別紙

機密情報の取扱い

第１　目　的

本件業務の調達により提供される役務等の実施（以下「本件委託業務」という。）において取り扱う機密情報について、本件委託業務を受注した者（以下「受託者」という。）による①適正なデータ保護・管理方策及び情報システムに係るセキュリティ方策並びに②機密情報の漏えい、滅失、改ざん及びき損（以下「漏えい等」という。）発生時に実施すべき事項・手順等を明確にすることを目的とする。

第２　適用範囲

本契約を履行するに当たり独立行政法人 農業者年金基金（以下「基金」という。）が交付若しくは使用を許可し、又は受託者が作成若しくは出力した全てのデータ（電子データ、印刷された情報を含む。）及び個人情報を含む機密情報を対象とする。

第３　受託者が遵守すべき事項

受託者は、本契約の履行に関して、以下の項目をすべて遵守すること。

１　基本的な遵守事項

（１）機密情報の保持

本業務に係る情報セキュリティ要件は次のとおりである。

ア　委託した業務以外の目的で利用しないこと。

イ　業務上知り得た情報について第三者への開示や漏えいしないこと。

ウ　基金の許可を得ずに、資料やデータを指定の作業場所から持出さないこと。

エ　基金が求める場合には、遵守状況を報告すること。

オ　基金が求める場合には、実地調査を受け入れること。なお、実地調査は、予告なしに実施する場合がある。

（２）個人情報の取扱い

ア　以下の事項を含む個人情報の取扱いに係る事項について、基金と協議の上決定し、書面にて提出すること。

・　個人情報取扱責任者等の管理体制及び必要な契約等の情報

・　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）

イ　受託者は、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、直ちに被害の拡大を防止等のため必要な措置を講ずるとともに、担当職員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。

ウ　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。

（３）業務上の遵守事項

ア　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を参考とすること。なお、これらが改正された場合は、最新のものを参照し、その内容に従うこと。

イ　独立行政法人農業者年金基金情報セキュリティポリシー（以下「基金の情報セキュリティポリシー」という。）、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。）及び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、基金の情報セキュリティポリシーは、統一基準群に準拠することとされていることから、統一基準群が改正された場合には、最新のものを参照し、その内容に従うこと。

（４）法令等の遵守事項

本業務の遂行に当たっては、日本国の法律を遵守して業務を行うこと。

（行政手続における特定の個人を識別するための番号の利用等に関する法律、個人情報の保護に関する法律、著作権法、不正競争防止法、民法等。）

受託者は、個人情報の保護に関する法律及び同法を遵守するために受託者が定めた個人情報保護に関するガイドライン等を遵守し、個人情報を取り扱うこと。

また、必要に応じてＧＤＰＲ（一般データ保護規則）等の適用に配慮すること。

２　委託作業開始前の遵守事項

受託者は、下記（１）から（６）に定める事前計画内容を作成すること。また、基金の主管部署が求める場合には、これらを取りまとめた「データ及び個人情報管理計画書」を提出すること。

（１）データ取扱者等の指定

受託者は、上記「第２　適用範囲」に定めるデータを取り扱う者（以下「データ取扱者」という。）及び個人情報を取り扱う者（以下「個人情報取扱者」という。）を指定すること。データ取扱者を統括する者として情報システム部門に精通した課長相当職以上の者（以下「データ取扱責任者」という。）を、個人情報取扱者を統括する者として情報システム部門に精通した課長相当職以上の者（以下「個人情報取扱責任者」という。）を指定すること。また、その所属、役職及び氏名等を記入した「データ取扱者及び個人情報取扱者等名簿」を作成すること。

なお、データ取扱者及びデータ取扱責任者（以下「データ取扱者等」という。）並びに個人情報取扱者及び個人情報取扱責任者（以下「個人情報取扱者等」という。）は、守秘義務等データの取扱いに関する社内教育又はこれに準ずる講習等を受講した者とし、その受講実績を併せて記入すること。

データ取扱者及び個人情報取扱者並びにデータ取扱責任者及び個人情報取扱責任者については各々兼務を認める。

（２）データ取扱者等及び個人情報取扱者等への教育及び周知

受託者は、本件委託業務で取り扱うデータについて、その取扱いや漏えい等防止に係る「教育及び周知計画書」を作成し、本データ保護、個人情報保護及び管理要領の内容に関して、データ取扱者等及び個人情報取扱者等に対する教育及び周知を行うこと。

（３）データ及び個人情報の取扱いに関する計画策定

受託者は、本件委託業務におけるデータ及び個人情報の取扱いに関し、データ及び個人情報の複製、破棄及び保管場所の変更が生じる場合の取扱いについて、「データ及び個人情報取扱計画書」を作成すること。

（４）作業場所等のセキュリティ確保

受託者は、基金以外の作業場所において本件委託業務を行う場合は、データ及び個人情報並びに基金の主管部署が保有する情報システムに係るセキュリティ確保のために講じる措置について、「作業場所等に係るセキュリティ措置計画書」を作成すること。

また、作業場所のセキュリティ確保のために講じる措置は、以下の例による。

例：データエントリールーム、データ保管室、電子計算室等に対する施錠設備、ID カードやパスワードを用いた入退出管理機能等、その他セキュリティ確保のために講じる措置

例：システムログインパスワード、データに対する専用の ID、アクセス権限の設定等

（５）セキュリティ確保状況の事前実査

受託者が基金以外の作業場所において本件委託業務を行う場合において、基金の主管部署がその施設及び設備に関し、上記（４）で作成した「作業場所等に係るセキュリティ措置計画書」に則したセキュリティ確保が図られているかを契約履行前に実査する旨申し出たときは速やかにこれを受け入れること。

なお、実査にあたっては、基金の主管部署のほか基金の内部監査部署及び主管部署が指定した外部監査人も立ち入りを可能とすること。

（６）データ又は個人情報の漏えい等発生時の対応手順作成

受託者は、データ又は個人情報の漏えい等が発生した場合を想定し、その対応手順書を作成すること。

３　委託作業中における遵守事項

（１）データ及び個人情報管理簿の作成

受託者は、基金の主管部署から貸与を受けた各種ドキュメント、電子データ及び個人情報並びに委託業務を実施するに当たり作成されたドキュメント、電子データ及び個人情報について、授受日時、授受方法、保管場所、保管方法、使用場所、使用目的等取扱方法を明確にするため「データ及び個人情報管理簿」を作成すること。

（２）作業場所の監査

受託者は、基金以外の作業場所において本件委託業務を行う場合に、基金の主管部署がその施設及び設備に関し、上記２（４）で受託者が作成した「作業場所等に係るセキュリティ措置計画書」に則したセキュリティ確保が図られているか監査する旨を申し出たときは、定期、不定期にかかわらず、これを受け入れること。

なお、監査にあたっては、基金の主管部署のほか基金の内部監査部署及び主管部署が指定した外部監査人の立ち入りを可能とすること。

（３）データ及び個人情報の取扱い

受託者は、本件委託業務において取り扱うデータ及び個人情報に関し、データ取扱責任者又は個人情報取扱責任者に以下の作業を行わせること。

ア　データ取扱責任者はデータ取扱者の作業に、個人情報取扱責任者は個人情報取扱者の作業に立ち会う等適切な管理を行うこと。

イ　データ取扱責任者はデータ取扱者を、個人情報取扱責任者は個人情報取扱者を作業に従事させる前に、データ取扱者又は個人情報取扱者ごとに使用するユーザーID 及びパスワード等、基金の主管部署が事前に指定する項目について主管部署へ報告を行い、承認を受けること。

なお、報告する時期等は基金の主管部署の指示に従うこと。また、報告した内容に変更が生じる場合も、事前に主管部署の承認を受けること。

ウ　データ取扱責任者は作業に従事する予定のデータ取扱者について、個人情報取扱責任者は作業に従事する予定の個人情報取扱者について、事前に氏名、勤務時間、作業内容並びに取扱データ及び取扱個人情報を記入した作業予定表を基金の主管部署へ提出し、承認を受けること。

エ　データ取扱責任者は作業に従事したデータ取扱者が、個人情報取扱責任者は作業に従事した個人情報取扱者が作業を終了し作業場所を離れる際は、データ及び個人情報の持ち出しの有無を厳重に検査すること。

オ　データ取扱責任者は作業に従事したデータ取扱者の、個人情報取扱責任者は作業に従事した個人情報取扱者の氏名、勤務時間、作業内容、取扱データ及び個人情報並びにデータ及び個人情報の持ち出しの有無等を記入した作業結果表を、作業終了後、基金の主管部署へ提出すること。その際、当初予定していた勤務時間を超えている場合は、その理由も併せて記入すること。

なお、作業結果表の提出時期については、基金の主管部署の指示によること。

カ　個人情報を取り扱う委託業務については、データの漏えい等の対策としてシステム等の監視状況やシステムログなどを管理し、独立行政法人 農業者年金基金の求めに応じて速やかに提出できるようにすること。

キ　本業務で入手又は作成した資料は、日本国内のみで取り扱うこととし、クラウドサービス等のインターネット上のサービスでは取り扱わず、必ず受託者の責任において、バックアップデータの確保とともに、専用の端末内又は外部電磁的記録媒体に暗号化する等、必要な対策を実施して保管すること。

ク　クラウドサービスやホスティング等受託者側でデータを管理する役務を提供する場合は、受託者の責任においてバックアップデータを確保するとともに、バックアップデータを含めたデータの消失防止対策書を事前に基金の主管部署へ提出し、主管部署の了承を得ること。

４　委託作業完了時の遵守事項

（１）データ返却、消去、破棄等処理

受託者は、委託業務完了時に上記３（１）で作成した「データ及び個人情報管理簿」に記載されている全てのデータ及び個人情報について、日時、場所、立会者、作業責任者等の事項を記載した「データ及び個人情報返却等計画書」を基金の主管部署に提出すること。その上で、返却、消去、破棄等の措置を行うこと。

ソフトウェアによるデータ消去を行う場合、米国国防総省規格（DoD5220.22-M）以上の基準にて消去を実施するものとし、データ消去の証明書を発行すること。

（２）成果物納入時処理

納入する成果物がマルウェアやウイルス等に汚染されていないことを確認して納入すること。電磁的記録媒体により納品する場合は、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、適切に対処すること。なお、対策ソフトウェアに関する情報（対策ソフトウェア名称、定義パターンバージョン、確認年月日）を記載したラベルを貼り付けること。

（３）作業後の報告

受託者は、上記（１）に基づき返却等の処理終了後、その結果を記載した「データ及び個人情報管理簿」を基金の主管部署へ提出すること。

５　上記以外の遵守事項

（１）データ又は個人情報の漏えい等発生時の対応

受託者は、本件委託業務に関し、データ又は個人情報の漏えい等が発生した場合は、以下のとおり直ちに対応を図ること。

ア　発生状況報告

委託業務中にデータの漏えい等が発生した場合は、その事由が発生した日時、場所、事由及びその時のデータ取扱者を明らかにし、又は委託業務中に個人情報の漏えい等が発生した場合は、その事由が発生した日時、場所、事由及びその時の個人情報取扱者を明らかにし、速やかに基金の主管部署へ報告すること。

イ　対応措置

受託者は、基金の主管部署の指示に基づき対応措置を実施すること。

ウ　報告書の提出

受託者は、基金の主管部署が指定する期日までに、発生した事態の具体的内容、原因、実施した対処措置等を内容とする報告書を作成の上、提出すること。

エ　再発防止策の策定、提出、実施

受託者は、データ又は個人情報の漏えい等が発生した場合、その処理後に再発を防止するための措置内容を策定し、基金の主管部署の承認を得た後、速やかに再発防止策を実施すること。

オ　損害賠償

受託者は、データ又は個人情報の漏えい等により発生した損害に対して賠償等の責任を負うこと。

（２）情報の管理

受託者は、基金の主管部署が交付又は使用を許可した情報に限らず、本件委託事務を履行するに当たり知り得た情報について、本契約の目的以外に使用又は第三者に開示若しくは漏えい等してはならない。

以上

個人情報に関する秘密保持

受託者（以下「乙」という。）は、契約を履行するにあたり、個人情報の保護の重要性を認識し、独立行政法人 農業者年金基金（以下「甲」という。）が保有する個人情報を取り扱う際には、個人の権利利益を侵害することのないよう、次の各項目に定める事項を遵守し、適正に取り扱わなければならない。

１．個人情報に関する秘密保持、目的外利用の禁止等の義務

乙は、契約を履行するにあたり知り得た個人情報を他人に知らせてはならない。この契約が終了し、又は解除された後においても同様とする。

２．再委託の制限

乙は、契約を履行するにあたり、甲から委託された個人情報を自ら取り扱うものとする。

３．個人情報の複製等の制限

あらかじめ甲の指示又は承諾があった場合を除き、甲から委託された個人情報が記録された資料等を複写し、又は複製してはならない。

４．安全管理の措置

⑴　乙は、個人情報を取り扱うにあたって事故等を防止する上で最も信頼性の高いと認められる安全管理措置を行うこと。

⑵　乙は、前項にて実施する安全管理措置のうち、少なくとも次の各号を定め甲の承認を得るものとし、甲が更に安全管理措置を指定する場合にはこれを実施するものとする。

①　個人情報の取扱責任者
②　個人情報に接する従業員その他業務遂行に従事する者
③　個人情報の授受、移送方法
④　個人情報の保管場所及び保管・管理の方法
⑤　個人情報の具体的な取扱手順及び利用方法
⑥　個人情報の取扱いに使用する装置、機器、媒体等への技術的安全措置の内容
⑦　従業員等への個人情報保護の教育、訓練の実施状況

⑶　乙は、業務を遂行するために個人情報に接する必要のある従業員その他業務遂行に従事する者（以下「従業員等」という。）以外の者が個人情報に接することのないように個人情報を保管・管理するものとし、また、乙の責任において個人情報に接する従業員等に本契約の義務を遵守させるものとする。

５．個人情報の漏えい等の事案の発生時における対応

上記１から４に規定するいずれかの項目に違反する事態が生じ、又は生じるおそれがあることを知ったときは、速やかに甲に報告し、甲の指示に従うものとする。この契約が終了し、又は解除された後においても同様とする。

６．契約終了時における個人情報の消去及び媒体の返却

契約を履行するために甲から貸与され、又は、乙が収集し、若しくは作成した個人情報が記録された資料等を、この契約の終了後直ちに甲へ返却し、又は引き渡すものとする。ただし、甲が別に指示したときは、その指示に従うものとする。

７．違反した場合における契約解除の措置

甲は、乙が上記１から４に規定するいずれかの項目に違反していると認めたときは、契約を解除できるものとする。

８．契約内容の遵守状況についての定期報告に関する事項及び監査の対応

(1)　乙は、業務期間中、甲が求めた場合はその都度、個人情報の取扱いに関して実施する安全管理措置の実施状況を甲に報告するものとする。
(2)　甲は、必要があると認めた場合において、乙の業務の履行場所、施設等に立ち入り、義務の遵守状況を確認できるものとする。なお、立ち入りの方法等については甲及び乙で協議するものとする。
(3)　甲は、上記(1)の報告又は(2)の確認の結果、不備等が確認された場合、必要な指示を行うことができるものとする。
(4)　上記(1)の報告又は(2)の確認の結果、重大な不備があると甲が判断した場合、或いは上記(3)の指示後相当の期間経過後においても不備が是正されない場合、又は指示に従わない場合、甲は直ちに無償にて業務の全部又は一部を解除できるものとする。また、甲に損害が生じた場合には、乙は、その損害を賠償するものとする。

９.その他
(1)　使用者への周知
　乙は、その使用する者に対し、在職中及び退職後においても、この契約を履行するにあたって知り得た個人情報を他人に知らせ、又は契約の目的以外の目的に利用してはならないなど、個人情報保護の徹底について周知しなければならない。
(2)　適正な管理
　乙は、契約の履行にあたって個人情報の漏えい、滅失、改ざん及びき損の防止を図るため、
　管理責任者を特定し、個人情報の適切な管理に努めなければならない。
(3)　収集の制限
　乙は、契約の履行にあたって個人情報を収集する必要があるときは、あらかじめ甲に承諾を得た上で、契約を履行するために必要な範囲内で、適正かつ公正な手段により収集しなければならない。
(4)　第三者への提供の禁止
　乙は、甲の指示又は承諾があるときを除き、この契約の履行にあたって知り得た個人情報を、この契約を履行するため以外に使用し、又は第三者に引き渡してはならない。