び本人への

対応等について直ちに報告すること。

５　個人情報の取扱いにおいて、適正な取扱いが行われなかった場合は、本業務の契約解除の措置を受けるものとする。

ＸＶ 情報セキュリティの確保等

受注者は、本業務の遂行に当たり、別添１「情報セキュリティの確保に関する共通基本仕様」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。

また、受注者は「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」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、「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」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。

ＸⅥ ソフトウェアライセンス

本業務に係るソフトウェアライセンスの要件は以下のとおりである。

１　マイクロソフト社製ソフトウェア

（１）Windows10 Pro 64bit

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

（２）Microsoft Office

農林水産省が保有するライセンスを使用するため、受注者はライセンス調達を行わないこと。

２　ジャストシステム社製ソフトウェア（一太郎）

原則として農林水産省とジャストシステム社の間で締結している JL-Excellent 契約（Ｅ区分）にて調達することとする。なお、JL-Excellent 番号の提供方法は別途指示する。

ＸⅦ その他

１　本業務に関して、担当部署に代わってＬＡＮシステムのサービスデスク要員（ＮＴＴコミュニケーションズ株式会社）が受注者への対応に当たる場合がある。

２　ＬＡＮシステムに接続することにより発生した欠陥については、担当部署と協議し、円滑な運用ができるよう対処すること。

３　詳細な事項及び本仕様書に定めのない事項については、システム担当者と必要に応じ打合せを行うこと。

４　その他、疑義が生じた場合は、システム担当者とそれぞれ協議し対応すること。

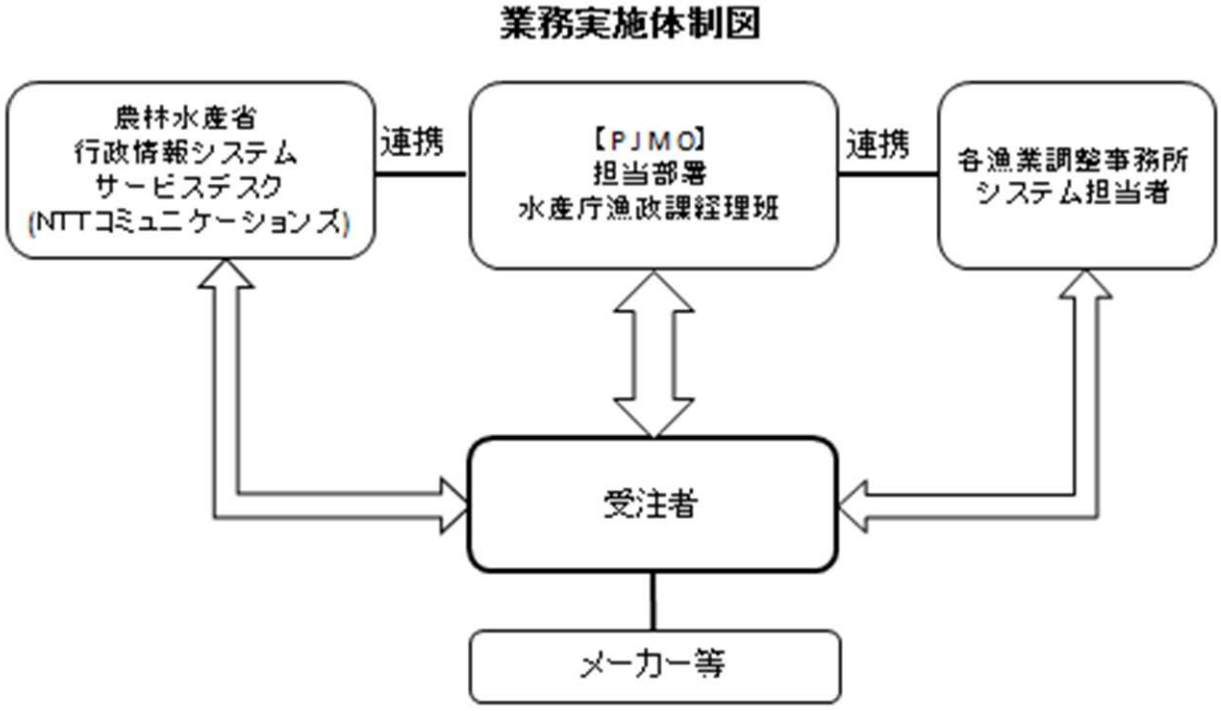
５　本業務を直接担当する農林水産省ＣＩＯ補佐官、農林水産省全体管理組織（ＰＭＯ）支援スタッフ及び農林水産省最高情報セキュリティアドバイザーが、その現に属する事業者及びこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」（昭和 38 年大蔵省令第 59 号）第８条に規定する親会社及び子会社、同一の親

会社を持つ会社並びに委託先等緊密な利害関係を有する事業者は、本書に係る業務に関して入札に参加できないものとする。

６　本業務の実施体制は次の図のとおりである。なお、受注者側の詳細な体制については、ＰＣ導入作業、運用・保守、賃貸借期間満了後の措置のそれぞれについて、受注者において別途示すこと。

７　本調達において整備又は管理を行う情報システムに伴うリスクとその対応状況を客観的に評価するために、農林水産省が情報システム監査の実施を必要と判断した場合は、農林水産省が定めた実施内容（監査内容、対象範囲、実施者等）に基づく情報システム監査を受注者は受け入れること（農林水産省が別途選定した事業者による監査を含む）。また、情報システム監査で問題点の指摘又は改善案の提示を受けた場合には、対応案を担当部署と協議し、指示された期間までに是正を図ること。

業務実施体制図


業務実施体制図
農林水産省
行政情報システム
サービスデスク
(NTTコミュニケーションズ)
連携
【PJMO】
担当部署
水産庁漁政課経理班
連携
各漁業調整事務所
システム担当者
受注者
メーカー等

別紙１事務所別配付一覧

事務所名	住　　所	電話番号	担当者(主・副)	台数
北海道漁業調整事務所	北海道札幌市北区北8条2丁目 札幌第1合同庁舎13階	011-709-2382	石橋(坂本)	10
仙台漁業調整事務所	宮城県仙台市宮城野区五輪１－３－１５ 仙台第3合同庁舎8階	022-291-2774	薮上(小松)	6
境港漁業調整事務所	鳥取県境港市昭和町９－１ 境港港湾合同庁舎1階	0859-44-3696	新呂(濵口)	4
九州漁業調整事務所	福岡県福岡市博多区沖浜町8番1号 福岡港湾合同庁舎5階	092-273-2001	堀江(植田)	24
合計				44

（別紙２）

事務所別受付時間一覧

事　務　所　名	受　付　時　間	
北海道漁業調整事務所	開庁日※の	８:３０～１７：１５
仙台漁業調整事務所		８:３０～１８：００
境港漁業調整事務所		８:３０～１７：１５
九州漁業調整事務所		８:３０～１７：１５

※行政機関の休日（行政機関の休日に関する法律（昭和 63 年法律第 91 号）第 1 条第 1 項各号に掲げる日）を含まない。

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、事態の収拾、被害の拡大防止、復旧、再発防止等に全力を挙げること。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が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に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に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・ガイダ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に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こと。

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っ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って提出し、総合評価落札方式にあっ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。