令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業に係る企画競争応募要領

本事業は、令和８年度予算に係る事業であることから、本企画競争に係る契約締結は、予算が成立し、予算の示達がなされることを条件とするものである。

第１　総則

令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業（以下「本委託事業」という。）に係る企画競争の実施については、この要領に定める。

第２　事業内容

本委託事業の内容は、仕様書のとおりとする。

第３　事業の実施期間及び委託費の限度額

（１）事業の実施期間

契約の締結の日から令和９年３月３１日（水）までとする。

（２）委託費の限度額

本委託事業の予算限度額は、10,000千円（消費税及び地方消費税込）以内とする。

第４　参加資格

（１）予算決算及び会計令（昭和22年勅令第165 号）第70条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。

（２）予算決算及び会計令第71条の規定に該当しない者であること。

（３）令和７・８・９年度農林水産省競争参加資格（全省庁統一資格）の「役務の提供等」において、「A」、「B」又は「C」の等級に格付けされた者であること。

（４）農林水産本省物品の製造契約、物品の購入契約及び役務等契約指名停止等措置要領に基づく指名停止を受けている期間中でないこと。

（５）経営状況又は信用度が極度に悪化していないと認められる者であること。

（６）複数の団体が本委託事業の受託のために組織した共同事業体（民法（明治29年法律第89 号）上の組合に該当するもの。以下同じ。）による参加も可とする。

この場合において共同事業体は、本委託事業を実施すること等について業務分担及び実施体制等を明確にした、構成する各団体（以下、「構成員」という。）の全てから同意を得た規約書、全構成員が交わした協定書又は全構成員間での契約締結書（又はこれに準ずる書類）（以下、「規約書等」という。）を作成する必要があり、全構成員の中から代表者を選定し、代表者は本委託事業に係る企画競争の参加及び事業の委託契約手続を行うものとする。

また代表者及び構成員は、上記（１）から（５）の要件に適合している必要があり、契約候補者となった場合は規約書等を契約締結前までに提出すること。

なお、共同事業体に参加する構成員は、本企画競争において他の共同事業体の構成員となること又は単独で参加することはできない。

第５　説明会の開催

説明会は開催しない。
必要に応じて、仕様書の記載に従って仕様書に関する質問又は資料閲覧の申込を行うこと。

第６　参加表明書及び企画書等の提出書類に関する事項

１　参加表明書及び提出書類の作成

参加表明書を、「企画競争参加表明書」（別紙様式第１号）により作成し、以下の（１）から（６）までの添付書類と併せて提出すること。

（１）企画書及びこれに付随する以下の書類

①　過去３年以内における類似事業(ローコードプラットフォームでのシステムの構築及び当該システムを用いた業務の実証事業)の実績があれば、これに関する資料（様式任意）

②　その他参考となる資料

（２）第４の（３）を証するものとして、令和７・８・９年度農林水産省競争参加資格（全省庁統一資格）の写し

※共同提案の場合は、併せて第４（６）中の資格を確認するため、全構成員分を提出すること。

（３）業務内容を示したパンフレット（又はリーフレット）

（４）民間企業にあっては、営業経歴書及び最新の決算（営業）報告書１年分（又はそれに準じるもの）

（５）民間企業以外の者にあっては、定款又は寄附行為及び最新の決算（営業）報告書１年分（又はそれに準じるもの）

（６）女性の職業生活における活躍の推進に関する法律に基づく認定（えるぼし認定企業、プラチナえるぼし認定企業、行動計画）、次世代育成支援対策推進法に基づく認定（くるみん認定企業、トライくるみん認定企業、プラチナくるみん認定企業、行動計画）及び青少年の雇用の促進等に関する法律に基づく認定（ユースエール認定企業）を受けている場合は、基準適合認定通知書等の写しなど認定状況の分かる資料（基準に適合し、認定されている者であることを企画書に記載しておくこと）

※ 共同提案の場合は、全構成員分を提出すること。

２　応募する企画書の内容

（１）事業実施体制

担当者数、担当者の経験（過去３年間（令和５年度～令和７年度）程度に同種又は類似業務の実績）、担当者のバックアップ体制等を明記すること。

なお、再委託をする場合には、再委託先の事業者名、再委託金額及び担当する業務の内容を明記すること。

また、再委託には以下の制限があるので留意すること。

【ｱ】事業の全部を一括して請け負わせてはならない。

【ｲ】事業の主たる部分を請け負わせてはならない。

【ｳ】再委託の合計金額は委託費の限度額の50%以内としなければならない。

ただし、以下の場合は上記また書き【ｲ】、【ｳ】の制限を適用しないこととする。

【ｴ】再委託先の業務が海外で行われる場合

【ｵ】広告、放送等の主たる業務を代理店が一括して請け負うことが慣習となっている場合

【ｶ】会社法（平成17年法律第86号）第２条第３号の規定に基づく子会社又は財務諸表等の用

語、様式及び作成方法に関する規則（昭和38年11月27日大蔵省令第59号）第８条第５項及び第６項に規定する関連会社に業務の一部を請け負わせる場合

なお、上記また書き【ｳ】の再委託の比率は、上記ただし書き【ｴ】～【ｶ】に該当する再委託の金額を委託費の限度額から減算して計算した率とする。

（２）事業を実施する上で必要となる応募者の知見・専門性・実績等

（３）企画提案を求める項目及び具体的提案

（４）各事業内容の計画や完了までのスケジュール

（５）第三者と共同提案を行う場合、それぞれの事業分担及び金額

（６）積算内訳（別紙様式第２号）（再委託先の内訳を明記すること。）

（７）女性の職業生活における活躍の推進に関する法律に基づく認定、次世代育成支援対策推進法に基づく認定及び青少年の雇用の促進等に関する法律に基づく認定を受けている者である場合は、基準に適合し認定されている者であることを企画書に記載すること。

また、基準適合認定通知書等の写しなど認定状況がわかる資料を提出すること。

３　参加表明書及び企画書等の提出期限等

（１）提出期限：令和８年４月２４日（金）１５時までとする。

（２）提出方法

上記（１）までに、原則、電子メールに整理番号【088009】を付して提出すること。

（詳細は別添「電子メールを利用した書類の提出方法」のとおり）

電子メール以外で提出する場合は、PDFファイルを電子媒体（CD-R又はDVD-Rとし、ウィルス対策を施すこと。）に格納し、当該電子媒体に契約件名及び事業者名を表示（ケースは不可）の上、提出すること。

なお、郵便・信書便で提出する場合は、書留郵便等の配達記録が残るものに限る。

４　作成・提出に当たっての留意事項

（１）日本語で作成するものとする。

（２）１応募者が提出できる企画提案は１提案までとする。

（３）提出された参加表明書及び企画書等はその事由のいかんにかかわらず、変更又は取消しを行うことはできない。また、返却もしない。

（４）企画書等の提出を持参により提出する場合の受付時間は、行政機関の休日を除く１０時から１７時（令和８年４月２４日は１５時）までとする。

（５）提出期限までに農林水産省大臣官房予算課契約班に到着しなかった場合は無効とする。

（６）企画書等の提出者は、暴力団排除に関する誓約事項（別紙様式第３号）について参加表明書の提出前に確認しなければならず、参加表明書の提出をもってこれに同意したものとする。

（７）暴力団排除に関する誓約事項（別紙様式第３号）について、虚偽又はこれに反する行為が認められた書類は、無効とする。

第７　審査方法

１　応募者は、以下のとおり開催する提案会において、提案書の説明を行うものとする。

①　開催日：令和８年４月２８日（火）

（開始時刻は別途連絡するものとする。）

②　開催方法：WEB形式（Teams）にて開催する。

③　説明時間はおおむね30分間（10分間程度の質疑応答を含む。）とする。

２　審査については、非公開とする。

３　提出された企画書について、「第８　審査基準及び審査項目」に基づいて採点・審査を行い、採点した得点の最上位の者（最上位の者が複数ある場合は、最高得点を獲得した審査項目が最も多い者とし、更に当該数が同一の場合にあって、審査委員会が選定した者）を本委託事業の委託契約候補者として支出負担行為担当官農林水産省大臣官房参事官（経理）（以下「支出負担行為担当官」という。）に推薦するものとする。

なお、契約候補者から契約候補辞退届（別紙様式第４号）の提出があった場合は、採点した得点が次に高かった者を契約候補者として、支出負担行為担当官に推薦することとする。

第８　審査基準及び審査項目

企画書の審査に当たっては、業務の目的の達成について判断するため、本委託事業を確実かつ効果的に実施できるか、また、留意事項が反映されているかを踏まえて、次の項目について採点を行う。

（１）仕様書全体の事業内容を把握し、網羅的に提案されているか。
（２）提案された事業の計画は、具体性及び実現可能性の観点で妥当なものになっているか。
（３）事業を効率的に推進し、事業の目的に適ったより良い成果を上げるための工夫や提案が優れているか。
（４）提案されたスケジュールは、作業の期間及び依存関係を十分に考慮し、事業の履行期間内に完遂できる、妥当なものになっているか。
（５）業務の実施内容に適した知識及び知見を持った人員を確保しているか。
（６）事業を計画どおりに推進するための手法及び管理体制が優れているか。
（７）農林水産省からの照会、追加の要望、報告の求め等に迅速かつ柔軟に対応できる体制が整備されているか。
（８）類似する事業(ローコードプラットフォームでのシステムの構築及び当該システムを用いた業務の実証事業)の実績及び知見を十分に有しているか。
（９）官公庁における業務のコンサルティング及びその結果に基づくシステム検討・実証に関するノウハウ・実績を有しているか。
(10) 事業を行う上で適切な財務基盤、経理処理能力を有しているか。
(11) ワーク・ライフ・バランスを推進する企業として、①女性の職業生活における活躍の推進に関する法律、②次世代育成支援対策推進法、③青少年の雇用の促進等に関する法律に基づく認定を受けているか。

第９　審査結果の通知

審査結果については、提出期限後、おおむね３週間以内に応募者に対し文書により通知することとする。

第10　企画提案に要する費用の負担

企画書等の作成等に要する費用は、選定の成否を問わず応募者が負担するものとする。

第11 契約の締結

契約は、国と契約候補者との間で委託契約に関する協議が調い次第締結する。

第12　契約保証金の扱い

会計法（昭和22年法律第35号）第29条の９第１項に規定する契約保証金の納付は、予算決算及び会計令第100条の３第３号の規定により免除する。

第13　委託料の支払い方法

委託費の額が確定した後、受託者からの適法な請求書を受理した日から30日以内にその支払を行うものとする。ただし、受託者の請求により、必要があると認められる金額については、概算払をすることができる。

なお、概算払の請求は、予算決算及び会計令第58条ただし書に基づく協議が整った日以降とする。また、契約金額は概算契約における上限額でしかなく、事業を実施した結果、実際の所要金額がこの契約金額を下回る場合には、額の確定の上、実際の所要金額を支払うこととする。

第14　その他

（１）応募者は「責任あるサプライチェーン等における人権尊重のためのガイドライン」（令和４年９月１３日ビジネス人権に関する行動計画の実施に係る関係府省庁施策推進・連絡会議決定）を踏まえて人権尊重に取り組むよう努めること。

（２）不明な点については、第15の応募・照会窓口までお問い合わせ願いたい。

第15　応募・照会窓口

【企画書等の作成、事業内容、応募要領全般について】

農林水産省農産局 穀物課米麦流通加工対策室

（別館２階、ドアNo.別202）

ＴＥＬ：03-6744-2184

E-Mail： komeryutsu/atmark/maff.go.jp

※スパムメール対策のため、「@」は「/atmark/」と表示している。

【企画書等の提出及び契約条項等について】

農林水産省大臣官房予算課契約班（本館１階、ドアNo.本135）

ＴＥＬ：03-6744-7162

※受付曜日：月曜日～金曜日（行政機関の休日を除く。）

※受付時間：10時～17時

（別紙様式第１号）**※単独での応募の場合**

令和　年　月　日

農林水産省大臣官房参事官（経理）　殿

住　　所
商号又は名称
代表者氏名

企 画 競 争 参 加 表 明 書

令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業の企画競争に参加することを表明します。

○ 担当者

所属・役職
担当者氏名
電話番号
ﾒｰﾙｱﾄﾞﾚｽ

（別紙様式第１号）**※共同事業体での応募の場合**

令和　年　月　日

農林水産省大臣官房参事官（経理）　殿

【共同事業体代表者】
住　　所
商号又は名称
代表者氏名

企 画 競 争 参 加 表 明 書

令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業の企画競争に下記のとおり共同事業体により参加することを表明します。

また、契約の候補者となった場合は、契約締結前までに共同事業体の構成・運営等に関する協定書を作成し提出します。

なお、規約書等には、事業分担及びその考え方並びに実施体制について明確に記載します。

記

１．共同事業体名：

２．共同事業体の構成員及び担当業務

	住所及び商号又は名称	分担事業内容
代表者	〒	
構成員	〒	
構成員	〒	

【共同事業体代表者】
○担当者
所属・役職
担当者氏名
電 話 番 号
ﾒｰﾙｱﾄﾞﾚｽ

（別紙様式第２号）

令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業

区　　分	予算額	備　　考
	円	
人件費		○○　　@△△△円×○○時間＝△△△円 ○○　　@△△△円×○○時間＝△△△円 計　　△△△円
事業費		ライセンス費 ○○○　　△△△円 ○○○　　△△△円
一般管理費		人件費及び事業費（再委託費を除く）×10%以内
消費税等		
計		

（注）・再委託先の内訳を明記すること。

・必要に応じて、資料を添付すること。

・備考欄には、区分欄に掲げる経費の根拠を詳細に記載すること。

・一般管理費及び率等を利用して経費を算出する場合は根拠となる資料を添付すること。

ただし、一般管理費を経費として計上する場合は、原則、人件費及び事業費（再委託を除く）の10%以内とし、これによりがたい場合は受託者の内部規程等で定められた率を使用すること。

・備品（原形のまま比較的長期の反復使用に耐え得るもののうち取得価格が 50,000 円以上の物品）の購入は認めない。

・人件費の算定については仕様書別紙４「委託事業における人件費の算定方法等の適正化について」を参照すること。

また、根拠となる資料を添付すること。

・消費税の算出にあたり１円未満の端数は切り捨てで計算すること。

（別紙様式第３号）

暴力団排除に関する誓約事項

当社（個人である場合は私、団体である場合は当団体）は、下記１及び２のいずれにも該当せず、また、将来においても該当しないことを誓約します。

この誓約が虚偽であり、又はこの誓約に反したことにより、当方が不利益を被ることとなっても、異議は一切申し立てません。

また、貴省の求めに応じ、当方の役員名簿（有価証券報告書に記載のもの。ただし、有価証券報告書を作成していない場合は、役職名、氏名及び生年月日の一覧表）を警察に提供することについて同意します。

記

１　契約の相手方として不適当な者

（１）法人等（個人、法人又は団体をいう。）の役員等（個人である場合はその者、法人である場合は役員又は支店若しくは営業所（常時契約を締結する事務所をいう。）の代表者、団体である場合は代表者、理事等、その他経営に実質的に関与している者をいう。以下同じ。）が、暴力団（暴力団員による不当な行為の防止等に関する法律（平成３年法律第77号）第２条第２号に規定する暴力団をいう。以下同じ。）又は暴力団員（同法第２条第６号に規定する暴力団員をいう。以下同じ。）であるとき

（２）役員等が、自己、自社若しくは第三者の不正の利益を図り、又は第三者に損害を加える目的をもって、暴力団又は暴力団員を利用するなどしているとき

（３）役員等が、暴力団又は暴力団員に対して、資金等を供給し、又は便宜を供与するなど直接的又は積極的に暴力団の維持、又は運営に協力し、又は関与しているとき

（４）役員等が、暴力団又は暴力団員であることを知りながらこれを利用するなどしているとき

（５）役員等が、暴力団又は暴力団員と社会的に非難されるべき関係を有しているとき

２　契約の相手方として不適当な行為をする者

（１）暴力的な要求行為を行う者

（２）法的な責任を超えた不当な要求行為を行う者

（３）取引に関して脅迫的な言動をし、又は暴力を用いる行為を行う者

（４）偽計又は威力を用いて契約担当官等の業務を妨害する行為を行う者

（５）その他前各号に準ずる行為を行う者

上記事項について、参加表明書の提出をもって誓約します。

（別紙様式第４号）

令和　　年　　月　　日

農林水産省大臣官房参事官（経理）　殿

住　　所
商号又は名称
代表者氏名

契　約　候　補　辞　退　届

令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業に関する契約候補について、〇〇〇〇の理由により、辞退します。

別添

電子メールを利用した書類の提出方法

１．送信先

農林水産省大臣官房予算課契約班　宛

メールアドレス：nousui_itakukeiyaku/atmark/maff.go.jp

※　スパムメール対策のため、「@」を「/atmark/」と表示しておりますので、送信の際は「@」に変更してください。

２．送信メールの件名

「整理番号・事業者名・○／○」としてください。

例：012345・○○○○○(株)・1／3

※　整理番号は公示等に記載された番号を必ず記載してください。

※　○／○は何分割の何番目のメールかを記載してください。（下記６参照）

３．メール本文への記載事項

件名、事業者名、担当者名、連絡先電話番号を記載してください。

４．メール容量

本文を含め７MB です。（下記６参照）

５．添付ファイルの形式及びファイル名

ＰＤＦファイルの電子データ形式で提出してください。

ファイル名は「整理番号・提出書類名・事業者名・○／○」としてください。

例１：012345・提案書・○○○○○(株)・1／3

例２：012345・企画提案書・○○○○○(株)・1／3

例３：012345・競争参加資格・○○○○○(株)・1／1

※　複数の提出書類を一つのファイルにまとめないでください。

６．メール容量を超える場合の送信方法

７MB を超えるファイルを送信する場合には、分割して送信してください。

なお、分割しない場合も含め、送信メールの件名及びファイル名の最後に「1／1」や「1／3」など、何分割の何番目であるかを必ず記載してください。

※　圧縮ファイルは使用しないでください。

７．受信確認

メール受信後、翌日の 17 時まで又は提出期限日の 17 時までのいずれか早い日時にメールを受信した旨を送信者にメールで返信します。受信のメールが届かない場合には、１の送信先（電話の場合：03-6744-7162）に連絡してください。

仕様書

令和８年度米穀流通事業者の
届出・報告に関する業務のシステム化
調査委託事業

農林水産省

目次

1. 業務の概要

1-1. 事業の名称

令和 8 年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業

1-2. 事業の背景及び目的

農林水産省では、主要食糧の需給及び価格の安定に関する法律（平成六年法律第百十三号）に基づき、米穀の出荷又は販売の事業を行おうとする者（以下、「米穀の出荷又は販売事業者」という。）の届出を義務付け、管理するとともに、米穀の出荷又は販売事業者に対し、その取扱量に応じて月ごと又は年ごとに報告徴収を行っている。当該業務は各都道府県を管轄する北海道農政事務所、地方農政局、内閣府沖縄総合事務局（以下、「地方農政局等」という。）が主体となって実施している。

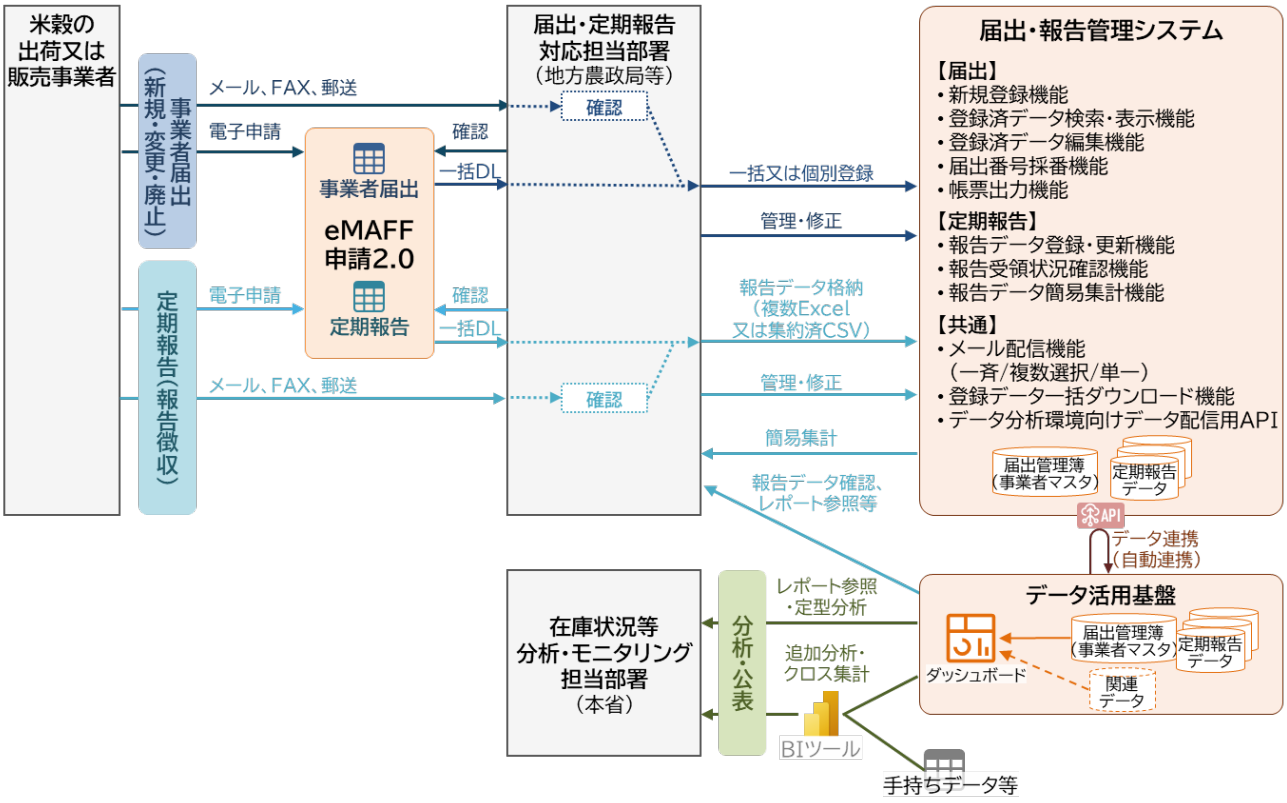
当該業務で管理するデータは、個別に Excel ファイルで管理されており、データを相互に関連づけた分析等を行うには非効率となっていることから、十分にデータを活用しきれていない。そのため、米穀流通の実態把握強化に向け、届出及び報告徴収に関するデータの管理を強化する必要がある。

また、現在は米穀の出荷又は販売事業者からの届出・報告の提出においてはメール、FAX 又は郵送が用いられているが、米穀の出荷又は販売事業者の利便性向上及び地方農政局等の業務効率化に向けた改善が必要である。

このような状況を踏まえ、農林水産省では、受領した届出・報告のデータを統合的に登録・管理する新たな情報システムを整備することを検討している。加えて、当該情報システムの整備にあわせて農林水産省共通申請サービス（eMAFF 申請 2.0）を用いた電子申請への対応、農林水産省データ活用基盤（BI 基盤）へのデータ連携及びレポートの整備を検討している（図1-2-1 参照）。

本事業は、この新たな情報システムの整備に先行してプロトタイプを構築し、システム要件及び実現方針を具体化するとともに、ユーザー視点での業務への適合性や操作性等を調査・改善することを通して、システムを用いた業務の実効性及び業務効率化等の導入効果を確認することを目的として、委託することとする。

図 1-2-1 米穀の出荷又は販売事業者の届出・定期報告に関する情報システムの将来像（案）



1-3.　業務の概要及び実施範囲

（1）業務の概要

米穀の出荷又は販売事業者の届出・報告にかかる業務のうち、届出の業務を対象として、まず必要機能及び実現方針を整理した上で、プロトタイプの作成範囲を検討し、文書にまとめる。その上で、プロトタイプをローコードプラットフォーム上に実装し、当該業務を担う職員の試用及びそのフィードバックを踏まえた機能の改善を行う。これら業務の完了後は、農産局穀物課米麦流通加工対策室（以下「事業担当部署」という。）の担当職員（以下、「監督職員」という。）等において環境の運用保守及び必要に応じた改修を実施するため、事業担当部署への支援及び環境の継続利用に必要となるライセンスを提供する。

なお、プロトタイプの環境は令和９年１月よりトライアル運用として実業務に使用予定である。

（2）業務の実施範囲

ア. 2.「業務の実施内容」に掲げる業務を実施すること。

イ. プロトタイプ環境の作成に供するローコードプラットフォームを農林水産省の職員及び受託者が利用する際に必要となるライセンスは、事業実施期間すべてにおいて受託者の負担にて提供すること。なお、プロトタイプ環境を利用する農林水産省の職員数は、管理者ユーザーが４名、一般ユーザーが 36 名とする。

ウ. 上記以外にサービス利用料、ライセンス費用、物品購入等で追加の費用を必要とする提案を行う場合、その費用は受託者の負担とする。

エ. 以下の業務及び環境利用にかかる費用は本事業の範囲外とする。

- 業務フローの検討及び業務マニュアルの作成
- 農林水産省共通申請サービス及び農林水産省データ活用基盤の利用の検討、実装に係る業務

1-4.　事業期間

委託契約締結の日から令和９年３月 31 日までとする。

1-5.　作業スケジュール

本業務及び関連する事業等のスケジュールは以下の図のとおりである。

図 1-5-1 作業スケジュール及び本業務の範囲

2. 業務の実施内容

2-1. 必要機能の検討

(1) 作業内容

① 事業担当部署が提供する現行業務に関する情報、図 2-1-1 及び 2-1-2、非機能要件等を分析し、必要機能及び実現方針を整理するとともに、プロトタイプとして作成する範囲を検討する。

② 検討結果を「届出・報告管理システム(プロトタイプ)概要設計書」にまとめる。

(2) 留意事項

ア. 業務機能の検討においては届出業務を対象とし、定期報告については考慮不要とする。

イ. 非機能要件については、以下の項目を検討対象とする。

(ア) データ活用基盤へのデータ連携を行うための機能(API 機能)

(イ) ユーザーアカウント管理(作成対象箇所、管理方法等)

(ウ) 権限管理(権限の種別、管理方法等)

(エ) バックアップ(インフラ障害、論理障害それぞれへの対策)

(オ) セキュリティ対策

(カ) その他、令和 9 年 1 月より開始予定のトライアル運用で必須となるシステム運用機能
※ 障害監視、開発環境の整備については検討対象外とする。その他検討すべき事項がなければ本項目は対応不要とする。

ウ. 各機能の実現方法の検討においては、ローコードプラットフォームに標準で組み込まれている機能や、簡易な追加設定で実現できる手法の利用を優先すること。

エ. プロトタイプとして作成する範囲の決定においては、当該機能の実現にかかる作業工数や技術的難易度を踏まえ、事業担当部署と協議の上で決定すること。

図 2-1-1 新規の届出における業務の流れとシステムの機能構成(案)

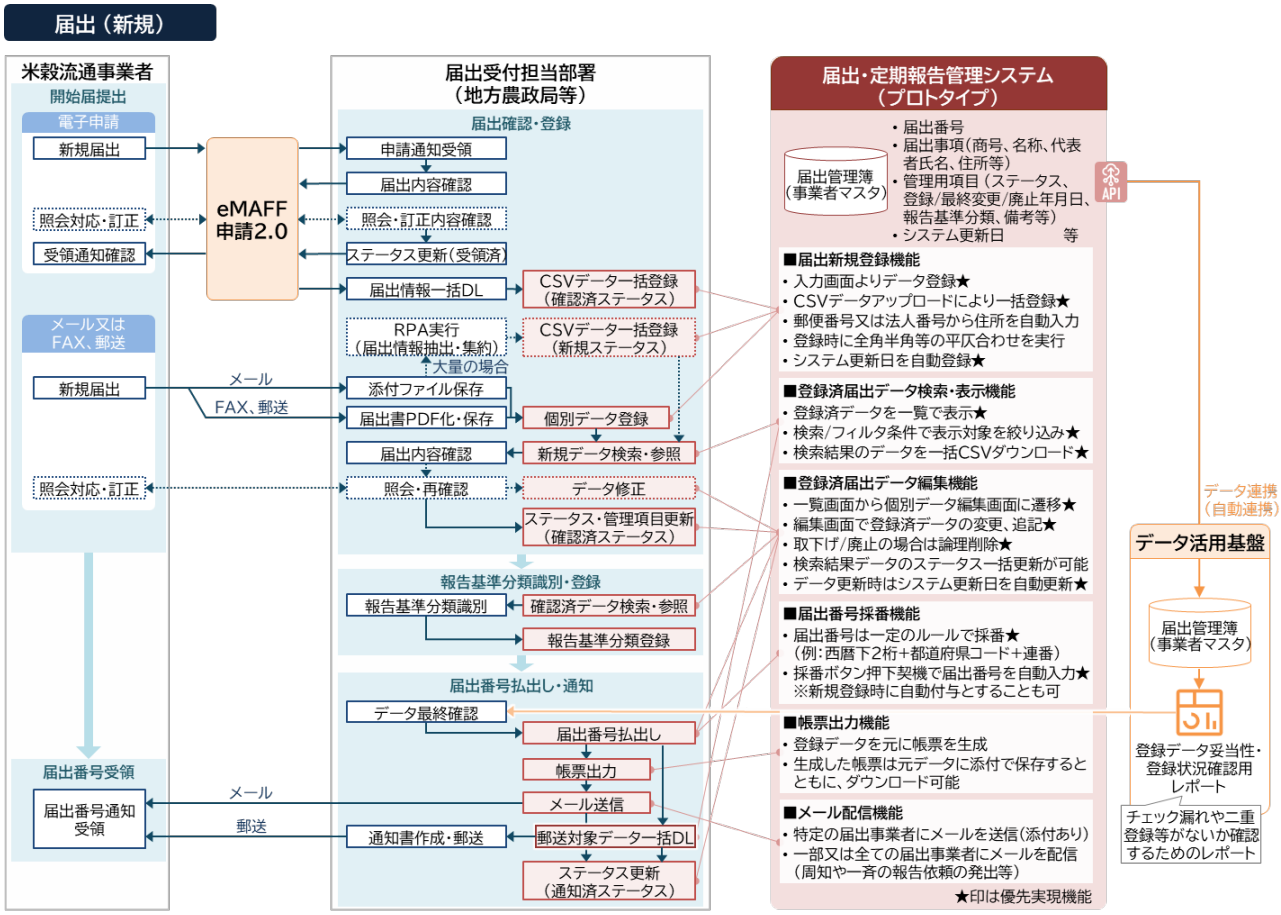
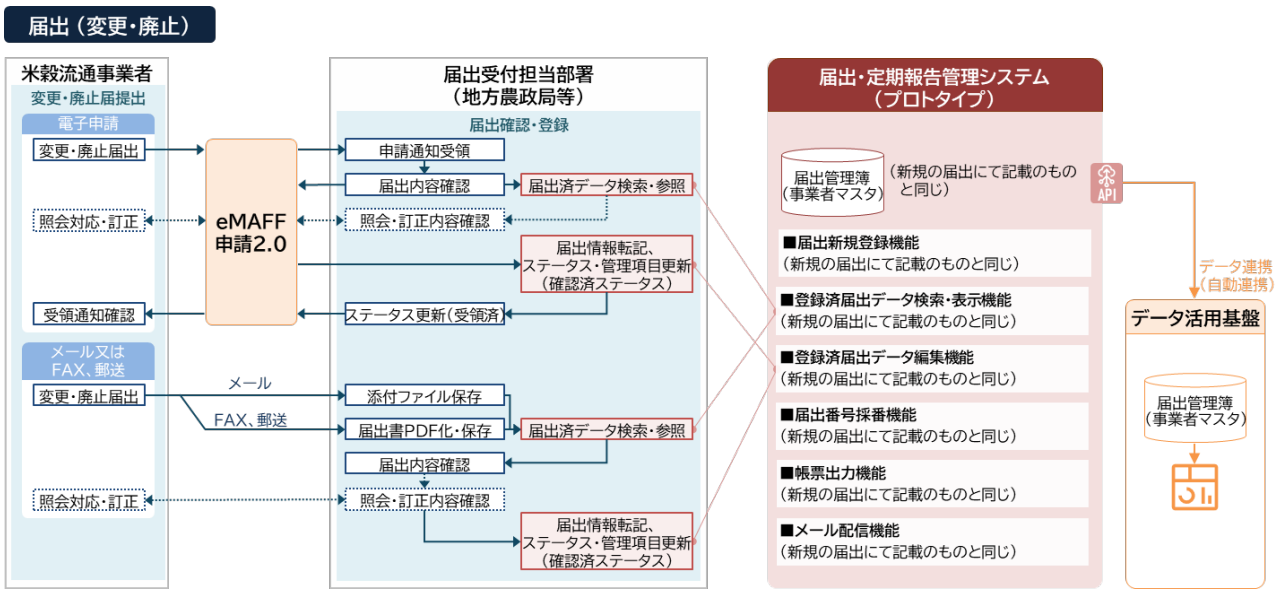


図 2-1-2 変更の届出又は廃止の届出における業務の流れとシステムの機能構成(案)



2-2. プロトタイプアプリの作成

（1）作業内容

① 事業担当部署が提供する管理対象データ項目を元にアプリ実装の具体的内容を検討する。

② 2-1 でプロトタイプとして作成する範囲としたものについて、あらかじめ選定したローコードプラットフォーム上でアプリとして実装し、その内容を事業担当部署に実際の画面を用いて説明する。

③ 事業担当部署から不備等の指摘を受けたものについて、修正の検討及び対応を行う。
ただし、工数及び技術的難易度の観点から対応が困難な場合は、事業担当者にその旨の説明及び回避策を検討の上、修正の対応をしないこととする。

④ 作成したアプリについて、簡易操作マニュアルを作成し、事業担当部署に説明する。

（2）留意事項

ア. プロトタイプのアプリを実装する上で必要となる要件や情報が不足している場合は、速やかにその内容を事業担当者に申し出て、情報の提供を受けること。

イ. 利用するローコードプラットフォームは、本業務の受託者が企画書提出時に採用を提案したサービスを使用する。なお、ローコードプラットフォームの提案における補足事項は、7.2「ローコードプラットフォームの提案に関する補足事項」を参照すること。

ウ. 簡易操作マニュアルは、以下の内容に沿って作成すること。

（ア）説明項目は以下の内容を含めること。

- 画面及び機能の構成及び概要
- ログイン及びパスワード変更の方法
- 機能ごと（図 2-1-1 の右方「届出・定期報告管理システム（プロトタイプ）」に記載のもの。ただしプロトタイプ実装対象外のものは除く。）の基本的な操作方法
- ユーザーメンテナンス・権限設定の方法（管理者向け）

（イ）各説明項目は、原則当該機能の使用にあたって発生する画面遷移、機能の呼び出し方法やデータ登録/更新の手順に焦点を絞って記載することとする。したがって、入力するデータ項目を個別に説明することは要しない。

（ウ）機能の制約や間違いやすい箇所がある場合は注意書きを記載すること。

2-3. アプリの実証と改善

（1）作業内容

① 地方農政局等の届出の受付業務を担当する部署及びその職員（以下、「届出受付業務担当部署」という。）に向けた説明会を開催し、以下について説明及び依頼を行う。なお、当該説明会は WEB

会議形式での開催とする。
- プロトタイプアプリの試用における進め方と依頼事項の説明
- 簡易操作マニュアル及び実際の画面を用いたプロトタイプアプリの操作方法の説明
- 「プロトタイプアプリ指摘事項一覧」の記載方法の説明

② 届出受付業務担当部署より提起された指摘事項について、それぞれ改善対応の可否及び方法を検討し、事業担当部署と協議して対応方針を決定する。

③ 改善対応を実施するとしたものについて、その対応を実施し、事業担当部署に説明する。
指摘内容に応じて起票者に確認を取るべきものと判断されるものについては、起票者に対応結果を報告し、課題等が解決していることを確認する。

（2）留意事項

ア. 本作業は、業務を担当する職員自らが操作の容易性や業務適合性を確認し、さらにその結果を踏まえて機能の改善を図ることにより、当該アプリを用いた業務の実施可能性を確保することを目的に実施するものである。

イ. プロトタイプアプリ試用の前に、効率的かつ実効性高くフィードバックを得るために有効と考えられる策の検討及び事業担当部署と協議し、説明会実施前に準備を行うこと。
（検討例： 試用における確認観点の提示、モデルシナリオやテストデータの提供 等）

ウ. 届出受付業務担当部署に向けた説明会では、受託者からの説明の前段で、事業担当部署より以下の説明を行う。
- 届出・報告に関する業務の見直し等に係る全体的な説明
- プロトタイプアプリの試用の位置づけ・目的
- プロトタイプアプリを用いた業務フローの説明

エ. 改善の検討に際しては、その内容の重要度、改善難易度や作業期間・工数等を鑑み、事業担当部署と協議して対応の要否及び対応内容を決定すること。

オ. 指摘事項に対する対応方針及び対応結果は、「プロトタイプアプリ指摘事項一覧」に列を設けてそれぞれ記録すること。なお、対応を見送った事項はその理由についても記録すること。

カ. 本作業は原則、令和 8 年 9 月末までに完了させること。

2-4. アプリ運用・改修を行う職員への支援等

（1）実施内容

① 2-3 に掲げた業務の完了後、事業担当部署にて、取り扱う報告様式の追加などのアプリ改修及び業務利用の試行等を想定しており、この期間においては、事業担当部署からの問合せ対応や技術的アドバイス等の支援を行う。

（2）留意事項

ア. 事業担当部署への支援にかかる工数は、1か月あたり16時間を目安とする。

イ. プロトタイプのアプリの利用に係るライセンスを引き続き提供するものとする。
利用ユーザー数は 1-3(2)のイに記載のとおり。

3. 成果物

3-1. 作成する成果物

（1）事業が終了したとき（委託事業を中止し、又は廃止したときを含む。）は、委託事業で実施した事項及びその成果を記載した委託事業実績報告書を提出し、監督職員に説明すること。

（2）委託事業実績報告書の付属資料として、業務実施の一環で作成した以下の文書を提出すること。

① 届出・報告管理システム（プロトタイプ）概要設計書

② 届出・報告管理システム（プロトタイプ）簡易操作マニュアル

③ プロトタイプアプリ指摘事項一覧

（3）その他、5-5「人件費の算定の適正化」の記載事項に基づき作成した作成した事業従事者ごとの業

務日誌をあわせて提出すること。

3-2. 成果物作成の要件

（1）成果物は、全て日本語で作成すること。ただし、日本国内においても英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。

（2）用字・用語・記述符号の表記については、「「公用文作成の考え方」の周知について（令和４年１月11日内閣文第１号内閣官房長官通知）」を参考にすること。

（3）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。

（4）成果物は原則 Microsoft Office 形式で作成すること。

（5）構成図等の複雑な図を作成する場合は Power Point 形式又は Draw.io 形式を使用すること。

（6）成果物の作成に当たって、特別なツールを使用する場合は、監督職員の承認を得ること。

（7）各成果物の提出にあたっては、事前にドラフト版の文書等を監督職員に説明する等、契約終了日に完成版の成果物提出を確実に完了できるよう適時の事前準備を行うこと。

3-3. 成果物の納品方法

（1）納品後、当省において編集が可能となるよう、図表等の元データも併せて納品すること。

（2）成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。

（3）納品する電子データについて不正プログラム対策ソフトウェアによる確認を行い、電子データの安全性を確認するととも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。

（4）納品対象データの受け渡しは、事業担当部署から特別に示す場合を除き、パスワードを付け、電子ファイルを大容量ファイル転送システム等により納品すること。

（5）成果物は事業担当部署に提出すること。

3-4. 成果物の取り扱いに関する事項

（1）本業務における成果物の原著作権及び二次的著作物の著作権（著作権法第 21 条から第 28 条に定める全ての権利を含む。）は、受託者が本業務の実施の従前から権利を保有していた等の明確な理由によりあらかじめ企画書にて権利譲渡不可能と示されたもの以外は、全て農林水産省に帰属するものとする。

（2）農林水産省は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改変等し、及びそれらの利用を第三者に許諾することができるとともに、任意に開示できるものとする。

（3）成果物に第三者が権利を有する著作物（以下「既存著作物等」という。）が含まれる場合には、受託者は、当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、本業務の受託者は、当該既存著作物の内容について事前に農林水産省 z の承認を得ることとし、農林水産省は、既存著作物等について当該許諾条件の範囲で使用するものとする。なお、本仕様に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争の原因が専ら農林水産省の責めに帰す場合を除き、受託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、農林水産省は係る紛争等の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者に委ねる等の協力措置を講じるものとする。

（4）成果物の所有権は、農林水産省から受託者に対価が完済されたとき受託者から農林水産省に移転するものとする。

（5）受託者は農林水産省に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。

（6）受託者は使用する画像、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。

4. 作業の実施体制・方法

4-1. 作業実施体制

本業務の作業実施体制は、原則、企画書提出時に提出した企画書に記載した体制案に沿って整備すること。

なお、本業務の実施体制には、届出・報告管理システムのプロトタイプアプリ実装に用いるローコードプラットフォームとして提案するクラウドサービスの資格を有している者又はそれと同等の知識を持つと認められる人員を含めることとする。

4-2. 作業実施方法

本業務の作業実施方法は、原則、企画書提出時に提出した企画書に記載したスケジュール及び実施方法等の計画に沿って推進すること。当該計画の変更の必要が生じた際は、速やかに事業担当部署に報告するとともに、見直し案を提出し、承認を得ること。

また、特に各業務で実施する検討やレビューにおいては、事業担当部署と密接に連携して実施することとし、チャットアプリの利用や必要に応じた WEB 会議の開催など、業務を円滑に推進するための方策を検討・実施すること。

なお、事業開始から 2-3 に掲げた業務(アプリの実証と改善)が完了するまでは少なくとも 1 週間に 1 度の頻度で、それ以降は必要な頻度で会議を行うこととする。

4-3. 作業場所

(1) 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、受託者の責任と負担において用意すること。また、必要に応じて監督職員が現地確認を実施することができるものとする。

(2) 事業担当部署が参加する会議は WEB 形式での開催又は農林水産省内での開催とし、事前に日程等を事業担当部署と協議し、会場の確保に努めること。なお、WEB 形式の場合は、事業担当部署に対し、WEB 会議に参加するための WEB 会議環境を提供すること。なお、農林水産省では、WEB 会議システムとして Teams、Webex 及び ZOOM が使用可能である。

5. 作業の実施に当たっての遵守事項

5-1. 機密保持、資料の取扱い

(1) 事業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3月31日農林水産省訓令第4号。以下「規則」という。)、「農林水産省における個人情報の適正な取扱いのための措置に関する訓令」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、政府機関等のサイバー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) 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. 受注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をしないこと。

ウ. 持出しを禁止すること。

エ. 受注事業者の責に起因する情報セキュリティインシデントが発生するなどの万一の事故があった場合に直ちに報告する義務や、損害に対する賠償等の責任を負うこと。

オ. 業務の履行中に受け取った情報の管理、業務終了後の返却又は抹消等を行い復元不可能な状態にすること。

カ. 適切な措置が講じられていることを確認するため、遵守状況の報告を求めることや、必要に応じて発注者による実地調査が実施できること。

(3) 上記以外に、別紙1「情報セキュリティの確保に関する共通基本仕様」に基づき、作業を行うこと。

5-2. 個人情報の取扱い

(1) 個人情報(生存する個人に関する情報であって、当該情報に含まれる氏名、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。)の取扱いに

係る事項について農林水産省と協議の上決定し、書面にて提出すること。なお、以下の事項を記載すること。

- 個人情報の取扱いに関する責任者が情報管理責任者と異なる場合には、個人情報の取扱いに関する責任者等の管理体制
- 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、作業実施前に教育を実施し、認識を徹底させること。なお、受託者はその旨を証明する書類を提出し、農林水産省の了承を得たうえで実施すること。

（3）個人情報を複製する際には、事前に担当職員の許可を得ること。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・消去を実施すること。なお、受託者は廃棄作業が適切に行われた事を確認し、その保証をすること。

（4）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。

（5）受託者は、農林水産省からの指示に基づき、個人情報の取扱いに関して原則として年1回以上の実地検査を受け入れること。なお、やむを得ない理由により実地検査の受入れが困難である場合は、書面検査を受け入れること。また、個人情報の取扱いに係る業務を再委託する場合は、受託者（必要に応じ農林水産省）は、原則として年1回以上の再委託先への実地検査を行うこととし、やむを得ない理由により実地検査の実施が困難である場合は、書面検査を行うこと。

（6）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。

5-3. 環境関係法令の遵守

受託者は、委託事業の提供に当たり、関連する環境関係法令を遵守するものとする。

（1）エネルギーの節減

- エネルギーの使用の合理化及び非化石エネルギーへの転換等に関する法律（昭和 54 年法律第 49 号）

（2）廃棄物の発生抑制、適正な循環的な利用及び適正な処分

- 廃棄物の処理及び清掃に関する法律（昭和 45 年法律第 137 号）
- 国等による環境物品等の調達の推進等に関する法律（平成 12 年法律第 100 号）
- プラスチックに係る資源循環の促進等に関する法律（令和3年法律第 60 号）

（3）環境関係法令の遵守等

- 労働安全衛生法（昭和 47 年法律第 57 号）
- 地球温暖化対策の推進に関する法律（平成 10 年法律第 117 号）

5-4. 環境負荷低減に係る取組の実施及び実施状況報告書の提出

受託者は、委託事業の提供に当たり、新たな環境負荷を与えることにならないよう、事業の最終報告時に様式を用いて以下の取組に努めたことを、別紙 3 「みどりチェック実施状況報告書」として提出すること。なお、全ての事項について「実施した／努めた」又は「左記非該当」のどちらかにチェックを入れるとともに、ア～エの各項目について、一つ以上「実施した／努めた」にチェックを入れること。

ア. 環境負荷低減に配慮したものを調達するよう努める。

イ. エネルギーの削減の観点から、オフィスや車両・機械などの電気、燃料の使用状況の記録・保存や、不必要・非効率なエネルギー消費を行わない取組（照明、空調のこまめな管理や、ウォームビズ・クールビズの励行、燃費効率の良い機械の利用等）の実施に努める。

ウ. 廃棄物の発生抑制、適正な循環的な利用及び適正な処分に努める。

エ. みどりの食料システム戦略の理解に努めるとともに、機械等を扱う場合は、機械の適切な整備及び管理並びに作業安全に努める。

5-5. 人件費の算定の適正化

本事業における人件費の算定及び報告にあたっては、別紙 4「委託事業における人件費の算定等の適正化について」に従うこと。

6. 再委託に関する事項

（1）受託者は、業務の全部を一括して、又は主たる部分を第三者に委任し、又は請け負わせてはならない。なお、主たる部分とは、業務における総合的企画、業務遂行管理、手法の決定及び技術的判断等をいう。

（2）受託者は、効率的な履行をはかるため、主たる部分以外の部分について、業務の一部を第三者に委任し、又は請け負わせること（以下「再委託」という。）を必要とするときは、契約書に定める様式に必要事項を記入してあらかじめ発注者の承認を得なければならない。なお、再委託先名及び金額が企画提案書に明記されている場合には、企画提案書の採用をもって事前の承認に代えることができる。

（3）受託者は、（2）の承認を受けた再委託について、その内容を変更する必要が生じたときは、同様式に必要事項を記入して、あらかじめ発注者の承認を得なければならない。

7. その他特記事項

7-1. 前提条件等

受託者は、本仕様書に明示されていない事項及び疑義が生じた事項については、事業担当部署と協議を行い、必要に応じ契約書に則った手続を行うものとする。

7-2. ローコードプラットフォームの提案に関する補足事項

（1）プロトタイプのアプリ実装に用いるローコードプラットフォームについて、本事業の企画書にて利用するクラウドサービス及び選定理由を記載すること。

（2）本業務の実施において利用するクラウドサービス（ローコードプラットフォームのサービス及び当該サービスと連携して動作するクラウドサービスを含む。）は、別紙 1「情報セキュリティの確保に関する共通基本仕様」に記載のとおり、以下の要件を満たす必要がある。

ア. 原則として、ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリスト（以下「ISMAP クラウドサービスリスト等」という。）に登録されているクラウドサービスであること。

イ. ISMAP クラウドサービスリスト等に登録されていないクラウドサービスの場合は、ISMAP の管理基準に従い、ガバナンス基準及びマネジメント基準における全ての基準、管理策基準における統制目標（3桁の番号で表現される項目）及び末尾にBが付された詳細管理策（4桁の番号で表現される項目）を原則として全て満たしていることを証明する資料を提出し、農林水産省の承認を得ること。

※「末尾にBが付された詳細管理策」には、末尾が「PB」となっているものを含む。

（3）ISMAP クラウドサービスリスト等に登録されていないクラウドサービスの提案を行う場合、本事業の公示期間中に事業担当部署にその旨を申し出ることにより、事業担当部署を通じて事前農林水産省のセキュリティ担当部署への事前の問合せ又は相談をすることができる。

（4）前項の申し出に際しては、7-3「本仕様書に関する質問」に沿って質問票対象のクラウドサービスが 7-2（2）イに掲げられた条件をすべて満たしていることを証明する資料として、別紙 2「ISMAP 基本言明要件の一覧」にある要件のうち、適合が求められるものについて、以下の事項を追記した一覧表を作成し、あわせて提出すること。

ア. 適合状況 ・・・「〇」又は「×」で表現

イ. 採用しているセキュリティ対策概要

・・・適合状況が「〇」の場合、その具体的な対策内容を記載する。当該対策が他の社内規則等に基づき実施している場合はその規則名を記載するなど、記載内容が妥当であると判断しやすいよう可能な限り具体的な内容を記載すること。

ウ. 非採用理由

・・・適合状況が「×」の場合、対策を取る必要がない理由又は採用している代替措置等、非採用としている理由の妥当性が判断できる事項を記載

7-3. 本仕様書に関する質問

本仕様書について疑義等がある場合、別紙5「質問票」にその内容を記載し、7-5「本仕様書に関する質問及び資料閲覧に関する連絡先」に記載の窓口に提出すること。なお、質問票に対する回答は適宜行うこととする。

7-4. 公示期間中の資料閲覧

本業務の実施に当たり参考となる資料について、公示期間中（行政機関の休日を除く。）に農林水産省内にて閲覧可能とする。

（1）資料閲覧場所

東京都千代田区霞が関 1-2-1
農林水産省農産局穀物課米麦流通加工対策室（別館 2 階、ドア No.別 202）

（2）閲覧期間及び時間

- 公示期間（行政機関の休日を除く）
- 10 時から 17 時まで。（12 時から 13 時を除く。）

（3）閲覧手続き

7-5「本仕様書に関する質問及び資料閲覧に関する連絡先」に記載の連絡先まで連絡し、閲覧日時を調整すること。また、閲覧日当日までに別紙6「資料閲覧申請書」及び別紙7「機密保持誓約書」を記入の上、提出すること。

（4）閲覧時の注意

閲覧にて知り得た内容については、企画書の作成以外には使用しないこと。また、本業務に関与しない者等に情報が漏えいしないように留意すること。閲覧資料の複写等による閲覧内容の記録は行わないこと。

（5）事業者が閲覧できる資料

ア. 届出事業者制度運用要領
イ. 現行業務整理・ヒアリング結果取りまとめ資料
ウ. 届出管理簿サンプル（現行及び見直し案）
エ. 届出様式見直し案
オ. 届出・定期報告システム整備計画書の一部

7-5. 本仕様書に関する質問及び資料閲覧に関する連絡先

課室名　農林水産省農産局穀物課米麦流通加工対策室
電話　03-6744-2184
E-Mail　komeryutsu/atmark/maff.go.jp
※スパムメール対策のため、「@」は「/atmark/」と表示している。

8. 附属文書

別紙１ 情報セキュリティの確保に関する共通基本仕様
別紙２ ISMAP 基本言明要件の一覧
別紙３ みどりチェック実施状況報告書
別紙４ 委託事業における人件費の算定等の適正化について
別紙５ 質問票
別紙６ 資料閲覧申請書
別紙７ 機密保持誓約書

以上

【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、政府機関等のサイバー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　応札者に関する情報の提供

１　応札者は、応札者の資本関係・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　応札者は、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）独立行政法人情報処理推進機構（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

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、以下の措置を講ずること。なお、応札者は、以下の措置を講ず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、第三者に開示し、又は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）本業務に係る情報を適切に取り扱うことが可能となるよう、情報セキュリティ対策の実施内容及び管理体制を整備すること。なお、本業務実施中及び実施後において検証が可能となるよう、必要なログの取得や作業履歴の記録等を行う実施内容及び管理体制とすること。

（4）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。

（5）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 26 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。

（6）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。

（7）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。

2　受託者は、委託期間を通じて以下の措置を講ずること。

（1）情報の適正な取扱いのため、取り扱う情報の格付等に応じ、以下に掲げる措置を全て含む情報セキュリティ対策を実施すること。また、実施が不十分の場合、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。

ア　情報セキュリティインシデント等への対処能力の確立・維持

イ　情報へアクセスする主体の識別とアクセスの制御

ウ　ログの取得・監視

エ　情報を取り扱う機器等の物理的保護

オ　情報を取り扱う要員への周知と統制

カ　セキュリティ脅威に対処するための資産管理・リスク評価

キ　取り扱う情報及び当該情報を取り扱うシステムの完全性の保護

ク　セキュリティ対策の検証・評価・見直し

（2）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。

（3）本業務において情報セキュリティインシデントの発生、情報の目的外使用等を認知した場合、直ちに委託事業の一時中断等、必要な措置を含む対処を実施すること。

（4）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。

（5）本業務において取り扱う情報が本業務上不要となった場合、担当部署の指示に従い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。

3　受託者は、委託期間の終了に際して以下の措置を講ずること。

（1）本業務の実施期間を通じてセキュリティ対策が適切に実施されたことを書面等により報告すること。

（2）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。

（3）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。

4　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。

Ⅳ　情報システム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に関する業務を行う場合には、以下の措置を講ずること。なお、応札者は、以下の措置を講ずることを証明する資料を提出すること。

（1）本業務の各工程において、農林水産省の意図しない情報システムに関する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。）。

（2）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。

2　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、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や監視のために必要な機能を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やサ

ービス不能攻撃を監視する機能

（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）端末等の農林水産省内ネットワークの末端に位置する機器及びサーバ装置において不正プログラムの挙動を監視する機能

（エ）農林水産省内通信回線への端末の接続を監視する機能

（オ）端末への外部電磁的記録媒体の挿入を監視する機能

（カ）サーバ装置等の機器の動作を監視する機能

（キ）ネットワークセグメント間の通信を監視する機能

（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。

（３）開発する情報システムに意図しない不正なプログラム等が組み込まれないよう、以下を全て含む対策を本業務の成果物に明記すること。

ア　情報システムで利用する機器等を調達する場合は、意図しない不正なプログラム等が組み込まれていないことを確認すること。

イ　アプリケーション・コンテンツの開発時に意図しない不正なプログラム等が混入されることを防ぐための対策を講ずること。

ウ　情報システムの構築を委託する場合は、委託先において農林水産省が意図しない変更が加えられないための管理体制を求めること。

（４）要安定情報を取り扱う情報システムを構築する場合は、許容される停止時間を踏まえて、情報システムを構成する要素ごとに、以下を全て含むセキュリティ要件を定め、本業務の成果物に明記すること。

ア　端末、サーバ装置及び通信回線装置等の冗長化に関する要件

イ　端末、サーバ装置及び通信回線装置並びに取り扱われる情報に関するバックアップの要件

ウ　情報システムを中断することのできる時間を含めた復旧に関する要件

（５）開発する情報システムのネットワーク構成について、以下を全て含む要件を定め、本業務の成果物に明記すること。

ア　インターネットやインターネットに接点を有する情報システム（クラウドサービスを含

む。）から分離することの要否の判断及びインターネットから分離するとした場合に、分離を確実にするための要件

イ　端末、サーバ装置及び通信回線装置上で利用するソフトウェアを実行するために必要な通信要件

ウ　インターネット上のクラウドサービス等のサービスを利用する場合の通信経路全般のネットワーク構成に関する要件

エ　農林水産省外通信回線を経由して機器等に対してリモートメンテナンスすることの要否の判断とリモートメンテナンスすることとした場合の要件

３　受託者は、本業務において情報システムの構築を行う場合には、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

ア　主体認証機能

イ　アクセス制御機能

ウ　権限管理機能

エ　識別コード・主体認証情報の付与管理

オ　ログの取得・管理

カ　暗号化機能・電子署名機能

キ　暗号化・電子署名に係る管理

ク　監視機能

ケ　ソフトウェアに関する脆（ぜい）弱性等対策

コ　不正プログラム対策

サ　サービス不能攻撃対策

シ　標的型攻撃対策

ス　動的なアクセス制御

セ　アプリケーション・コンテンツのセキュリティ

ソ　政府ドメイン名（go.jp）の使用

タ　不正なウェブサイトへの誘導防止

チ　農林水産省外のアプリケーション・コンテンツの告知

（２）監視機能及び監視のための復号・再暗号化

監視のために必要な機能について、２（１）イの各項目を例として必要な機能を設けること。また、必要に応じ、監視のために暗号化された通信データの復号化や、復号されたデータの再暗号化のための機能を設けること。

（３）情報セキュリティの観点に基づくソフトウェアの選定

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可能な限り最新版を選定し、利用するソフトウェアの種類、バージョン及びサポート期限に係る情報を農林水産省に提供すること。

ただし、サポート期限が公表されていないソフトウェアについては、情報システムのライフサイクルを踏まえ、ソフトウェアの発売等からの経過年数や後継となるソフトウェアの有無等を考慮して選定すること。

（4）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の分離

イ　試験項目及び試験方法の決定並びにこれに基づいた試験の実施

ウ　試験の実施記録の作成・保存

（5）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　変更管理、アクセス制御、バックアップの取得等、ソースコードの不正な変更・消去を防止するための管理

イ　調達仕様書等に規定されたセキュリティ実装方針の適切な実施

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の設計レビュー及びソースコードレビューの範囲及び方法の決定並びにこれに基づいたレビューの実施

エ　オフショア開発を実施する場合の試験データに実データを使用することの禁止

（6）政府共通利用型システムの利用における情報セキュリティ対策

ガバメントソリューションサービス（GSS）等、政府共通利用型システムが提供するセキュリティ機能を利用する情報システムを構築する場合は、政府共通利用型システム管理機関が定める運用管理規程等に基づき、政府共通利用型システムの情報セキュリティ水準を低下させることがないように、適切なセキュリティ要件を実装すること。

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、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。

ア　情報システムの運用環境に課せられるべき条件の整備

イ　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

ウ　情報システムの保守における情報セキュリティ対策

エ　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

オ　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

カ　「デジタル・ガバメント推進標準ガイドライン」(デジタル社会推進会議幹事会決定。最終改定:2025 年 5 月 27 日)の「別紙3 調達仕様書に盛り込むべき情報資産管理標準シートの提出等に関する作業内容」に基づく情報資産管理を行うために必要な事項を記載した情報資産管理標準シートの提出

キ　アプリケーション・コンテンツ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、サポートを継続している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アプリケーション・コンテンツ等の修正

（2）情報システムの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。

ア　情報セキュリティに関わる運用保守体制の整備

イ　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

ウ　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

（3）情報システムのセキュリティ監視を行う場合には、以下の内容を全て含む監視手順を定め、適切に監視運用すること。

ア　監視するイベントの種類や重要度

イ　監視体制

ウ　監視状況の報告手順や重要度に応じた報告手段

エ　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

オ　監視運用における情報の取扱い（機密性の確保）

（4）　情報システムで不要となった識別コードや過剰なアクセス権限等の付与がないか定期的に見直しを行うこと。

（5）　情報システムにおいて定期的に脆（ぜい）弱性対策の状況を確認すること。

（6）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。

（7）要安定情報を取り扱う情報システムについて、以下の内容を全て含む運用を行うこと。

ア　情報システムの各構成要素及び取り扱われる情報に関する適切なバックアップの取得及びバックアップ要件の確認による見直し

イ　情報システムの構成や設定の変更等が行われた際及び少なくとも年１回の頻度で定期的に、情報システムが停止した際の復旧手順の確認による見直し

（8）ガバメントソリューションサービス（GSS）等、本業務の調達範囲外の政府共通利用型システムが提供するセキュリティ機能を利用する情報システムを運用する場合は、政府共通利用型システム管理機関との責任分界に応じた運用管理体制の下、政府共通利用型システム管理機関が定める運用管理規程等に従い、政府共通利用型システム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）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し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直すこと。

５　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　情報システムの一部の機能を提供するサービスに関する情報セキュリティの確保

応札者は、要機密情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除くものとし、以下「業務委託サービス」という。）に関する業務を実施する場合は、業務委託サービス毎に以下の措置を講ずること。

１　業務委託サービスの中断時や終了時に円滑に業務を移行できるよう、取り扱う情報の可用性に応じ、以下を例としたセキュリティ対策を実施すること。

（1）業務委託サービス中断時の復旧要件

（2）業務委託サービス終了または変更の際の事前告知の方法・期限及びデータ移行方法

２　業務委託サービスを提供する情報処理設備が収容されているデータセンターが設置されている独立した地域（リージョン）が国内であること。

３　業務委託サービスの契約に定める準拠法が国内法のみであること。

４　ペネトレーションテストや脆（ぜい）弱性診断等の第三者による検査の実施状況と受入に関する情報が開示されていること。

５　業務委託サービスの利用を通じて農林水産省が取り扱う情報について、目的外利用を禁止すること。

６　業務委託サービスの提供に当たり、業務委託サービスの提供者若しくはその従業員、再委託先又はその他の者によって、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）。

７　業務委託サービスの提供者の資本関係、役員等の情報、業務委託サービスの提供が行われる施設等の場所、業務委託サービス提供に従事する者（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（情報セキュリティに係る資格、研修実績等）、実績及び国籍に関する情報を記載した資料を提出すること。

８　業務委託サービスの提供者の情報セキュリティ水準を証明する、Ⅱの2で掲げる証明書等または同等以上の国際規格等の証明書の写しを提出すること。

９　情報セキュリティインシデントへの対処方法を確立していること。

10　情報セキュリティ対策その他の契約の履行状況を確認できること。

11　情報セキュリティ対策の履行が不十分な場合の対処方法を確立していること。

12　業務委託サービスの提供者との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について業務委託サービスの提供者と合意し、定められた手順により情報を取り扱うこと。

Ⅵ　クラウドサービスに関する情報セキュリティの確保

応札者は、本業務において、クラウドサービス上で要機密情報を取り扱う場合は、当該クラウドサービスごとに以下の措置を講ずること。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、Ｘの措置を講ずること。

１　サービス条件

（１）クラウドサービスを提供する情報処理設備が収容されているデータセンターについて、設置されている独立した地域（リージョン）が国内であること。

（２）クラウドサービスの契約に定める準拠法が国内法のみであること。

（３）クラウドサービス終了時に情報を確実に抹消することが可能であること。

（４）本業務において要求されるサービス品質を満たすクラウドサービスであること。

（５）クラウドサービス提供者の資本関係、役員等の情報、クラウドサービス提供に従事する者（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）のうち農林水産省の情報又は農林水産省が利用するクラウドサービスの環境に影響を及ぼす可能性のある者の所属、専門性（情報セキュリティに係る資格、研修実績等）、実績及び国籍に関する情報を記載した資料を提出すること。

（６）ペネトレーションテストや脆（ぜい）弱性診断等の第三者による検査の実施状況と受入に関する情報が開示されていること。

（７）原則として、ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリスト（以下「ISMAP クラウドサービスリスト等」という。）に登録されているクラウドサービスであること。

（８）ISMAP クラウドサービスリスト等に登録されていないクラウドサービスの場合は、ISMAP の管理基準に従い、ガバナンス基準及びマネジメント基準における全ての基準、管理策基準における統制目標（３桁の番号で表現される項目）及び末尾にＢが付された詳細管理策（４桁の番号で表現される項目）を原則として全て満たしていることを証明する資料を提出し、農林水産省の承認を得ること。

２　クラウドサービスのセキュリティ要件

（１）クラウドサービスについて、以下の要件を満たしていること。

ア　クラウドサービス提供者が提供する主体認証情報の管理機能が農林水産省の要求事項を満たすこと。

イ　クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御できること。

ウ　クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作が特定されていること。

エ　クラウドサービス内及び通信経路全般における暗号化が行われていること。

オ　クラウドサービス上に他ベンダが提供するソフトウェア等を導入する場合、ソフトウェアのクラウドサービス上におけるライセンス規定に違反していないこと。

カ　クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合、その機能を確認していること。

キ　暗号鍵管理機能をクラウドサービス提供者が提供する場合、鍵管理手順、鍵の種類の情報及び鍵の生成から廃棄に至るまでのライフサイクルにおける情報をクラウドサービス提供者から入手し、またリスク評価を実施していること。

ク　利用するクラウドサービスのネットワーク基盤が他のネットワークと分離されていること。

ケ　クラウドサービス提供者が提供するバックアップ機能を利用する場合、農林水産省の要求事項を満たすこと。

（2）クラウドサービスで利用するアカウント管理に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービス提供者が付与し、又はクラウドサービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理

イ　クラウドサービスを利用する情報システムの管理者権限を保有するクラウドサービス利用者に対する、強固な認証技術による認証

ウ　クラウドサービス提供者が提供する主体認証情報の管理機能について、農林水産省の要求事項を満たすための措置の実施

（3）クラウドサービスで利用するアクセス制御に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービス上に保存する情報やクラウドサービスの機能に対する適切なアクセス制御

イ　インターネット等の農林水産省外通信回線から農林水産省内通信回線を経由せずにクラウドサービス上に構築した情報システムにログインすることを認める場合の適切なセキュリティ対策

（4）クラウドサービスで利用する権限管理に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービス利用者によるクラウドサービスに多大な影響を与える誤操作の抑制

イ　クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の利用者の制限

（5）クラウドサービスで利用するログの管理に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービスが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために必要なログの管理

（6）クラウドサービスで利用する暗号化に関して、以下のセキュリティ機能要件を満たしていること。

ア　クラウドサービス内及び通信経路全般における暗号化の適切な実施

イ　情報システムで利用する暗号化方式の遵守度合いに係る法令や農林水産省訓令等の関連する規則の確認

ウ　暗号化に用いる鍵の保管場所等の管理に関する要件

エ　クラウドサービスで利用する暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理

（7）クラウドサービスを利用する際の設計・設定時の誤り防止に関して、以下のセキュリティ要件を満たしていること。

ア　クラウドサービス上で構成される仮想マシンに対する適切なセキュリティ対策

イ　クラウドサービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用

ウ　クラウドサービス提供者への設計、設定、構築等における知見等の情報の要求とその活用

エ　クラウドサービスの設定の誤りを見いだすための対策

（8）クラウドサービス運用時の監視等に関して、以下の運用管理機能要件を満たしていること。

ア　クラウドサービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視

イ　利用するクラウドサービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測

ウ　クラウドサービス内における時刻同期の方法

エ　利用するクラウドサービスの不正利用の監視

（9）クラウドサービス上で要安定情報を取り扱う場合は、その可用性を考慮した設計となっていること。

（10）クラウドサービスにおいて、不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施を含む、情報セキュリティインシデントが発生した際の復旧に関する対策要件が策定されていること。

3　クラウドサービスを利用した情報システム

クラウドサービスを利用した情報システムについて、以下の措置を講ずること。

（1）導入・構築時の対策

ア　クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順について、以下の内容を全て含む実施手順を整備すること。

（ア）クラウドサービス利用のための責任分界点を意識した利用手順

（イ）クラウドサービス利用者が行う可能性がある重要操作の手順

イ　情報システムの運用・監視中に発生したクラウドサービスの利用に係る情報セキュリティインシデントを認知した際の対処手順について、以下の内容を全て含む実施手順を整備すること。

（ア）クラウドサービス提供者との責任分界点を意識した責任範囲の整理

（イ）クラウドサービスのサービスごとの情報セキュリティインシデント対処に関する事項

（ウ）クラウドサービスに係る情報セキュリティインシデント発生時の連絡体制

ウ　クラウドサービスが停止し、又は利用できなくなった際の復旧手順を実施手順として整

備すること。なお、要安定情報を取り扱う場合は十分な可用性を担保した手順とすること。

（2）運用・保守時の対策

ア　クラウドサービスの利用に関して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）クラウドサービス提供者に対する定期的なサービスの提供状態の確認

（イ）クラウドサービス上で利用するIT資産の適切な管理

イ　クラウドサービスで利用するアカウントの管理、アクセス制御、管理権限に関して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）管理者権限をクラウドサービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録

（イ）クラウドサービス利用者に割り当てたアクセス権限に対する定期的な確認による見直し

ウ　クラウドサービスで利用する機能に対する脆（ぜい）弱性対策を実施すること。

エ　クラウドサービスを運用する際の設定変更に関して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）クラウドサービスのリソース設定を変更するユーティリティプログラムを使用する場合の利用者の制限

（イ）クラウドサービスの設定を変更する場合の設定の誤りを防止するための対策

（ウ）クラウドサービス利用者が行う可能性のある重要操作に対する監督者の指導の下での実施

オ　クラウドサービスを運用する際の監視に関して、以下の内容を全て含む対策を実施すること。

（ア）クラウドサービスの不正利用の監視

（イ）クラウドサービスで利用しているデータ容量、性能等の監視

カ　クラウドサービスを運用する際の可用性に関して、以下の内容を全て含む情報セキュリティ対策を実施すること。

（ア）不測の事態に際してサービスの復旧を行うために必要なバックアップの確実な実施

（イ）要安定情報をクラウドサービスで取り扱う場合の十分な可用性の担保、復旧に係る定期的な訓練の実施

（ウ）クラウドサービス提供者からの仕様内容の変更通知に関する内容確認と復旧手順の確認

キ　クラウドサービスで利用する暗号鍵に関して、暗号鍵の生成から廃棄に至るまでのライフサイクルにおける適切な管理の実施を含む情報セキュリティ対策の実施

（3）更改・廃棄時の対策

ア　クラウドサービスの利用終了に際して、以下の内容を全て含む情報セキュリティ対策

を実施すること。

（ア）クラウドサービスで取り扱った情報の廃棄

（イ）暗号化消去が行えない場合の基盤となる物理機器の廃棄

（ウ）作成されたクラウドサービス利用者アカウントの削除

（エ）利用したクラウドサービスにおける管理者アカウントの削除又は返却

（オ）クラウドサービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

Ⅶ Web システム／Web アプリケーション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、Web システム／Web アプリケーションを開発、利用または運用等を行う場合、別紙１－２「Web システム／Web アプリケーションセキュリティ要件書 Ver.4.0」の各項目について、対応可、対応不可あるいは対象外等の対応方針を記載した資料を提出すること。

Ⅷ 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、以下の措置を講ずること。

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）

Ⅸ 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専属的な合意管轄裁判所は、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。

Ⅹ 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、Ⅲの1及びⅣ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。

Ⅺ 資料等の提出

上記Ⅱの1、Ⅱの2、Ⅲの1、Ⅳの1、Ⅴの6、Ⅴの7、Ⅴの8、Ⅵの1（5）、Ⅵの1（6）、Ⅵの1（8）、Ⅷの1及びⅧ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、総合評価落札方式及び企画競争方式にあっては提案書等の評価のための書類に添付して提出すること。

Ⅻ 変更手続

受託者は、上記Ⅱ、Ⅲ、Ⅳ、Ⅴ、Ⅵ、Ⅶ、Ⅷ及びⅩ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。

【別紙1－2】

項目		見出し		要件		備考	必須可否
1	認証・認可	1.1	ユーザー認証	1.1.1	特定のユーザーや管理者のみに表示・実行を許可すべき画面や機能、APIでは、ユーザー認証を実施すること	特定のユーザーや管理者のみにアクセスを許可したいWebシステムでは、ユーザー認証を行う必要があります。また、ユーザー認証が成功した後にはアクセス権限を確認する必要があります。そのため、認証済みユーザーのみがアクセス可能な箇所を明示しておくことが望ましいでしょう。 リスクベース認証や二要素認証など認証をより強固にする仕組みもあります。不特定多数がアクセスする必要がない場合には、IPアドレスなどによるアクセス制限も効果があります。 OpenIDなどIdP(ID Provider)を利用する場合には信頼できるプロバイダであるかを確認する必要があります。IdPを使った認証・認可を行う場合も他の認証・認可に関する要件を満たすものを利用することが望ましいです。	必須
				1.1.2	上記画面や機能に含まれる画像やファイルなどの個別のコンテンツ（非公開にすべきデータは直接URLで指定できる公開ディレクトリに配置しない）では、ユーザー認証を実施すること		必須
				1.1.3	多要素認証を実施すること	多要素認証（Multi Factor Authentication: MFA）とは、例えばパスワードによる認証に加え、TOTP（Time-Based One-Time Password：時間ベースのワンタイムパスワード）やデジタル証明書など二つ以上の要素を利用した認証方式です。手法については NIST Special Publication 800-63B などを参照してください。	推奨
		1.2	ユーザーの再認証	1.2.1	個人情報や機微情報を表示するページに遷移する際には、再認証を実施すること	ユーザー認証はセッションにおいて最初の一度だけ実施するのではなく、重要な情報や機能へアクセスする際には再認証を行うことが望ましいでしょう。	推奨
				1.2.2	パスワード変更や決済処理などの重要な機能を実行する際には、再認証を実施すること		推奨
		1.3	パスワード	1.3.1	ユーザー自身が設定するパスワード文字列は最低 8文字以上であること	認証を必要とするWebシステムの多くは、パスワードを本人確認の手段として認証処理を行います。そのためパスワードを盗聴や盗難などから守ることが重要になります。	必須
				1.3.2	登録可能なパスワード文字列の最大文字数は64文字以上であること	パスワードを処理する関数の中には最大文字数が少ないものもあるので注意する必要があります。	必須
				1.3.3	パスワード文字列として使用可能な文字種は制限しないこと	任意の大小英字、数字、記号、空白、Unicode文字など任意の文字が利用可能である必要があります。	必須
				1.3.4	パスワード文字列の入力フォームはinput type="password"で指定すること	基本的にinputタグのtype属性には「password」を指定しますが、パスワードを一時的に表示する可視化機能を実装する場合にはこの限りではありません。	必須
				1.3.5	ユーザーが入力したパスワード文字列を次画面以降で表示しないこと（hiddenフィールドなどのHTMLソース内やメールも含む）		必須

項目	見出し		要件		備考	必須可否
			1.3.6	パスワードを保存する際には、平文で保存せず、Webアプリケーションフレームワークなどが提供するハッシュ化とsaltを使用して保存する関数を使用すること	関数が存在しない場合にはパスワードは「パスワード文字列＋salt（ユーザー毎に異なるランダムな文字列）」をハッシュ化したものとsaltのみを保存する必要があります。（saltは20文字以上であることが望ましい） パスワード文字列のハッシュ化をさらに安全にする手法としてストレッチングがあります。	必須
			1.3.7	ユーザー自身がパスワードを変更できる機能を用意すること		必須
			1.3.8	パスワードはユーザー自身に設定させること システムが仮パスワードを発行する場合はランダムな文字列を設定し、安全な経路でユーザーに通知すること		推奨
			1.3.9	パスワードの入力欄でペースト機能を禁止しないこと	長いパスワードをユーザーが利用出来るようにするためにペースト機能を禁止しないようにする必要があります。	推奨
			1.3.10	パスワード強度チェッカーを実装すること	使用する文字種や文字数を確認し、ユーザー自身にパスワードの強度を示せるようにします。またユーザーIDと同じ文字列や漏洩したパスワードなどのリストとの突合を行う必要があります。手法については NIST Special Publication 800-63B などを参照してください。	推奨
	1.4	アカウントロック機能について	1.4.1	認証時に無効なパスワードで10回試行があった場合、最低30分間はユーザーがロックアウトされた状態にすること	パスワードに対する総当たり攻撃や辞書攻撃などから守るためには、試行速度を遅らせるアカウントロック機能の実装が有効な手段になります。アカウントロックの試行回数、ロックアウト時間については、サービスの内容に応じて調整することが必要になります。	必須
			1.4.2	ロックアウトは自動解除を基本とし、手動での解除は管理者のみ実施可能とすること		推奨
	1.5	パスワードリセット機能について	1.5.1	パスワードリセットを実行する際にはユーザー本人しか受け取れない連絡先（あらかじめ登録しているメールアドレス、電話番号など）にワンタイムトークンを含むURLなどの再設定方法を通知すること	連絡先については、事前に受け取り確認をしておくことでより安全性を高めることができます。 使用されたワンタイムトークンは破棄し、有効期限を12時間以内とし必要最低限に設定してください。	必須
			1.5.2	パスワードはユーザー自身に再設定させること		必須
	1.6	アクセス制御について	1.6.1	Web ページや機能、データをアクセス制御（認可制御）する際には認証情報・状態を元に権限があるかどうかを判別すること	認証により何らかの制限を行う場合には、利用しようとしている情報や機能へのアクセス（読み込み・書き込み・実行など）権限を確認することでアクセス制御を行うことが必要になります。 画像やファイルなどのコンテンツ、APIなどの機能に対しても、全て個別にアクセス権限を設定、確認する必要があります。 これらはアクセス権限の一覧表に基づいて行います。 CDNなどを利用してコンテンツを配置するなどアクセス制御を行うことが困難な場合、予測が困難なURLを利用することでアクセスされにくくする方法もあります。	必須

項目		見出し		要件		備考	必須可否
				1.6.2	公開ディレクトリには公開を前提としたファイルのみ配置すること	公開ディレクトリに配置したファイルは、URLを直接指定することでアクセスされる可能性があります。そのため、機微情報や設定ファイルなどの公開する必要がないファイルは、公開ディレクトリ以外に配置する必要があります。	必須
		1.7	アカウントの無効化機能について	1.7.1	管理者がアカウントの有効・無効を設定できること	不正にアカウントを利用されていた場合に、アカウントを無効化することで被害を軽減することができます。	推奨
2	セッション管理	2.1	セッションの破棄について	2.1.1	認証済みのセッションが一定時間以上アイドル状態にあるときはセッションタイムアウトとし、サーバー側のセッションを破棄しログアウトすること	認証を必要とするWebシステムの多くは、認証状態の管理にセッションIDを使ったセッション管理を行います。認証済みの状態にあるセッションを不正に利用されないためには、使われなくなったセッションを破棄する必要があります。セッションタイムアウトの時間については、サービスの内容やユーザー利便性に応じて設定することが必要になります。また、NIST Special Publication 800-63B などを参照してください。	必須
				2.1.2	ログアウト機能を用意し、ログアウト実行時にはサーバー側のセッションを破棄すること	ログアウト機能の実行後にその成否をユーザーが確認できることが望ましい。	必須
		2.2	セッションIDについて	2.2.1	Webアプリケーションフレームワークなどが提供するセッション管理機能を使用すること	セッションIDを用いて認証状態を管理する場合、セッションIDの盗聴や推測、攻撃者が指定したセッションIDを使用させられる攻撃などから守る必要があります。 また、セッションIDは原則としてcookieにのみ格納すべきです。	必須
				2.2.2	セッションIDは認証成功後に発行すること 認証前にセッションIDを発行する場合は、認証成功直後に新たなセッションIDを発行すること		必須
				2.2.3	ログイン前に機微情報をセッションに格納する時点でセッションIDを発行または再生成すること		必須
				2.2.4	認証済みユーザーの特定はセッションに格納した情報を元に行うこと		必須
		2.3	CSRF（クロスサイトリクエストフォージェリー）対策の実施について	2.3.1	ユーザーにとって重要な処理を行う箇所では、ユーザー本人の意図したリクエストであることを確認できるようにすること	正規ユーザー以外の意図により操作されては困る処理を行う箇所では、フォーム生成の際に他者が推測困難なランダムな値（トークン）をhiddenフィールドやcookie以外のヘッダーフィールド（X-CSRF-TOKENなど）に埋め込み、リクエストをPOSTメソッドで送信します。フォームデータを処理する際にトークンが正しいことを確認することで、正規ユーザーの意図したリクエストであることを確認することができます。 また、別の方法としてパスワード再入力による再認証を求める方法もあります。 cookieのSameSite属性を適切に使うことによって、CSRFのリスクを低減する効果があります。SameSite属性は一部の状況においては効果がないこともあるため、トークンによる確認が推奨されます。	必須
3	入力処理	3.1	パラメーターについて	3.1.1	URLにユーザーID やパスワードなどの機微情報を格納しないこと	URLは、リファラー情報などにより外部に漏えいする可能性があります。そのため URLには秘密にすべき情報は格納しないようにする必要があります。	必須

項目		見出し		要件		備考	必須可否
				3.1.2	パラメーター（クエリーストリング、エンティティボディ、cookieなどクライアントから受け渡される値）にパス名を含めないこと	ファイル操作を行う機能などにおいて、URL パラメーターやフォームで指定した値でパス名を指定できるようにした場合、想定していないファイルにアクセスされてしまうなどの不正な操作を実行されてし まう可能性があります。	必須
				3.1.3	パラメーター要件に基づいて、入力値の文字種や文字列長の検証を行うこと	各パラメーターは、機能要件に基づいて文字種・文字列長・形式を定義する必要があります。入力値に想定している文字種や文字列長以外の値の入力を許してしまう場合、不正な操作を実行されてしまう可能性があります。サーバー側でパラメーターを受け取る場合、クライアント側での入力値検証の有無に関わらず、入力値の検証はサーバー側で実施する必要があります。	必須
		3.2	ファイルアップロードについて	3.2.1	入力値としてファイルを受け付ける場合には、拡張子やファイルフォーマットなどの検証を行うこと	ファイルのアップロード機能を利用した不正な実行を防ぐ必要があります。画像ファイルを扱う場合には、ヘッダー領域を不正に加工したファイルにも注意が必要です。	必須
				3.2.2	アップロード可能なファイルサイズを制限すること	圧縮ファイルを展開する場合には、解凍後のファイルサイズや、ファイルパスやシンボリックリンクを含む場合のファイルの上書きにも注意が必要です。	必須
		3.3	XMLを使用する際の処理について	3.3.1	XMLを読み込む際は、外部参照を無効にすること	手法についてはXML External Entity Prevention Cheat Sheetなどを参照してください。 https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html	必須
		3.4	デシリアライズについて	3.4.1	信頼できないデータ供給元からのシリアライズされたオブジェクトを受け入れないこと	デシリアライズする場合は、シリアライズしたオブジェクトにデジタル署名などを付与し、信頼できる供給元が発行したデータであるかを検証してください。	必須
		3.5	外部リソースへのリクエスト送信について	3.5.1	他システムに接続や通信を行う場合は、外部からの入力によって接続先を動的に決定しないこと	外部から不正なURLやIPアドレスなどが挿入されると、SSRF(Server-Side Request Forgery)の脆弱性になる可能性があります。外部からの入力によって接続先を指定せざるを得ない場合は、ホワイトリストを基に入力値の検証を実施するとともに、アプリケーションレイヤーだけではなくネットワークレイヤーでのアクセス制御も併用する必要があります。	推奨
4	出力処理	4.1	HTMLを生成する際の処理について	4.1.1	HTMLとして特殊な意味を持つ文字（< > " ' &）を文字参照によりエスケープすること	外部からの入力により不正なHTMLタグなどが挿入されてしまう可能性があります。「<」→「<」や「&」→「&」、「"」→「"」のようにエスケープを行う必要があります。スクリプトによりクライアント側でHTMLを生成する場合も、同等の処理が必要です。実装の際にはこれらを自動的に実行するフレームワークやライブラリを使用することが望ましいでしょう。また、その他にもスクリプトの埋め込みの原因となるものを作らないようにする必要があります。 XMLを生成する場合も同様にエスケープが必要です。	必須
				4.1.2	外部から入力したURLを出力するときは「http://」または「https://」で始まるもののみを許可すること		必須

項目	見出し		要件		備考	必須可否
			4.1.3	<script>...</script>要素の内容やイベントハンドラ（onmouseover=""など）を動的に生成しないようにすること	<script>...</script>要素の内容やイベントハンドラは原則として動的に生成しないようにすべきですが、jQueryなどのAjaxライブラリを使用する際はその限りではありません。ライブラリについては、アップデート状況などを調べて信頼できるものを選択するようにしましょう。	必須
			4.1.4	任意のスタイルシートを外部サイトから取り込めないようにすること		必須
			4.1.5	HTMLタグの属性値を「"」で囲うこと	HTMLタグ中のname="value"で記される値(value)にユーザーの入力値を使う場合、「"」で囲わない場合、不正な属性値を追加されてしまう可能性があります。	必須
			4.1.6	CSSを動的に生成しないこと	外部からの入力により不正なCSSが挿入されると、ブラウザに表示される画面が変更されたり、スクリプトが埋め込まれる可能性があります。	必須
	4.2	JSONを生成する際の処理について	4.2.1	文字列連結でJSON文字列を生成せず、適切なライブラリを用いてオブジェクトをJSONに変換すること	適切なライブラリがない場合は、JSONとして特殊な意味を持つ文字（ " ￥ , : { } [ ] ）をUnicodeエスケープする必要があります。	必須
	4.3	HTTPレスポンスヘッダーについて	4.3.1	HTTPレスポンスヘッダーのContent-Typeを適切に指定すること	一部のブラウザではコンテンツの文字コードやメディアタイプを誤認識させることで不正な操作が行える可能性があります。これを防ぐためには、HTTPレスポンスヘッダーを「Content-Type: text/html; charset=utf-8」のように、コンテンツの内容に応じたメディアタイプと文字コードを指定する必要があります。	必須
			4.3.2	HTTPレスポンスヘッダーフィールドの生成時に改行コードが入らないようにすること	HTTPヘッダーフィールドの生成時にユーザーが指定した値を挿入できる場合、改行コードを入力することで不正なHTTPヘッダーやコンテンツを挿入されてしまう可能性があります。これを防ぐためには、HTTPヘッダーフィールドを生成する専用のライブラリなどを使うようにすることが望ましいでしょう。	必須
	4.4	その他の出力処理について	4.4.1	SQL文を組み立てる際に静的プレースホルダを使用すること	SQL文の組み立て時に不正なSQL文を挿入されることで、SQLインジェクションを実行されてしまう可能性があります。これを防ぐためにはSQL文を動的に生成せず、プレースホルダを使用してSQL文を組み立てるようにする必要があります。 静的プレースホルダとは、JIS/ISOの規格で「準備された文(Prepared Statement)」と規定されているものです。	必須
			4.4.2	プログラム上でOSコマンドやアプリケーションなどのコマンド、シェル、eval()などによるコマンドの実行を呼び出して使用しないこと	コマンド実行時にユーザーが指定した値を挿入できる場合、外部から任意のコマンドを実行されてしまう可能性があります。コマンドを呼び出して使用しないことが望ましいでしょう。	必須
			4.4.3	リダイレクタを使用する場合には特定のURLのみに遷移できるようにすること	リダイレクタのパラメーターに任意のURLを指定できる場合（オープンリダイレクタ）、攻撃者が指定した悪意のあるURLなどに遷移させられる可能性があります。	必須
			4.4.4	メールヘッダーフィールドの生成時に改行コードが入らないようにすること	メールの送信処理にユーザーが指定した値を挿入できる場合、不正なコマンドなどを挿入されてしまう可能性があります。これを防ぐためには、不正な改行コードを使用できないメール送信専用のライブラリなどを使うようにすることが望ましいでしょう。	必須

項目		見出し		要件		備考	必須可否
				4.4.5	サーバ側のテンプレートエンジンを使用する際に、テンプレートの変更や作成に外部から受け渡される値を使用しないこと	サーバ側のテンプレートエンジンを使用してテンプレートを組み立てる際に不正なテンプレートの構文を挿入されることで、任意のコードを実行される可能性があります。 外部から渡される値をテンプレートの組み立てに使用せず、レンダリングを行う際のデータとして使用する必要があります。 また、レンダリング時にはクロスサイトスクリプティングの脆弱性が存在しないか確認してください。	必須
5	HTTPS	5.1	HTTPSについて	5.1.1	Webサイトを全てHTTPSで保護すること	適切にHTTPSを使うことで通信の盗聴・改ざん・なりすましから情報を守ることができます。次のような重要な情報を扱う画面や機能ではHTTPSで通信を行う必要があります。 ・入力フォームのある画面 ・入力フォームデータの送信先 ・重要情報が記載されている画面 ・セッションIDを送受信する画面 HTTPSの画面内で読み込む画像やスクリプトなどのコンテンツについてもHTTPSで保護する必要があります。	必須
				5.1.2	サーバー証明書はアクセス時に警告が出ないものを使用すること	HTTPSで提供されているWebサイトにアクセスした場合、Webブラウザから何らかの警告がでるということは、適切にHTTPSが運用されておらず盗聴・改ざん・なりすましから守られていません。適切なサーバー証明書を使用する必要があります。	必須
				5.1.3	TLS1.2以上のみを使用すること	SSL2.0／3.0、TLS1.0／1.1には脆弱性があるため、無効化する必要があります。使用する暗号スイートは、7.2.1を参照してください。	必須
				5.1.4	レスポンスヘッダーにStrict-Transport-Securityを指定すること	Hypertext Strict Transport Security(HSTS)を指定すると、ブラウザがHTTPSでアクセスするよう強制できます。	必須
6	cookie	6.1	cookieの属性について	6.1.1	Secure属性を付けること	Secure属性を付けることで、http://でのアクセスの際にはcookieを送出しないようにできます。特に認証状態に紐付けられたセッションIDを格納する場合には、Secure属性を付けることが必要です。	必須
				6.1.2	HttpOnly属性を付けること	HttpOnly属性を付けることで、クライアント側のスクリプトからcookieへのアクセスを制限することができます。	必須
				6.1.3	Domain属性を指定しないこと	セッションフィクセイションなどの攻撃に悪用されることがあるため、Domain属性は特に必要がない限り指定しないことが望ましいでしょう。	推奨
7	その他	7.1	エラーメッセージについて	7.1.1	エラーメッセージに詳細な内容を表示しないこと	ミドルウェアやデータベースのシステムが出力するエラーには、攻撃のヒントになる情報が含まれているため、エラーメッセージの詳細な内容はエラーログなどに出力するべきです。	必須

項目	見出し		要件		備考	必須可否
	7.2	暗号アルゴリズムについて	7.2.1	ハッシュ関数、暗号アルゴリズムは『電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）』に記載のものを使用すること	広く使われているハッシュ関数、疑似乱数生成系、暗号アルゴリズムの中には安全でないものもあります。安全なものを使用するためには、『電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）』や『TLS暗号設定ガイドライン』に記載されたものを使用する必要があります。	必須
	7.3	乱数について	7.3.1	鍵や秘密情報などに使用する乱数的性質を持つ値を必要とする場合には、暗号学的な強度を持った疑似乱数生成系を使用すること	鍵や秘密情報に予測可能な乱数を用いると、過去に生成した乱数値から生成する乱数値が予測される可能性があるため、ハッシュ関数などを用いて生成された暗号学的な強度を持った疑似乱数生成系を使用する必要があります。	必須
	7.4	基盤ソフトウェアについて	7.4.1	基盤ソフトウェアはアプリケーションの稼働年限以上のものを選定すること	脆弱性が発見された場合、修正プログラムを適用しないと悪用される可能性があります。そのため、言語やミドルウェア、ソフトウェアの部品などの基盤ソフトウェアは稼働期間またはサポート期間がアプリケーションの稼働期間以上のものを利用する必要があります。もしアプリケーションの稼働期間中に基盤ソフトウェアの保守期間が終了した場合、危険な脆弱性が残されたままになる可能性があります。	必須
			7.4.2	既知の脆弱性のないOSやミドルウェア、ライブラリやフレームワーク、パッケージなどのコンポーネントを使用すること	利用コンポーネントにOSSが含まれる場合は、SCA（ソフトウェアコンポジション解析）ツールを導入し、依存関係を包括的かつ正確に把握して対策が行えることが望ましいでしょう。	必須
	7.5	ログの記録について	7.5.1	重要な処理が行われたらログを記録すること	ログは、情報漏えいや不正アクセスなどが発生した際の検知や調査に役立つ可能性があります。認証やアカウント情報の変更などの重要な処理が実行された場合には、その処理の内容やクライアントのIPアドレスなどをログとして記録することが望ましいでしょう。ログに機微情報が含まれる場合にはログ自体の取り扱いにも注意が必要になります。	必須
	7.6	ユーザーへの通知について	7.6.1	重要な処理が行われたらユーザーに通知すること	重要な処理（パスワードの変更など、ユーザーにとって重要で取り消しが困難な処理）が行われたことをユーザーに通知することによって異常を早期に発見できる可能性があります。	推奨
	7.7	Access-Control-Allow-Originヘッダーについて	7.7.1	Access-Control-Allow-Originヘッダーを指定する場合は、動的に生成せず固定値を使用すること	クロスオリジンでXMLHttpRequest (XHR)を使う場合のみこのヘッダーが必要です。不要な場合は指定する必要はありませんし、指定する場合も特定のオリジンのみを指定する事が望ましいです。	必須
	7.8	クリックジャッキング対策について	7.8.1	レスポンスヘッダーにX-Frame-OptionsとContent-Security-Policyヘッダーのframe-ancestors ディレクティブを指定すること	クリックジャッキング攻撃に悪用されることがあるため、X-Frame-Optionsヘッダーフィールドに DENYまたはSAMEORIGINを指定する必要があります。 Content-Security-Policyヘッダーフィールドに frame-ancestors 'none' または 'self' を指定する必要があります。 X-Frame-Options ヘッダーは主要ブラウザーでサポートされていますが標準化されていません。CSP レベル 2 仕様で frame-ancestors ディレクティブが策定され、X-Frame-Options は非推奨とされました。	必須

項目		見出し		要件		備考	必須可否
		7.9	キャッシュ制御について	7.9.1	個人情報や機微情報を表示するページがキャッシュされないよう Cache-Control: no-store を指定すること	個人情報や機密情報が含まれたページはCDNやロードバランサー、ブラウザなどのキャッシュに残ってしまうことで、権限のないユーザーが閲覧してしまう可能性があるためキャッシュ制御を適切に行う必要があります。	必須
		7.10	ブラウザのセキュリティ設定について	7.10.1	ユーザーに対して、ブラウザのセキュリティ設定の変更をさせるような指示をしないこと	ユーザーのWebブラウザのセキュリティ設定などを変更した場合や、認証局の証明書をインストールさせる操作は、他のサイトにも影響します。	必須
		7.11	ブラウザのセキュリティ警告について	7.11.1	ユーザーに対して、ブラウザの出すセキュリティ警告を無視させるような指示をしないこと	ブラウザの出す警告を通常利用においても無視させるよう指示をしていると、悪意のあるサイトで同様の指示をされた場合もそのような操作をしてしまう可能性が高まります。	必須
		7.12	WebSocketについて	7.12.1	Originヘッダーの値が正しいリクエスト送信元であることが確認できた場合にのみ処理を実施すること	WebSocketにはSOP (Same Origin Policy)という仕組みが存在しないため、Cross-Site WebSocket Hijacking(CSWSH)対策のためにOriginヘッダーを確認する必要があります。	必須
		7.13	HTMLについて	7.13.1	html開始タグの前に<!DOCTYPE html>を宣言すること	DOCTYPEで文書タイプをHTMLと明示的に宣言することでCSSなど別フォーマットとして解釈されることを防ぎます。	必須
				7.13.2	CSSファイルやJavaScriptファイルをlinkタグで指定する場合は、絶対パスを使用すること	linkタグを使用してCSSファイルやJavaScriptファイルを相対パス指定した場合にRPO (Relative Path Overwrite) が起きる可能性があります。	必須
8	提出物	8.1	提出物について	8.1.1	サイトマップを用意すること	認証や再認証、CSRF対策が必要な箇所、アクセス制御が必要なデータを明確にするためには、Webサイト全体の構成を把握し、扱うデータを把握する必要があります。そのためには上記の資料を用意することが望ましいでしょう。	必須
				8.1.2	画面遷移図を用意すること		必須
				8.1.3	アクセス権限一覧表を用意すること	誰にどの機能の利用を許可するかまとめた一覧表を作成することが望ましいでしょう。	必須
				8.1.4	コンポーネント一覧を用意すること	依存しているライブラリやフレームワーク、パッケージなどのコンポーネントに脆弱性が存在する場合がありますので、依存しているコンポーネントを把握しておく必要があります。	推奨
				8.1.5	上記のセキュリティ要件についてテストした結果報告書を用意すること	自社で脆弱性診断を実施する場合には「脆弱性診断士スキルマッププロジェクト」が公開している「Webアプリケーション脆弱性診断ガイドライン」などを参照してください。	推奨

別紙2

_ISMAP 基本言明要件の一覧

1. ガバナンス基準

ガバナンス基準	
3	情報セキュリティガバナンス
	情報セキュリティガバナンスは、組織の情報セキュリティ活動を指導し、管理するシステムである。情報セキュリティの目的及び戦略を、事業の目的及び戦略に合わせて調整する必要があり、法制度、規制及び契約を遵守する必要がある。また、情報セキュリティガバナンスは、内部統制の仕組みによって遂行されるリスクマネジメント手法を通じて、評価、分析及び実施する。
3.1	情報セキュリティガバナンスのプロセス
3.1.1 概要	
	経営陣は、情報セキュリティを統治するために、評価、指示、モニタ及びコミュニケーションの各プロセスを実行する。さらに、保証プロセスによって、情報セキュリティガバナンス及び達成したレベルについての独立した客観的な意見が得られる。
3.1.2　評価	
	評価とは、現在のプロセス及び予定している変更に基づくセキュリティ目的の現在及び予想される達成度を考慮し、将来の戦略的目的の達成を最適化するために必要な調整を決定するガバナンスプロセスである。
	“評価”プロセスを実施するために、経営陣は、次のことを行う。
3.1.2.1	経営陣は、事業の取組みにおいて情報セキュリティ問題を考慮することを確実にする。 ・経営陣は、管理者に、情報セキュリティが事業目的を十分にサポートし、支えることを確実にさせる。
3.1.2.2	経営陣は、情報セキュリティのパフォーマンス結果に対応し、必要な処置の優先順位を決めて開始する。
3.1.2.3	経営陣は、管理者に、重大な影響のある新規情報セキュリティプロジェクトを経営陣に付託するようにさせる。
3.1.3　指示	
	指示は、経営陣が、実施する必要がある情報セキュリティの目的及び戦略についての指示を与えるガバナンスプロセスである。指示には、資源供給レベルの変更、資源の配分、活動の優先順位付け並びに、方針、適切なリスク受容及びリスクマネジメント計画の承認が含まれる。
	“指示”プロセスを実施するために、経営陣は次のことを行う。
3.1.3.1	経営陣は、その組織のリスク選好を決定する。
3.1.3.2	経営陣は、情報セキュリティの戦略及び方針を承認する。 (ア)経営陣は、管理者に、情報セキュリティの戦略及び方針を策定・実施させる。 (イ)経営陣は、管理者に、情報セキュリティの目的を事業目的に合わせて調整させる。
3.1.3.3	経営陣は、適切な投資及び資源を配分する。
3.1.3.4	経営陣は、管理者に、情報セキュリティに積極的な文化を推進させる。
3.1.4　モニタ	
	モニタは、経営陣が戦略的目的の達成を評価することを可能にするガバナンスプロセスである。
	“モニタ”プロセスを実施するために、経営陣は次のことを行う。
3.1.4.1	経営陣は、情報セキュリティマネジメント活動の有効性を評価する。 (ア)経営陣は、管理者に、事業の観点から適切なパフォーマンス指標を選択させる。 (イ)経営陣は、管理者に、経営陣が以前に特定した措置の実施及びそれらの組織への影響を含む、情報セキュリティのパフォーマンス成果についてのフィードバックを経営陣へ提供させる。
3.1.4.2	経営陣は、内部及び外部の要求事項への適合性を確実にする。

ガバナンス基準	
3.1.4.3	経営陣は、変化する事業、法制度、規制の環境、及びそれらの情報リスクへの潜在的影響を考慮する。
3.1.4.4	経営陣は、管理者に、情報リスク及び情報セキュリティに影響する新規開発案件について、経営陣に対し注意を喚起させる。
3.1.5　コミュニケーション	
	コミュニケーションは、経営陣及び利害関係者が、双方の特定のニーズに沿った情報セキュリティに関する情報を交換する双方向のガバナンスプロセスである。
	コミュニケーションの方法の一つは、情報セキュリティの活動及び課題を利害関係者に説明する情報セキュリティ報告書である。
	“コミュニケーション”プロセスを実施するために、経営陣は次のことを行う。
3.1.5.1	経営陣は、外部の利害関係者に、組織がその事業特性に見合った情報セキュリティのレベルを実践していることを報告する。
3.1.5.2	経営陣は、管理者に、情報セキュリティ課題を特定した外部レビューの結果を通知し、是正処置を要請する。
3.1.5.3	経営陣は、情報セキュリティに関する規制上の義務、利害関係者の期待及び事業ニーズを認識する。
3.1.5.4	経営陣は、管理者に、注意が必要な問題、また、できれば決定が必要な問題について、経営陣へ助言させる。
3.1.5.5	経営陣は、管理者に、関連する利害関係者に対し、経営陣の方向性及び決定を支援するためにとるべき詳細な行動を、経営陣の方向性及び決定に沿って説明させる。
3.1.6　保証	
	保証は、経営陣が独立した客観的な監査、レビュー又は認証を委託するガバナンスプロセスである。これは、望ましいレベルの情報セキュリティを達成するためのガバナンス活動の実行及び運営の遂行に関連した目的及び処置を特定し、妥当性を検証する。
	“保証”プロセスを実施するために、経営陣は次のことを行う。
3.1.6.1	経営陣は、要求している情報セキュリティ水準に対し、どのように説明責任を果たしているかについて、独立した客観的な意見を監査人等に求める。
3.1.6.2	経営陣は、管理者に、経営陣が委託する監査、レビュー又は認証をサポートさせる。

2. マネジメント基準

マネジメント基準	
4.1	マネジメント基準
	マネジメント基準は、JIS Q 27001:2014 を基に、情報セキュリティについて組織を指揮統制するために調整された活動である情報セキュリティマネジメントを確立、導入、運用、監視、維持及び改善するための基準を定める。マネジメント基準は、原則としてすべて実施しなければならないものである。
4.2	記載内容について
	「情報セキュリティ管理基準」の「マネジメント基準」に同じ。 クラウドサービスにおいては、クラウドサービス利用者の環境等を考慮して、クラウドサービス提供者の管理策等を検討し、実施する必要がある。そのため、クラウドサービス利用者及びクラウドサービス事業者間において、クラウドサービスにおける情報セキュリティリスクとその対応について、情報交換することが非常で重要である。 当該情報セキュリティリスクコミュニケ―ションについては、クラウドサービスにおいて特に考慮するべき事項として、4.9 章に規定する。
4.3	凡例
	4.4 章以降は、以下の構成をとる。 4.4　情報セキュリティマネジメント確立　［27001-4］ 4.4.1　組織の役割、責任及び権限［27001-5.3 / 5.1］ 4.4.1.1　トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。［27001-5.1b) / 5.1e) / 5.1f)］ その際は、以下を行うこととする。 ・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する ： ［27001-X.X.X］は、JIS Q 27001:2014 において関連する条項(X.X.X)を示す。

マネジメント基準	
4.4	情報セキュリティマネジメントの確立［27001-4.4］
	情報セキュリティマネジメントを確立するために、その基盤となる適用範囲を決定し、方針を確立する。これらをもとに、情報セキュリティリスクアセスメントを実施し、その対応を計画し実施する。それにより、組織が有効な情報セキュリティマネジメントを実施するための基盤作りを行う。
4.4.1	組織の役割、責任及び権限［27001-5.3 / 5.1］
4.4.1.1	トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。［27001-5.1b) / 5.1e) / 5.1f)］ ・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する。 ・情報セキュリティマネジメントがその意図した成果を達成することを確実にする。 ・情報セキュリティマネジメントの有効性に寄与するよう人々を指揮し、支援する。 また、トップマネジメントがリーダーシップ及びコミットメントを発揮していることを以下により確認する。 ・経営会議等の議事録に、トップマネジメントの情報セキュリティマネジメントに関する意思、判断、指示等が記録されていること。 ・情報セキュリティ方針、情報セキュリティ目的及びそれを達成する計画を策定する際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・達成すべきセキュリティの水準として、リスクレベルをトップマネジメントが決定していること。 ・リスクレベルに応じて選択したセキュリティ管理策を実施させる際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・内部監査において確認すべき事項に、トップマネジメントが要求する情報セキュリティ要求事項等が含まれていること。 ・内部監査報告書やそれらに基づく是正処置、マネジメントビュー議事録等に、トップマネジメントの意思、判断、指示等が含まれていること。
4.4.1.2	トップマネジメントは、組織の役割について、以下の責任及び権限を割り当て、伝達する。［27001-5.3］ ・情報セキュリティマネジメントを、本管理基準の要求事項として適合させる。 ・情報セキュリティマネジメントのパフォーマンス評価をトップマネジメントに報告する。 また、情報セキュリティマネジメントを本管理基準の要求事項に適合させるために、以下のような責任・権限を割り当てていることを確認する。 ・セキュリティ要求事項を盛り込んだ情報セキュリティ方針等の文書を策定する責任・権限 ・リスクアセスメントにおいて、リスクを運用管理する責任・権限を持つリスク所有者 ・セキュリティ要求事項を満たす管理策を教育、普及させる責任・権限 ・セキュリティ要求事項を満たしているか監査する責任・権限 ・各プロセスの結果及び効果をトップマネジメントに報告する責任・権限 ・各プロセスの結果及び効果を組織内に周知する責任・権限
4.4.1.3	トップマネジメントは、管理層がその責任の領域においてリーダーシップを発揮できるよう、管理層の役割を支援する。［27001-5.1h)］ 管理層が、その職掌範囲、組織等において、リーダーシップを発揮できるよう、トップマネジメントは、管理層に、必要な権限を委譲していることを確認する。
4.4.2	組織及びその状況の理解［27001-4.1］
4.4.2.1	組織は、組織の目的に関連し、かつ、情報セキュリティマネジメントの意図した成果を達成する組織の能力に影響を与える、以下の課題を決定する。［27001-4.1］ ・外部の課題 ・内部の課題 これらの課題の決定とは、組織の外部状況及び内部状況の確定のことをいう。外部状況及び内部状況には、以下のようなものが含まれる。 a） 外部状況 ・国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 ・組織の目的に影響を与える主要な原動力及び傾向 ・外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観
	b） 内部状況 ・統治、組織体制、役割及びアカウンタビリティ ・方針、目的及びこれらを達成するために策定された戦略 ・資源及び知識として見た場合の能力(例えば、資本、時間、人員、プロセス、システム及び技術)

マネジメント基準	
	・情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） ・内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 ・組織文化 ・組織が採択した規格、指針及びモデル ・契約関係の形態及び範囲
4.4.3	利害関係者のニーズ及び期待の理解［27001-4.2］
4.4.3.1	組織は、利害関係者のニーズ及び期待を理解するために、以下を決定する。［27001-4.2］ ・情報セキュリティマネジメントに関連する利害関係者 ・利害関係者の、情報セキュリティに関連する要求事項 利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含めてもよいが、利害関係者には、以下のようなものが含まれる。 ・組織内で情報セキュリティマネジメントプロセスを推進する役割・権限を持つ人又は組織。例えば、以下のようなものをいう。 -情報セキュリティに関する方針等を策定する人又は組織（トップマネジメント等） -セキュリティ管理策を全組織に徹底させる人又は組織（総務部、情報システム部等） -情報セキュリティ監査を行う人又は組織（監査室等） -組織内の情報セキュリティ専門家 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・所属するセキュリティ団体、協会
4.4.4	適用範囲の決定［27001-4.3］
	情報セキュリティマネジメントを確立、導入、運用、監視、レビュー、維持及び改善するために、まず適用範囲を明確にし、組織に合った情報セキュリティマネジメントを構築する基盤を整える。
4.4.4.1	組織は、情報セキュリティマネジメントの境界及び適用可能性を明確にし、適用範囲を決定する。［27001-4.3］ a）組織は以下の点を考慮して適用範囲及び境界を定義する。 ・自らの事業 ・体制 ・所在地 ・資産 ・技術の特徴 ・外部及び内部の課題 ・利害関係者の情報セキュリティに関連する要求事項 ・組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係 b）情報セキュリティマネジメントの目的や目標は、組織の特徴によって異なる。
	c）情報セキュリティマネジメントに対する要求事項はそれぞれの組織の事業によって、外部状況、内部状況の双方があり、これらを考慮して適用範囲を定義する。 ・外部状況には、以下のようなものが含まれる。 －国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 －組織の目的に影響を与える主要な原動力及び傾向 －外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 ・内部状況には、以下のようなものが含まれる。 －統治、組織体制、役割及びアカウンタビリティ －方針、目的及びこれらを達成するために策定された戦略

マネジメント基準	
	－資源及び知識として見た場合の能力(例えば、資本、時間、人員、プロセス、システム及び技術) －情報システム、情報の流れ及び意思決定プロセス(公式及び非公式の双方を含む。) －内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 －組織文化 －組織が採択した規格、指針及びモデル －契約関係の形態及び範囲
4.4.5	方針の確立［27001-5.2 / 6.2 / 5.1］
4.4.5.1	トップマネジメントは、以下を満たす組織の情報セキュリティ方針を確立する。［27001-5.2］ ・組織の目的に対して適切であること。 ・情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組 ・情報セキュリティに関連して適用する要求事項を満たすことへのコミットメントを含むこと。 ・情報セキュリティマネジメントの継続的改善へのコミットメントを含むこと。 また、情報セキュリティ方針は情報セキュリティマネジメントにおける判断の基盤となる考え方を記載したものであり、組織の戦略に従って慎重に作成する。
4.4.5.2	組織は、情報セキュリティ目的及びそれを達成するための計画を策定する。［27001-6.2］ a）情報セキュリティ目的は、以下を満たすこととする。 ・情報セキュリティ方針と整合していること。 ・(実行可能な場合)測定可能であること。 ・適用される情報セキュリティ要求事項、並びにリスクアセスメント及びリスク対応の結果を考慮に入れること。 b）情報セキュリティ目的は、関係者に伝達し、必要に応じて更新するとともに、情報セキュリティ目的を達成するための計画においては、以下を決定する。 ・実施事項 ・必要な資源 ・責任者 ・達成期限 ・結果の評価方法
4.4.5.3	トップマネジメントは、以下によって、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。［27001-5.1a)］ ・情報セキュリティ方針及び情報セキュリティ目的を確立すること。 ・情報セキュリティ方針及び情報セキュリティ目的は組織の戦略的な方向性と相矛盾しないこと。 また、情報セキュリティ方針は組織に伝えられるように文書化され、しかるべき方法で利害関係者が入手できるようにするとともに、トップマネジメントが情報セキュリティ方針にコミットした証拠を、以下のような記録をもって示す。 ・文書化された情報セキュリティ方針への署名 ・情報セキュリティ方針が議論された会議の議事録 これらはトップマネジメントの責任を明確にするために実施する。
4.4.6	リスク及び機会に対処する活動［27001-6.1］
4.4.6.1	リスク及び機会を決定する。［27001-6.1.1］ a）組織は、外部及び内部の課題、利害関係者の情報セキュリティに関連する要求事項を考慮し、以下のために対処する必要があるリスク及び機会を決定する。 ・情報セキュリティマネジメントが、組織が意図した成果を達成する。 ・望ましくない影響を防止又は低減する。 ・継続的改善を達成する。 当該決定の際、組織は、以下を計画する。 ・決定したリスク及び機会に対処する活動 ・リスク及び機会に対処する活動の情報セキュリティマネジメントプロセスへの統合及び実施方法

マネジメント基準	
	・リスク及び機会に対処する活動の有効性の評価方法 b）リスク及び機会に対処する活動の記録として、具体的な対処計画（実施時期、実施内容、実施者、実施場所、実施に必要な資源などを規定した計画）を作成していることを確認するとともに、当該計画を作成する際、各対処計画が、情報セキュリティマネジメントプロセスの一部として実施されるよう、考慮するとともに、当該対処の有効性を評価する方法（実施状況や実施したことによる効果を評価する方法）を作成していることも確認する。
4.4.7	情報セキュリティリスクアセスメント［27001-6.1.2］
4.4.7.1	組織は、以下によって、情報セキュリティリスクアセスメントのプロセスを定め、適用する。［27001-6.1.2a）/ 6.1.2b）］ a）以下を含む情報セキュリティのリスク基準を確立し、維持する。 ・リスク受容基準 ・情報セキュリティリスクアセスメントを実施するための基準 b）リスク受容基準に、以下を反映するよう、考慮する。 ・組織の価値観 ・目的 ・資源
	c）リスク受容基準を策定する際には、以下の点を考慮する。 ・原因及び発生し得る結果の特質及び種類、並びにこれらの測定方法 ・発生頻度 ・発生頻度、結果を考える時間枠 ・リスクレベルの決定方法 ・利害関係者の見解 ・リスク基準は、法令及び規制の要求事項、並びに組織が合意するその他の要求事項によって、組織に課せられるもの又は策定されるものもあること。 d）情報セキュリティアセスメントを繰り返し実施した際に、以下の結果を生み出すこと。 ・情報セキュリティリスクアセスメントの結果に、一貫性及び妥当性があること。 ・情報セキュリティリスクアセスメントの結果が比較可能であること。 なお、情報セキュリティマネジメントにおけるリスクアセスメント手法には、定番といえるものがなく、それぞれの組織に適合したものを選択している場合が多いことから、必要に応じてツールを利用するなどが必要になる。
4.4.7.2	組織は、以下によって、情報セキュリティリスクを特定する。［27001-6.1.2c）］ a）情報セキュリティリスクアセスメントのプロセスを適用し、情報の機密性、完全性及び可用性の喪失に伴うリスクを特定する。 b）リスクを特定する過程において、リスク所有者を特定する。 c）リスクを特定する際には、以下について考慮する。 ・リスク源 が組織の管理下にあるか否かに関わらず、リスク源又はリスクの原因が明らかでないリスクも特定の対象にすること。 ・波及効果及び累積効果を含めた、特定の結果の連鎖を注意深く検討すること。 ・何が起こり得るのかの特定に加えて、考えられる原因及びどのような結果が引き起こされることがあるのかを示すシナリオ ・全ての重大な原因及び結果 ・以下を特定すること。 －リスク源 －影響を受ける領域、事象 －原因及び起こり得る結果 この段階で特定されなかったリスクは、今後の分析の対象から外されてしまうため、ある機会を追及しなかったことに伴うリスクも含め、リスクの包括的な一覧を作成する。
4.4.7.3	組織は、以下によって、情報セキュリティリスクを分析する。［27001-6.1.2d）］a）以下の手順によりリスク分析を行う。・特定されたリスクが実際に生じた場合に起こり得る結果の分析を行う。・特定されたリスクの発生頻度の分析を行う。・リスクレベルを決定する。・特定した脅威やぜい弱性を基に、以下の点を考慮する。－セキュリティインシデントが発生した場合の事業影響度－セキュリティインシデントの発生頻度－管理策が適用されている場合はその効果 b）リスク分析の際には、以下の点についても考慮する。・

マネジメント基準	
	リスクの原因及びリスク源・リスクの好ましい結果及び好ましくない結果・リスクの発生頻度・リスクの結果及び発生頻度に影響を与える要素　なお、リスク分析は、状況に応じて、定性的、半定量的、定量的、又はそれらを組み合わせた手法で行うことが可能である。
4.4.7.4	組織は、以下によって、情報セキュリティリスクを評価する。[27001-6.1.2e)] ・リスク分析の結果、決定されたリスクレベルとリスク基準との比較をする。 ・リスク対応のための優先順位付けを行う。 ・リスク評価の結果は今後の改善に利用するため保管する。 　なお、リスク対応の優先順位を決定する際には、より広い範囲の状況を考慮し、他者が負うリスクの受容レベルについて考慮するとともに、法令、規制、その他の要求事項についても考慮する。
4.4.8	情報セキュリティリスク対応［27001-6.1.3］
4.4.8.1	組織は、情報セキュリティアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。[27001-6.1.3a)] 情報セキュリティリスク対応の選択肢には、以下が含まれる。 ・リスクを生じさせる活動を開始又は継続しないと決定することによるリスクの回避 ・ある機会を目的としたリスクの引受け又はリスクの負担 ・リスク源の除去 ・発生頻度の変更 ・結果の変更 ・(契約及びリスクファイナンス　を含む)他者とのリスクの共有 ・情報に基づいた意思決定によるリスクの保有 　さらに、リスク対応の評価や改善に役立てるため、どの選択肢を選んだ場合も、その理由を明確にし、記載する。
4.4.8.2	組織は、選定した情報セキュリティリスク対応の実施に必要な全ての管理策を決定する。[27001-6.1.3b)] 　リスク対応のための方針を決めた上で、管理策の目的(管理目的)及び管理策について検討する。以下を考慮しつつ、対応による効果と対応に必要な費用及び労力のバランスを取り、適切な情報セキュリティ対応の選択肢を選定する。 ・リスクの受容可能レベル ・関連する法令 ・規制や契約上の要求事項 ・その他の社会的責任 　なお、具体的な管理策の選定においては、管理目的に対応した「管理策基準」から適切なものを選択するが、「管理策基準」はすべてを網羅しているわけではないので、組織の事業や業務などによってその他の管理策を追加してもよい　。
4.4.8.3	組織は、管理策が見落とされていないことを検証する。　[27001-6.1.3c)] 　必要な管理策の見落としがないか、管理策基準を参照するが、管理策基準に示す管理目的及び管理策以外の管理目的及び管理策が必要になった場合、他の管理目的及び管理策を追加することができる。
4.4.8.4	組織は、情報セキュリティリスク対応計画を策定する。[27001-6.1.3e)] a)情報セキュリティリスク対応計画には、以下を含む。 ・期待される効果を含む、対応選択肢選定の理由 ・情報セキュリティリスク対応計画の承認者及び対応計画の実施責任者 ・対応内容 ・必要な資源 ・費用・労力、制約 ・後日の報告、監視に必要な要求事項 ・対応工程における節目ごとの目標 ・対応時期及び日程

マネジメント基準	
	b）責任及び権限について 情報セキュリティマネジメントにおいては最終的な承認をトップマネジメントが行っていることがほとんどであり、責任がトップマネジメントに集中している。 一方で、情報セキュリティリスクアセスメント及びリスク対応については、責任及び権限を持つリスク所有者が、責任及び権限を持つ。 リスク所有者は、トップマネジメント、又はトップマネジメントから任命され、責任及び権限が委譲された者であることが多いことから、情報セキュリティマネジメントにおいて、トップマネジメント及びリスク所有者が、どのような責任を持つかについて明確にする。
4.4.8.5	組織は、リスク所有者から、情報セキュリティリスク対応計画について承認を得、かつ、リスク所有者に、残留している情報セキュリティリスクを受け入れてもらう。［27001-6.1.3f)］ すべてのリスクについて管理目的や管理策を選択した時点で、残留リスクについて明確にし、今後の対応計画を作成する。計画の作成においては以下の点について考慮する。 ・技術的に対応可能になる時期 ・コスト的に対応可能になる時期 残留リスクについては、定期的に見直しを行い、必要に応じて、対応の対象とするとともに、リスク対応後の残留リスクについては、リスク所有者のほか、経営陣やその他の利害関係者に認識させることを考慮する。 また、リスク所有者の責任を明確にするために、承認された会議の議事録を正しく保管する。
4.5	情報セキュリティマネジメントの運用［27001-8］
4.5.1	資源管理［27001-7.1 / 5.1］
4.5.1.1	組織は、情報セキュリティマネジメントの確立、実施、維持及び継続的改善に必要な資源を決定し、提供する。［27001-7.1］ 管理目的を満たすためには、継続的に管理策を実施するとともに、人員の増加、システムの増加などの環境の変化に対応するために、適切な時期に適切に提供できるよう、経営資源を確保する。
4.5.1.2	トップマネジメントは、情報セキュリティマネジメントに必要な資源が利用可能であることを確実にするため、以下のような資源を割り当てる。［27001-5.1c)］ ・情報セキュリティマネジメントの各プロセスに必要な人又は組織 ・情報セキュリティマネジメントの各プロセスに必要な設備、装置、システム ・上記に必要な費用
4.5.2	力量、認識［27001-7.2 / 7.3 / 5.1］
4.5.2.1	トップマネジメントは、有効な情報セキュリティマネジメント及びその要求事項への適合の重要性を伝達する。［27001-5.1d)］ トップマネジメントは情報セキュリティマネジメントについて責任を負うが、実施においては組織全体の協力が必要であることを、情報セキュリティ方針と共に関係者に伝える。 また、組織が同じ規定に従って同じ判断ができるように、情報分類等の基準を策定するが、個人情報のように組織によって解釈が一部異なる情報の場合は、一般的な考え方に加え、自社の考え方を明確にした上で、関係者に伝える。
4.5.2.2	組織は、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。［27001-7.2a)］ 情報セキュリティマネジメントに関係する業務及び影響のある業務を特定し、役割を明確にした業務分掌を作成する。これらの業務分掌においては以下の点を明確にする。 ・役職名 ・業務内容 ・担当者の責任範囲 ・業務に必要な知識 ・業務に必要な資格 ・業務に必要な経験 知識や資格、経験などは環境や目的の変化によって変更される可能性があるため、最新の情報となるように随時見直しを行う。
4.5.2.3	組織は、適切な教育、訓練又は経験に基づいて、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）が力量を備えられるようにする。［27001-7.2b)］ 適用される処置には、例えば、現在雇用している人々に対する教育訓練の提供、指導の実施、配置転換の実施などがある（教育や訓練などが間に合わないと判断される場合には相応の力量を有した要員の雇用が、また、社内業務との関連が少ない業務においては外部委託などがある。）。

マネジメント基準	
4.5.2.4	組織は、必要な力量を身に着けるための処置をとり、とった処置の有効性を評価する。[27001-7.2c)] 必要な力量を身に着けるための処置としては、教育訓練が重要である。教育は「必要な知識を得させる」、訓練は「必要なスキル及び経験を得させる」ために実施する。教育の内容は一般的な脅威やぜい弱性などの知識だけではなく、業務上のリスクについてなど、組織の特徴を反映した内容を盛り込むなど、実効性のある内容となるようにする。 教育及び訓練を実施した結果、必要な力量が持てたかどうかを確認するために、以下を実施する。 ・知識の確認テスト ・スキルの実習テスト ・チェックリストなどによるベンチマーク 実施結果については記録し、要員選択の客観性を確保する。
4.5.2.5	組織は、力量を常に把握し、その証拠として、適切な文書化した情報を組織が定めた期間保持する。[27001-7.2d)] 教育、訓練については以下を検討し、定期的に実施する。 ・教育・訓練基本計画 ・教育・訓練実施計画 ・確認テスト又は評価報告 教育や訓練の一部を免除する場合は、それがどの技能や経験、資格に当てはまるかを明確にし、それぞれの担当者について調査し、一覧にする。資格については有効期限などを明確にし、更新する。
4.5.2.6	組織の管理下で働く人々は、情報セキュリティ方針を認識する。[27001-7.3a)] 情報セキュリティの活動について、組織が定めた目的と重要性について、情報セキュリティ方針の通達や教育の一環として周知徹底することによって、管理策がなぜ実施されているのかについての関係者の理解を深める。
4.5.2.7	組織の管理下で働く人々は、情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティマネジメントの有効性に対する自らの貢献を認識する。[27001-7.3b)] 以下の点について組織の管理下で働く人々に伝えることによって、各人の役割及び情報セキュリティマネジメントの有効性に対する自らの貢献を明確にする。 ・情報セキュリティマネジメントにおけるそれぞれの役割 ・役割を実行するための業務と手順(異常を検知した場合の報告手順も含む。) ・これらが記載された文書の所在
4.5.2.8	組織の管理下で働く人々は、情報セキュリティマネジメントの要求事項に適合しないことの意味を認識する。[27001-7.3c)]
4.5.3	コミュニケーション[27001-7.4]
4.5.3.1	組織は、情報セキュリティマネジメントに関連する内部及び外部のコミュニケーションを実施する必要性を決定する。[27001-7.4] a) 内部及び外部のコミュニケーションを実施する際は、以下を考慮することとする。 ・コミュニケーションの内容(何を伝達するか。) ・コミュニケーションの実施時期 ・コミュニケーションの対象者 ・コミュニケーションの実施者 ・コミュニケーションの実施プロセス b) 内部コミュニケーションでは、以下に示すような者と、適宜及び定期的なコミュニケーションを実施する。 ・トップマネジメント ・情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者 ・情報セキュリティマネジメントのパフォーマンスをトップマネジメント又は組織内に報告する権限者 ・組織内の従業員
	c) 外部コミュニケーションでは、以下に示すような者と、必要に応じて、コミュニケーションを実施する。 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・所属するセキュリティ団体、協会
4.5.4	情報セキュリティマネジメントの運用の計画及び管理[27001-8.1]
4.5.4.1	組織は、情報セキュリティ要求事項を満たすため、リスク及び機会に対処する活動を実施するために必要なプロセスを計画し、実施し、かつ管理する。[27001-8.1]

マネジメント基準	
4.5.4.2	組織は、情報セキュリティ目的を達成するための計画を実施する。[27001-8.1]
4.5.4.3	組織は、計画通りに実施されたことを確信するために、文書化した情報を保持する。[27001-8.1] 文書化した情報に、以下の情報が集められているかどうかを確認する。 ・管理策の実施状況 ・管理策の有効性 ・管理策を取り巻く環境の変化 また、これらの情報を把握し判断する体制を構築する。
4.5.4.4	組織は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置をとる。[27001-8.1]
4.5.4.5	組織は、外部委託するプロセスを決定し、かつ、管理する。[27001-8.1]
4.5.5	情報セキュリティリスクアセスメントの実施[27001-8.2 / 8.3]
4.5.5.1	組織は、以下のいずれかの場合において、情報セキュリティリスクアセスメントを実施する。[27001-8.2] ・あらかじめ定めた間隔 ・重大な変更が提案された場合 ・重大な変化が生じた場合
4.5.5.2	組織は、情報セキュリティリスク対応計画を実施する。[27001-8.3] 情報セキュリティリスク対応計画の実施においては、明確にされた個々の責任について全うしていることを確認するための方策を講じる。
4.5.5.3	トップマネジメントは、情報セキュリティリスク対応計画のために十分な経営資源を提供する。 情報セキュリティリスク対応計画には相応の経営資源が必要になるところ、以下の点について考慮する。 ・管理策の導入及び運用にかかる費用、人員、作業工数、技術 ・セキュリティインシデント発生時の一時対応にかかる費用 ・その他のリスク対応にかかる費用 運用においては管理策の効果測定などを実施するために必要な経営資源について考察し、予算化する。
4.6	情報セキュリティマネジメントの監視及びレビュー[27001-5.1 / 8.2 / 9 / 10.2]
4.6.1	有効性の継続的改善[27001-10.2 / 8.2 / 9.2 / 9.3 / 5.1]
4.6.1.1	組織は、以下を実施し、情報セキュリティマネジメントの適切性、妥当性及び有効性を継続的に改善する。[27001-10.2 / 8.2 / 9.2 / 9.3] ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・トップマネジメントによる定期的なマネジメントレビュー 継続的改善においては、これまで実施してきた管理策だけはなく、環境の変化に伴う新たな脅威やぜい弱性についても不適合を検出し処置する。
4.6.1.2	トップマネジメントは、継続的改善を促進する。[27001-5.1g)] 4.6.1.1.を実施するための、役割、責任及び権限を割り当て、実施するよう関係者に伝達する。
4.6.2	パフォーマンス評価[27001-9]
4.6.2.1	組織は、情報セキュリティパフォーマンス及び情報セキュリティマネジメントの有効性を継続的に評価し、以下を決定する。[27001-9.1] ・必要とされる監視及び測定の対象(情報セキュリティプロセス及び管理策を含む。) ・妥当な結果を確実にするための、監視、測定、分析及び評価の方法(比較可能で再現可能な結果を生み出す方法とする。) ・監視及び測定の実施時期及び頻度 ・監視及び測定の実施者 ・監視及び測定の結果の、分析(因果関係、相関関係を含む)及び評価の時期及び頻度 ・監視及び測定の結果の、分析及び評価の実施者 ・分析及び評価の結果に応じた対応措置 ・分析及び評価の結果の報告頻度

マネジメント基準	
4.6.2.2	組織は、あらかじめ定めた間隔で内部監査を実施する。[27001-9.2a) / 9.2b)] a）内部監査を実施する際は、以下を確認する。 ・以下に適合していること。 －情報セキュリティマネジメントに関して、組織自体が規定した要求事項 －本マネジメント基準の要求事項 ・情報セキュリティマネジメントが有効に実施され、維持されていること。 b）内部監査は、管理策の有効性を総合的に確認するために定期的に実施し、計画及び結果について以下の文書で管理する。 ・内部監査基本計画 ・内部監査実施計画 ・内部監査報告書 基本計画書では対象範囲、目的、管理体制及び期間又は期日について、実施計画では実施時期や実施場所、実施担当者及びその割当て及び詳細な監査の手法についてあらかじめ決める。予定通り実施されたことを証明するためにも、実施報告書を作成する。
	c）適合性の監査においては、以下の項目を対象に含む。 ・関連する法令又は規制の要求事項 ・情報セキュリティリスクアセスメントなどによって特定された情報セキュリティ要　求事項 d）情報セキュリティマネジメントが有効に実施され、維持されていることの監査においては、以下の項目を対象に含む。 ・管理策の有効性及び維持 ・管理策が期待通りに実施されていること。
4.6.2.3	組織は、頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持する。[27001-9.2c)] 監査プログラムでは、関連するプロセスの重要性及び前回までの監査の結果を考慮する。 監査は一度にすべての適用範囲について実施するだけではなく、範囲の一部のみを対象とする場合もあり、毎回の監査の目的を明確にし、適切な監査計画を実施することが重要であることから、監査プログラムの作成においては、以下の点を考慮する。 ・監査の目的と重点目標 ・対象となる監査プロセスの状況と重要性 ・対象となる領域の状況と重要性 ・前回までの監査結果
4.6.2.4	組織は、監査基準及び監査範囲を明確にする。[27001-9.2d)]監査プログラムでは全体的な監査の日程だけではなく、以下の内容について含める。 ・監査の基準(以下の内容も含む。)－目的、権限と責任－独立性、客観性と職業倫理－専門能力－業務上の義務－品質管理－監査の実施方法－監査報告書の形式 ・監査の範囲 ・監査の頻度又は時期 ・監査の方法(個別の情報セキュリティ監査基準を作成し、内部監査、外部組織による監査のいずれにおいても、品質の高い監査を実施できるように準備を整える。)
4.6.2.5	組織は、監査プロセスの客観性及び公平性を確実にする監査員の選定及び監査の実施を行う。[27001-9.2e)] 監査人の選定においては監査基準に従い、以下の点を考慮する。 ・外観上の独立性 ・精神上の独立性 ・職業倫理と誠実性 なお、内部の監査員の場合は、自らが従事している業務については自身で監査しないように、他の担当者を割り当てる。
4.6.2.6	組織は、監査の結果を関連する管理層に報告することを確実にする。[27001-9.2f)]
4.6.2.7	組織は、監査プログラム及び監査結果の証拠として、文書化した情報を保持する。[27001-9.2g)] 監査手順に以下の内容を反映させるとともに、文書化し、お互いのコミュニケーションのために活用する。 ・監査の計画・実施に関する責任及び要求事項 ・結果報告・記録維持に関する責任と要求事項 要求事項については監査品質を確保するための必須条件であり、責任者と監査人が同じ目的をもって監査を実施する。

マネジメント基準	
4.6.3	マネジメントレビュー［27001-9.3］
4.6.3.1	トップマネジメントは、あらかじめ定めた間隔で、マネジメントレビューする。［27001-9.3］ あらかじめ定められた間隔でマネジメントレビューを実施するために、以下の点について考慮するとともに、文書化する。 ・マネジメントレビュー基本計画 ・マネジメントレビュー実施計画 ・マネジメントレビューのための実施報告 基本計画書では目的及び実施時期について、実施計画では詳細な監査の手法についてあらかじめ決める。
4.6.3.2	トップマネジメントは、マネジメントレビューにおいて、以下を考慮する。［27001-9.3］ ・前回までのマネジメントレビューの結果とった処置の状況 ・情報セキュリティマネジメントに関連する外部及び内部の課題の変化 ・以下に示す内容を含めた、情報セキュリティパフォーマンスに関するフィードバック -不適合及び是正処置 -監視及び測定の結果 -監査結果 -情報セキュリティ目的の達成 ・利害関係者からのフィードバック ・情報セキュリティリスクアセスメントの結果及び情報セキュリティリスク対応計画の状況 ・継続的改善の機会 また、これらの情報を構成することが予想される活動及び事象を記録し、必要に応じて報告するとともに、緊急性が高いものについてはあらかじめ定義しておき、誰もが同じ判断をできるように基準を定める。
4.6.3.3	マネジメントレビューからのアウトプットには、継続的改善の機会及び情報セキュリティマネジメントのあらゆる変更の必要性に関する決定を含める。［27001-9.3］ マネジメントレビューの結果を改善策に反映するために、以下の活動を実施し、改善策を検討する。 ・情報セキュリティマネジメントの有効性の改善 ・情報セキュリティリスクアセスメント及び情報セキュリティリスク対応計画の更新 ・情報セキュリティマネジメントに影響を与える可能性のある内外の事象を考慮の上での手順及び管理策の修正 ・必要となる経営資源の特定 ・パフォーマンス測定方法の改善 なお、改善策の立案においては、情報セキュリティリスク対応の選択肢を選択した際の記録を参考にする。
4.6.3.4	組織は、マネジメントレビューの結果の証拠として文書化した情報を保持する。［27001-9.3］ マネジメントレビューの結果は次回のマネジメントレビューに活用されるため、実施内容と結果が分かるように具体的に記録する。
4.7	情報セキュリティマネジメントの維持及び改善［27001-10］
4.7.1	是正処置［27001-10.1］
4.7.1.1	組織は、不適合が発生した場合、不適合の是正のための処置を取る。［27001-10.1a)］ a）是正措置 を取る際は、以下を実施する。 ・その不適合を管理し、是正するための処置 ・その不適合によって起こった結果への対処 ・是正処置を手順どおりに実施するために、以下について文書化する。 －不適合の再発防止を確実にするために選択した処置の必要性の評価 －必要な是正処置の決定 －必要な是正処置の実施 －実施した処置の記録

マネジメント基準	
	－実施した是正処置のレビュー
	b）不適合は以下の活動によって検出される。 ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・定期的なマネジメントレビュー ・不適合を手順どおりに検出するために、以下について文書化する。 －情報セキュリティマネジメントに対する不適合の特定 －情報セキュリティマネジメントに対する不適合の原因の決定 なお、単一の活動だけでは判断できない場合もあるので、複合的な結果の考察から不適合を検出する。
4.7.1.2	組織は、不適合が再発又は他のところで発生しないようにするため、その不適合の原因を除去するための処置をとる必要性を評価する。［27001-10.1b)］ 必要性を評価する際は、以下を実施する。 ・その不適合のレビュー ・その不適合の原因の明確化 ・類似の不適合の有無、又はそれが発生する可能性の明確化
4.7.1.3	組織は、必要な処置を実施する。［27001-10.1c)］
4.7.1.4	組織は、とった全ての是正処置の有効性をレビューする。［27001-10.1d)］
4.7.1.5	組織は、必要な場合には、情報セキュリティマネジメントの変更を行う。［27001-10.1e)］
4.7.1.6	組織は、是正処置は、検出された不適合のもつ影響に応じたものとする。［27001-10.1］
4.7.1.7	組織は、是正処置の証跡として、以下の文書化した情報を保持する。［27001-10.1f) / 10.1g)］ ・不適合の性質及びとった処置 ・是正処置の結果
4.8	文書化した情報の管理［27001-7.5］
4.8.1	文書化の指針［27001-7.5.1］
4.8.1.1	組織は、情報セキュリティマネジメントが必要とする以下の情報を文書化する。［27001-7.5.1］ ・情報セキュリティ方針 ・情報セキュリティ目的 ・情報セキュリティリスクアセスメントのプロセス ・情報セキュリティリスク対応のプロセス ・情報セキュリティリスクアセスメントの結果 ・情報セキュリティリスク対応計画 ・パフォーマンス測定の結果 これらの内容についてはどの文書に記載されていてもかまわないが、その内容を知る必要がある担当者には必ず伝わるように構成するとともに、知る必要性のない者が閲覧できないことを確実にする。
4.8.2	文書の作成・変更及び管理［27001-7.5.2 / 7.5.3］
4.8.2.1	組織は、以下を行うことによって、文書化した情報を作成及び更新する。［27001-7.5.2］・適切な識別情報の記述（例えば、表題、日付、作成者、参照番号）・適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）の選択・適切性及び妥当性に関する、適切なレビュー及び承認・文書化した情報のライフサイクルの定義や、それに応じた処理ができるような手順の策定・文書を発行する前における、適正性のレビュー及び承認・必要に応じた、文書の更新及び再承認・廃止文書の誤使用の防止・廃止文書を何らかの目的で保持する場合における、廃止文書であることが分かる適切な識別情報の記述・法的及び規制の要求事項及び環境の変化に従い、定めた頻度での更新 また、これらのすべての活動が文書管理に反映されているか、またその活動が業務に大きな障害を与えていないかなどを考慮し、適切な文書管理手順を策定する。
4.8.2.2	組織は、以下のことを確実にするために、情報セキュリティマネジメントで要求された文書化した情報を、管理する。［27001-7.5.3］ ・文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態であること。

マネジメント基準	
	・文書化した情報が十分に保護されていること(例えば、機密性の喪失、不適切な使用及び完全性の喪失からの保護)。 ・文書化した情報の配付、アクセス 、検索及び利用 ・文書化した情報の読みやすさが保たれることを含む、保管及び保存 ・文書化した情報の変更の管理(例えば、版の管理) ・文書化した情報の保持及び廃棄 また、情報セキュリティマネジメントの計画及び運用のために組織が必要と決定した文書は、外部から入手したものであっても、必要に応じて、特定し、管理する。
4.9	情報セキュリティリスクコミュニケ―ション
	利害関係者間の有効なコミュニケーションは、意思決定に大きな影響を与えることがある。情報セキュリティリスクコミュニケーションは、意思決定者とその他の利害関係者(クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。)との間で情報セキュリティリスクに関する情報を交換、共有し、リスクを管理する方法に関する合意を得る。
4.9.1	リスクコミュニケーションの計画
4.9.1.1	リスクコミュニケ―ション計画を策定する。 リスクコミュニケーション計画は、以下の2つに分けて策定し、文書化する。 ・通常運用のためのリスクコミュニケーション計画 ・緊急事態のためのリスクコミュニケーション計画 リスクコミュニケーション計画は、意思決定者とその他の利害関係者(クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。)との間でどのようにコミュニケーションを図るかに留意し、以下の内容について含める。 ・適切な利害関係者の参画による、効果的な情報交換／共有 ・法令、規制及びガバナンスの要求事項の順守 ・コミュニケーション及び協議に関するフィードバック及び報告の提供 ・組織に対する信頼を醸成するためのコミュニケーションの活用 ・危機又は不測の事態発生時の利害関係者とのコミュニケーションの実施
4.9.2	リスクコミュニケーションの実施
4.9.2.1	リスクコミュニケ―ションを実施する仕組みを確定する。 リスクに関する論議、その優先順位の決定及び適切なリスク対応、並びにリスク受容を行い、主要な意思決定者と利害関係者(クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。)の協調を得る仕組みを確定する。この仕組みでは次の事項を確実にする。 ・リスクマネジメントの枠組みの主要な構成要素、及びその後に行うあらゆる修正の適切な伝達 ・枠組み、その有効性及び成果に関する適切な内部報告 ・適切な階層及び時期に利用可能な、リスクマネジメントの適応から導出される関連情報の提供 ・内部の利害関係者との協議のためのプロセス 仕組みには、適切な場合には、多様な情報源からのリスク情報について、まとめ上げるプロセスが含まれ、また、リスク情報の影響の受けやすさを考慮する必要がある場合もある。なお、この仕組みを設ける場として、委員会がある。
4.9.2.2	リスクコミュニケ―ションを実施する。 リスクコミュニケーションは、次の点を達成するために、リスクマネジメントプロセスのすべての段階で継続的に実施する。 ・組織のリスクマネジメント結果の保証を提供する ・リスク情報を収集する ・リスクアセスメントの結果を共有しリスク対応計画を提示する ・意思決定者と利害関係者(クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。)の相互理解の欠如による情報セキュリティ違反の発生及び結果を回避又は低減する ・意思決定を支援する ・新しい情報セキュリティ知識を入手する

マネジメント基準	
	・他の組織と協調しすべてのインシデントの結果を低減するための対応計画を立案する ・意思決定者及び利害関係者(クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。)にリスクについての責任を意識させる ・セキュリティ意識を改善する リスクコミュニケーションの実施においては、組織内の適切な広報又はコミュニケーション部門と協力し、リスクコミュニケーション関連の全タスクを調整して行う。

3. 管理策基準

管理策基準	
5	情報セキュリティのための方針群
5.1	情報セキュリティのための経営陣の方向性 管理目的:情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制に従って提示するため。
5.1.1	情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知する。 (脚注)管理層には、経営陣及び管理者が含まれる。ただし、実務管理者(administrator)は除かれる。
5.1.2	情報セキュリティのための方針群は、あらかじめ定めた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューする。
6	情報セキュリティのための組織
6.1	内部組織 管理目的:組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。
6.1.1	全ての情報セキュリティの責任を定め、割り当てる。
6.1.1.13.PB	クラウドサービス事業者は、クラウドサービス利用者、クラウドサービス事業者及び供給者と、情報セキュリティの役割及び責任の適切な割当てについて合意し、文書化する。
6.1.2	相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離する。
6.1.3	関係当局との適切な連絡体制を維持する。
6.1.3.3.PB	クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービス事業者の組織の地理的所在地、及びクラウドサービス事業者がクラウドサービス利用者のデータを保管する可能性のある国々及びその法管轄を通知する。
6.1.4	情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持する。
6.1.5	プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組む。
6.2	モバイル機器及びテレワーキング 管理目的:モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。
6.2.1	モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用する。
6.2.2	テレワーキングの場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施する。
6.3.P	クラウドサービス利用者及びクラウドサービス事業者の関係 管理目的:情報セキュリティマネジメントのための、クラウドサービス利用者及びクラウドサービス提供者間の共同責任の関係を説明するため。
6.3.1.P	クラウドサービス利用者及びクラウドサービス事業者の両者は、クラウドサービスの利用における情報セキュリティの共同責任について、文書化し、公表し、伝達し、実装する。
6.3.1.1.PB	クラウドサービス事業者は、クラウドサービス利用の一環としてクラウドサービス利用者が実施及び管理を必要とする情報セキュリティの役割と責任に加え、クラウドサービスの利用に対する、クラウドサービス事業者の情報セキュリティ管理策及び責任を文書化し、通知する。
7	人的資源のセキュリティ

管理策基準	
7.1	雇用前 管理目的:従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。
7.1.1	全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。
7.1.2	従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載する。
7.2	雇用期間中 管理目的:従業員及び契約相手が、情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするため。
7.2.1	経営陣は、組織の確立された方針及び手順に従った情報セキュリティの適用を、全ての従業員及び契約相手に要求する。
7.2.2	組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受ける。
7.2.2.19.PB	クラウドサービス事業者は、クラウドサービス利用者のデータ及びクラウドサービスの派生データの適切な取扱いに関して、従業員に意識向上のための教育及び訓練を提供し、かつ同じことをするよう契約相手に要請する。
7.2.3	情報セキュリティ違反を犯した従業員に対して処置をとるための、正式かつ周知された懲戒手続を備える。
7.3	雇用の終了及び変更 管理目的:雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。
7.3.1	雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、その従業員又は契約相手に伝達し、かつ、遂行させる。
8	資産の管理
8.1	資産に対する責任 管理目的:組織の資産を特定し、適切な保護の責任を定めるため。
8.1.1	情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持する。
8.1.1.6.PB	クラウドサービス事業者の資産目録は、クラウドサービス利用者のデータ及びクラウドサービスの派生データを明確に特定する。
8.1.2	目録の中で維持される資産は、管理する。
8.1.2.7.PB	クラウドサービス事業者は、クラウドサービス利用者に対し、当該利用者の資産(バックアップを含む)を管理するため、次のいずれかを提供する。 (a)当該利用者の管理する資産を、記録媒体に記録する(バックアップを含む)前に暗号化し、当該利用者が暗号鍵を管理し消去する機能 (b) 当該利用者が、当該利用者の管理する資産を記録媒体に記録する(バックアップを含む)前に暗号化し、暗号鍵を管理し消去する機能を実装するために必要となる情報
8.1.3	情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施する。
8.1.4	全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。
8.1.5.P	クラウドサービス事業者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時機を失せずに返却または除去する。
8.2	情報分類 管理目的:組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。
8.2.1	情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類する。
8.2.2	情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施する。
8.2.2.7.PB	クラウドサービス事業者は、クラウドサービス利用者が扱う情報及び関連資産を当該利用者が分類し、ラベル付けするためのサービス機能について文書化し、開示する。
8.2.3	資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施する。
8.3	媒体の取扱い 管理目的:媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。
8.3.1	組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施する。
8.3.2	媒体が不要になった場合は、正式な手順を用いて、セキュリティを保って処分する。
8.3.3	情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護する。

管理策基準	
9	アクセス制御
9.1	アクセス制御に対する業務上の要求事項 管理目的:情報及び情報処理施設へのアクセスを制限するため。
9.1.1	アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューする。
9.1.2	利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供する。
9.2	利用者アクセスの管理管理目的:システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。
9.2.1	アクセス権の割当てを可能にするために、利用者の登録及び登録削除についての正式なプロセスを実施する。
9.2.1.6.PB	クラウドサービスのユーザによるクラウドサービスへのアクセスをクラウドサービス利用者が管理するため、クラウドサービス事業者は、クラウドサービス利用者に、ユーザの登録及び登録削除の機能及び仕様を提供する。
9.2.2	全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者アクセスの提供についての正式なプロセスを実施する。
9.2.2.8.PB	クラウドサービス事業者は、クラウドサービスのユーザのアクセス権を管理する機能及び仕様を提供する。
9.2.3	特権的アクセス権の割当て及び利用は、制限し、管理する。
9.2.3.11.PB	クラウドサービス事業者は、特定したリスクに応じて、クラウドサービスの管理能力にあわせたクラウドサービス利用者の管理者認証に、十分に強固な認証技術(例えば、多要素認証機能)を提供する。
9.2.4	秘密認証情報の割当ては、正式な管理プロセスによって管理する。
9.2.4.9.PB	クラウドサービス事業者は、秘密認証情報を割り当てる手順、及びユーザ認証手順を含む、クラウドサービス利用者の秘密認証情報の管理手順について、情報を提供する。
9.2.5	資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューする。
9.2.6	全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正する。
9.3	利用者の責任 管理目的:利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。
9.3.1	秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求する。
9.4	システム及びアプリケーションのアクセス制御 管理目的:システム及びアプリケーションへの、認可されていないアクセスを防止するため。
9.4.1	情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限する。
9.4.1.8.PB	クラウドサービス事業者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス、及びサービスにて保持されるクラウドサービス利用者のデータへのアクセスを、クラウドサービス利用者が制限できるよう、アクセス制御を提供する。
9.4.2	アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御する。
9.4.2.2.B	強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、暗号による手段、スマートカード、トークン、生体認証などの認証方法を用いる。
9.4.3	パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にするものとする。
9.4.4	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。
9.4.5	プログラムソースコードへのアクセスは、制限する。
9.5.P	共有化された仮想環境におけるクラウドサービス利用者のデータのアクセス制御 管理目的:共有化されたクラウドコンピューティング上の仮想環境における情報セキュリティを確実にするため。
9.5.1.P	クラウドサービス利用者のクラウドサービス上の仮想環境は、他のクラウドサービス利用者及び認可されていない者から保護する。
9.5.2.P	クラウドコンピューティング環境における仮想マシンは、事業上のニーズを満たすため、要塞化する。
9.5.2.1.PB	クラウドサービス事業者は、仮想マシンを設定する際には、適切に要塞化し(例えば、クラウドサービスを実行するのに必要なポート、プロトコル及びサービスのみを有効とする)、利用する各仮想マシンに適切な技術的管理策(例えば、マルウェア対策、ログ取得)を実施する。
10	暗号

管理策基準	
10.1	暗号による管理策 管理目的:情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。
10.1.1	情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施する。
10.1.1.9.PB	クラウドサービス事業者は、クラウドサービス利用者に、当該利用者が処理する情報を保護するために暗号技術を利用する機能を提供し、または、暗号技術を利用する環境についての情報を提供する。
10.1.2	暗号鍵の利用、保護及び有効期間(lifetime)に関する方針を策定し、そのライフサイクル全体にわたって実施する。
10.1.2.20.PB	クラウドサービス事業者は、クラウドサービス利用者に、当該利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供する。
11	物理的及び環境的セキュリティ
11.1	セキュリティを保つべき領域 管理目的:組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。
11.1.1	取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。
11.1.2	セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護する。
11.1.3	オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する。
11.1.4	自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用する。
11.1.5	セキュリティを保つべき領域での作業に関する手順を設計し、適用する。
11.1.6	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。また、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す。
11.2	装置 管理目的:資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。
11.2.1	装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、保護する。
11.2.2	装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。
11.2.3	データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。
11.2.4	装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。
11.2.5	装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さない。
11.2.6	構外にある資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用する。
11.2.7	記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証する。
11.2.7.4.PB	クラウドサービス事業者は、資源(例えば、装置、データストレージ、ファイル、メモリ)のセキュリティを保った処分又は再利用の取り決めを、時期を失せずに行うことを確実にする仕組みを整備する。
11.2.8	利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にする仕組みを整備する。
11.2.9	書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用する。 (脚注)クリアデスクとは、机上に書類を放置しないことをいう。また、クリアスクリーンとは、情報をスクリーンに残したまま離席しないことをいう。
12	運用のセキュリティ
12.1	運用の手順及び責任 管理目的:情報処理設備の正確かつセキュリティを保った運用を確実にするため。
12.1.1	操作手順は、文書化し、必要とする全ての利用者に対して利用可能とする。
12.1.2	情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理する。
12.1.2.11.PB	クラウドサービス事業者は、クラウドサービス利用者の情報セキュリティに悪影響を及ぼす可能性のあるクラウドサービスの変更に関する情報を、クラウドサービス利用者に提供する。

管理策基準	
12.1.3	要求された主要なシステム資源の使用を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。
12.1.3.9.PB	クラウドサービス事業者は、資源不足による情報セキュリティインシデントを防ぐため、全資源の容量を監視する。
12.1.4	開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離する。
12.1.5.P	クラウドコンピューティング環境の、管理のための操作手順を定義し、文書化し、監視する。
12.1.5.1.PB	クラウドサービス事業者は、重要な操作及び手順に関する文書を、それを求めるクラウドサービス利用者に提供する。
12.2	マルウェアからの保護 管理目的:情報及び情報処理施設がマルウェアから保護されることを確実にするため。
12.2.1	マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施する。
12.3	バックアップ 管理目的:データの消失から保護するため。
12.3.1	情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査する。
12.4	ログ取得及び監視 管理目的:イベントを記録し、証拠を作成するため。
12.4.1	利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。
12.4.1.15.PB	クラウドサービス事業者は、クラウドサービス利用者に、ログ取得機能を提供する。
12.4.2	ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護する。
12.4.3	システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューする。
12.4.4	組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させる。
12.4.4.4.PB	クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービス事業者のシステムで利用するクロックに関する情報及びクラウドサービス利用者がクラウドサービスのクロックにローカルクロックを同期させる方法についての情報を提供する。
12.4.5.P	クラウドサービス利用者は、利用するクラウドサービスの操作を監視する機能を有する。
12.5	運用ソフトウェアの管理 管理目的:運用システムの完全性を確実にするため。
12.5.1	運用システムに関わるソフトウェアの導入を管理するための手順を実施する。
12.6	技術的ぜい弱性管理 管理目的:技術的ぜい弱性の悪用を防止するため。
12.6.1	利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価する。さらに、それらと関連するリスクに対処するために、適切な手段をとる。
12.6.1.18.PB	クラウドサービス事業者は、提供するクラウドサービスに影響を及ぼす可能性のある技術的ぜい弱性の管理についての情報を、クラウドサービス利用者が利用可能となるようにする。
12.6.2	利用者によるソフトウェアのインストールを管理する規則を確立し、実施する。
12.7	情報システムの監査に対する考慮事項 管理目的:運用システムに対する監査活動の影響を最小限にするため。
12.7.1	運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意する。
13	通信のセキュリティ
13.1	ネットワークセキュリティ管理 管理目的:ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。
13.1.1	システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御する。
13.1.2	組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定し、また、ネットワークサービス合意書にもこれらを盛り込む。

管理策基準	
13.1.3	情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離する。
13.1.4.P	仮想ネットワークを設定する際には、クラウドサービス事業者のネットワークセキュリティ方針に基づき、仮想ネットワークと物理ネットワークの設定の整合性を検証する。
13.2	情報の転送 管理目的:組織の内部及び外部に転送した情報のセキュリティを維持するため。
13.2.1	あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備える。
13.2.2	合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱う。
13.2.3	電子的メッセージ通信に含まれた情報は、適切に保護する。
13.2.4	情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューし、文書化する。
14	システムの取得、開発及び保守
14.1	情報システムのセキュリティ要求事項 管理目的:ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。
14.1.1	情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含める。
14.1.2	公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護する。
14.1.3	アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。 ・不完全な通信 ・誤った通信経路設定 ・認可されていないメッセージの変更 ・認可されていない開示 ・認可されていないメッセージの複製又は再生
14.2	開発及びサポートプロセスにおけるセキュリティ 管理目的:情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。
14.2.1	ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用する。
14.2.1.13.PB	クラウドサービス事業者は、開示方針に反しない範囲で、セキュリティを保つための開発手順及び慣行についての情報を提供する。
14.2.2	開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理する。
14.2.3	オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験する。
14.2.4	パッケージソフトウェアの変更は、抑止し、必要な変更だけに限る。また、全ての変更は、厳重に管理する。
14.2.5	セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用する。
14.2.6	組織は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護する。
14.2.7	組織は、外部委託したシステム開発活動を監督し、監視する。
14.2.8	セキュリティ機能(functionality)の試験は、開発期間中に実施する。
14.2.9	新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立する。
14.3	試験データ 管理目的:試験に用いるデータの保護を確実にするため。
14.3.1	試験データは、注意深く選定し、保護し、管理する。
15	供給者関係
15.1	供給者関係における情報セキュリティ 管理目的:供給者がアクセスできる組織の資産の保護を確実にするため。
15.1.1	組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化する。

管理策基準	
15.1.1.14.B	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実化を含める。
15.1.1.16.B	当該事業者が提供するサービス上で取り扱われる情報に対して国内法以外の法令及び規制が適用された結果、クラウドサービス利用者の意図しないまま当該利用者の管理する情報にアクセスされ、又は処理されるリスクを評価して外部委託先を選定し、必要に応じてクラウドサービス利用者が扱う情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を指定する。
15.1.2	関連する全ての情報セキュリティ要求事項を確立し、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のための IT 基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意する。
15.1.2.18.PB	クラウドサービス事業者は、クラウドサービス事業者とクラウドサービス利用者の間に誤解が生じないように、クラウドサービス事業者が実行する適切な情報セキュリティ対策を、合意の一環として定める。
15.1.3	供給者との合意には、情報通信技術(以下「ICT」という。)サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含める。
15.2	供給者のサービス提供の管理 管理目的:供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。
15.2.1	組織は、供給者のサービス提供を定常的に監視し、レビューし、監査する。
15.2.2	関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更(現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む)を管理する。
16	情報セキュリティインシデント管理
16.1	情報セキュリティインシデントの管理及びその改善 管理目的:セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。
16.1.1	情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立する。
16.1.2	情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告する。
16.1.3	組織の情報システム及びサービスを利用する従業員及び契約相手に、システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は、どのようなものでも記録し、報告するように要求する。
16.1.4	情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定する。
16.1.5	情報セキュリティインシデントは、文書化した手順に従って対応する。
16.1.6	情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いる。
16.1.7	組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用する。
16.1.7.13.PB	クラウドサービス事業者は、クラウドサービス利用者と、クラウドコンピューティング環境内の潜在的なディジタル形式の証拠、又はその他の情報の要求に対応する手順を合意する。
17	事業継続マネジメントにおける情報セキュリティの側面
17.1	情報セキュリティ継続 管理目的:情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。
17.1.1	組織は、困難な状況(adverse situation)(例えば、危機又は災害)における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定する。
17.1.2	組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持する。
17.1.3	確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、組織は、定められた間隔でこれらの管理策を検証する。
17.2	冗長性 管理目的:情報処理施設の可用性を確実にするため。
17.2.1	情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。
18	順守

管理策基準	
18.1	法的及び契約上の要求事項の順守 管理目的:情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。
18.1.1	各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。
18.1.2	知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施する。
18.1.2.13.PB	クラウドサービス事業者は、知的財産権の順守に対応するためのプロセスを確立する。
18.1.3	記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。
18.1.3.13.PB	クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービスの利用に関して、クラウドサービス事業者が収集し、蓄積する記録の保護について、情報を提供する。
18.1.4	プライバシー及び個人識別情報(PII)の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実に行う。
18.1.5	暗号化機能は、関連する全ての協定、法令及び規制を順守して用いる。
18.1.5.7.PB	クラウドサービス事業者は、クラウドサービス利用者に、適用する協定、法令及び規則を順守していることをレビューするため、クラウドサービス事業者が実装した暗号による管理策の記載を、提供する。
18.2	情報セキュリティのレビュー 管理目的:組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。
18.2.1	情報セキュリティ及びその実施の管理(例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順)に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。
18.2.2	管理者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューする。
18.2.3	情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューする。

【別紙３】

様式

みどりチェック実施状況報告書

事業名	
事業者名	
担当者・連絡先	

（注）共同事業体の場合は代表機関のみ提出してください。

以下のア～エの取組について、実施状況を報告します。

ア　環境負荷低減に配慮したものを調達するよう努める。

具体的な事項	実施した／努めた	左記非該当
・対象となる物品の輸送に当たり、燃料消費を少なくするよう検討する（もしくはそのような工夫を行っている配送業者と連携する）。	□	□
・対象となる物品の輸送に当たり、燃費効率の向上や温室効果ガスの過度な排出を防ぐ観点から、輸送車両の保守点検を適切に実施している。	□	□
・農林水産物や加工食品を使用する場合には、農薬等を適正に使用して（農薬の使用基準等を遵守して）作られたものを調達することに努めている。	□	□
・事務用品を使用する場合には、詰め替えや再利用可能なものを調達することに努めている。	□	□
・その他（　　）		

・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由
（　　）

イ　エネルギーの削減の観点から、オフィスや車両・機械などの電気、燃料の使用状況の記録・保存や、不必要・非効率なエネルギー消費を行わない取組（照明、空調のこまめな管理や、ウォームビズ・クールビズの励行、燃費効率の良い機械の利用等）の実施に努める。

具体的な事項	実施した／努めた	左記非該当
・事業実施時に消費する電気・ガス・ガソリン等のエネルギーについて、帳簿への記載や伝票の保存等により、使用量・使用料金の記録に努めている。	□	□
・事業実施時に使用するオフィスや車両・機械等について、不要な照明の消灯やエンジン停止に努めている。	□	□
・事業実施時に使用するオフィスや車両・機械等について、基準となる室温を決めたり、必要以上の冷暖房、保温を行わない等、適切な温度管理に努めている。	□	□
・事業実施時に使用する車両・機械等が効果的に機能を発揮できるよう、定期的な点検や破損があった場合は補修等に努めている。	□	□
・夏期のクールビズや冬期のウォームビズの実施に努めている。	□	□
・その他（　　）		

・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由
（　　）

ウ　廃棄物の発生抑制、適正な循環的な利用及び適正な処分に努める。

具体的な事項	実施した／努めた	左記非該当
・事業実施時に使用する資材について、プラスチック資材から紙などの環境負荷が少ない資材に変更することを検討する。	□	□
・資源のリサイクルに努めている（リサイクル事業者に委託することも可）。	□	□
・事業実施時に使用するプラスチック資材を処分する場合に法令に従って適切に実施している。	□	□
・その他（　　）		

・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由
（　　）

エ　みどりの食料システム戦略の理解に努めるとともに、機械等を扱う場合は、機械の適切な整備及び管理並びに作業安全に努める。

具体的な事項	実施した／努めた	左記非該当
・「環境配慮のチェック・要件化（みどりチェック）チェックシート解説書 －民間事業者・自治体等編－」にある記載内容を了知し、関係する事項について取り組むよう努める。	□	□
・事業者として独自の環境方針やビジョンなどの策定している、もしくは、策定を検討する。	□	□
・従業員等向けの環境や持続性確保に係る研修などを行っている、もしくは、実施を検討する。	□	□
・作業現場における、作業安全のためのルールや手順などをマニュアル等に整理する。また、定期的な研修などを実施するように努めている。	□	□
・資機材や作業機械・設備が異常な動作などを起こさないよう、定期的な点検や補修などに努めている。	□	□
・作業現場における作業空間内の工具や資材の整理などを行い、安全に作業を行えるスペースを確保する。	□	□
・労災保険等の補償措置を備えるよう努めている。	□	□
・その他（　　）		

・上記で「実施した／努めた」に一つもチェックが入らず（全て「左記非該当」）、その他の取組も行っていない場合は、その理由
（　　）

【別紙４】

委託事業における人件費の算定等の適正化について

１．委託事業に係る人件費の基本的な考え方

（１）人件費とは委託事業に直接従事する者（以下「事業従事者」という。）の直接作業時間に対する給料その他手当をいい、その算定に当たっては、原則として以下の計算式により構成要素ごとに計算する必要がある。

また、委託事業計画書及び実績報告書の担当者の欄に事業従事者の役職及び氏名を記載すること。

人件費＝　時間単価※1　×　直接作業時間数※2

※１　時間単価

時間単価については、契約締結時に後述する算定方法により、事業従事者一人一人について算出し、原則として額の確定時に時間単価の変更はできない。

ただし、以下に掲げる場合は、額の確定時に時間単価を変更しなければならない。

・事業従事者に変更があった場合

・事業従事者の雇用形態に変更があった場合（正職員が嘱託職員として雇用された等）

・委託先における出向者の給与の負担割合に変更があった場合

・超過勤務の概念がない管理職や研究職等職員（以下、「管理者等」という。）が当該委託事業に従事した時間外労働の実績があった場合

また、上記のほか、地域別、業種別等の賃金水準の変動に伴い、委託先において賃金改定をした場合であって、実施中の委託事業に適用される時間単価が適当でないと認められるときは、別途委託先と協議の上、時間単価を変更することができる。その場合、委託先との協議は、履行期限まで３か月以上ある場合に限り開始できるものとし、協議が調ったときは、当該賃金改定が適用された日（月を単位として適用された場合はその月）以降の人件費について、変更後の時間単価を適用するものとする。

※２　直接作業時間数

①　正職員、出向者及び嘱託職員

直接作業時間数については、当該委託事業に従事した実績時間についてのみ計上すること。

②　管理者等

原則、管理者等については、直接作業時間数の算定に当該委託事業に従事した時間外労働時間（残業・休日出勤等）を含めることはできない。ただし、当該委託事業の遂行上やむを得ず当該委託事業のために従事した時間外労働にあっては、直接作業時間数に当該委託事業に従事した時間外労働時間（残業・休日出勤等）を含めることができることとする。

（２）一の委託事業だけに従事することが、雇用契約書等により明らかな場合は、上記によらず次の計算式により算定することができる

人件費＝　日額単価　×　勤務日数

人件費＝　給与月額　×　勤務月数（１月に満たない場合は、日割り計算による。）

２．受託単価による算定方法

委託先（地方公共団体を除く。以下２．において同じ。）において、受託単価規程等が存在する場合には、同規程等における単価（以下「受託単価」という。）の構成要素等の精査を委託契約締結時に行った上で、受託単価による算定を認める。

○　受託単価の構成要素を精査する際の留意点

ア　事業従事者の職階（課長級、係長級などに対応した単価）に対応しているか。

イ　受託単価に人件費の他に技術経費、一般管理費、その他経費が含まれている場合は、各単価及びその根拠を確認すること。

ウ　受託単価に技術経費、一般管理費等が含まれている場合は、委託事業計画書及び委託事業実績報告書の経費の区分欄に計上する技術経費、一般管理費に重

複計上されていないか確認すること。

＜受託単価による算定方法＞

○正職員及び管理者等の時間単価は、受託単価規定等に基づく時間単価を使用すること。

○出向者、嘱託職員の受託単価計算

事業従事者が出向者、嘱託職員である場合は、受託単価規程等により出向者受託単価、嘱託職員受託単価が規定されている場合は、それぞれの受託単価を使用することができる。ただし、出向者及び嘱託職員に係る給与については、委託先が全額を負担、一部のみ負担、諸手当が支給されていない等多様であるため、適用する受託単価の構成要素のうち人件費分について精査し、後述する実績単価により算出された人件費単価を超えることはできない。

３．実績単価による算定方法

委託先に受託単価規程等が存在しない場合には、時間単価は以下の計算方法（以下「時間単価計算」という。）により算定する。（円未満は切捨て）

＜実績単価の算定方法＞

○正職員、出向者（給与等を全額委託先で負担している者に限る。）及び嘱託職員の人件費時間単価の算定方法

原則として下記により算定する。

人件費時間単価＝（年間総支給額＋年間法定福利費等）÷年間理論総労働時間

・年間総支給額及び年間法定福利費の算定根拠は、「前年又は前年度若しくは直近１年間の支給実績」を用いるものとする。ただし、中途採用など前年又は前年度若しくは直近１年間の支給実績による算定が困難な場合は、別途委託先と協議の上定めるものとする（以下同じ。）。

・年間総支給額は、基本給、管理職手当、都市手当、住宅手当、家族手当、通勤手当等の諸手当及び賞与の年間合計額とし、時間外手当、食事手当などの福利厚生面

で支給されているものは除外する（以下同じ。）。

・年間法定福利費等は、健康保険料、厚生年金保険料（厚生年金基金の掛金部分を含む。）、労働保険料、児童手当拠出金、身体障害者雇用納付金、労働基準法の休業補償及び退職手当引当金の年間事業者負担分とする（以下同じ。）。

・年間理論総労働時間は、年間総支給額の算定期間に係る営業カレンダー等から年間所定営業日数を算出し、就業規則等から１日当たりの所定労働時間を算出し、これらを乗じて得た時間とする（以下同じ。）。

○出向者（給与等の一部を委託先で負担している者）の時間単価の算定方法

出向者（給与等の一部を委託先で負担している者）の時間単価は、原則として下記により算定する。

人件費時間単価＝委託先が負担する（した）（年間総支給額＋年間法定福利費等） ÷年間理論総労働時間

・事業従事者が出向者である場合の人件費の精算に当たっては、当該事業従事者に対する給与等が委託先以外（出向元等）から支給されているかどうか確認するとともに、上記計算式の年間総支給額及び年間法定福利費は、委託先が負担した額しか計上できないことに注意すること。

○管理者等の時間単価の算定方法

原則として管理者等の時間単価は、下記の（１）により算定する。ただし、やむを得ず時間外に当該委託事業に従事した場合は、（２）により算定した時間単価を額の確定時に適用する。

（１）原則

人件費時間単価＝（年間総支給額＋年間法定福利費等）÷年間理論総労働時間

（２）時間外に従事した場合

人件費時間単価＝（年間総支給額＋年間法定福利費等）÷年間実総労働時間

・時間外の従事実績の計上は、業務日誌以外にタイムカード等により年間実総労働時間を立証できる場合に限る。

・年間実総労働時間＝年間理論総労働時間＋当該委託事業及び自主事業等における時間外の従事時間数の合計

４．一般競争入札により委託契約を締結する場合の例外について

一般競争入札により委託契約を締結する場合、受託規程で定める単価よりも低い受託単価又は本来の実績単価よりも低い実績単価を定めている場合は、精算時においても同単価により人件費を算定すること。

５．直接作業時間数を把握するための書類整備について

直接作業時間数の算定を行うためには、実際に事業に従事した事を証する業務日誌が必要となる。また、当該業務日誌において事業に従事した時間のほか、他の業務との重複がないことについて確認できるよう作成する必要がある。

【業務日誌の記載例】

（4月）　所属　○○○部 ××課　　役職 ○○○○　　氏名 ○○ ○○　　時間外手当支給対象者か否か

時／日	0	…	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	業務時間及び業務内容
1				←A→				←B→												A(3h)○○検討会資料準備 B(5．25h)○○調査打ち合わせ
2				←A→				←A→			←C→									A(6h)○○検討会資料準備、検討会 C(2h)○○開発打ち合わせ
3				←D→				←B→			←A→									D(3h)自主事業 B(2h)○○調査打ち合わせ A(4h)現地調査事前準備
4				←A→																A(9．5h)○○調査現地調査
5				←A→				←D→												A(3h)○○検討会資料準備 D(5h)自主事業
・																				
・																				
・																				
・																				
30																				
31																				
勤務時間管理者　所属：○○部長 氏名：○○○○												A:○○○○委託事業(○○農政局) B:○○○○委託事業(○○農政局) C:○○○○補助事業(○○局) D:自主事業							合計		A(○○h) B(○○h) C(○○h) D(○○h)

① 人件費の対象となっている事業従事者ごとの業務日誌を整備すること（当該委託事業の従事時間と他の事業及び自主事業等に係る従事時間・内容との重複記載は認められないことに留意する。）。

② 業務日誌の記載は、事業に従事した者本人が原則毎日記載すること（数週間分まとめて記載することや、他の者が記載すること等、事実と異なる記載がなされることが

ないよう適切に管理すること。）。

③　当該委託事業に従事した実績時間を記載すること。なお、従事した時間に所定時間外労働（残業・休日出勤等）時間を含める場合は、以下の事由による場合とする。

・委託事業の内容から、平日に所定時間外労働が不可欠な場合

・委託事業の内容から、休日出勤（例：土日にシンポジウムを開催等）が必要である場合で、委託先が休日手当を支給している場合。ただし、支給していない場合でも委託先において代休など振替措置を手当している場合は同様とする。

④　昼休みや休憩時間など勤務を要しない時間は、除外すること。

⑤　当該委託事業における具体的な従事内容が分かるように記載すること。なお、出張等における移動時間についても当該委託事業のために従事した時間として計上することができるが、出張行程に自主事業等他の事業が含まれる場合は、按分計上を行う必要がある。

⑥　当該委託事業以外の業務を兼務している場合には、他の事業と当該委託事業の従事状況を確認できるように区分して記載すること。

⑦　委託先における勤務時間管理者は、タイムカード（タイムカードがない場合は出勤簿）等帳票類と矛盾がないか、他の事業と重複して記載していないかを確認の上、記名する。

附　則

（施行期日）

１　この通知は、平成２２年９月２７日以降に制定する委託事業仕様書等に基づく委託事業から適用する。

（経過措置）

２　この通知の施行日現在、既に制定されている委託事業仕様書等に基づき実施されている平成２２年度の委託事業における人件費の算定等について、当該委託事業に係る委託元又は委託先において本通知の趣旨を踏まえた対応が可能な事項がある場合には、当該事項については、本通知により取り扱うものとする。

３　前項の委託事業仕様書等に基づく委託事業を平成２３年度以降も実施する場合には、本通知を適用する。

附　則

この通知は、令和３年１月１日から施行する。

【別紙４】

附　則（令和８年１月１９日付け７予第１９４２号）

（施行期日）

１　この通知は、令和８年１月１９日から施行する。

（経過措置）

２　この通知の施行前に、この通知による改正前の委託事業における人件費の算定等の適正化について（平成 22 年９月 27 日付け 22 経第 961 号大臣官房経理課長通知。以下「人件費通知」という。）に基づき、この通知による改正後の人件費通知と異なる取扱いをしている委託事業における人件費の算定については、この通知による改正前の人件費通知の規定を適用することができる。

別紙５　質問票

事業者名：
日付：　　令和　　年　　月　　日

No.	資料名	頁	仕様書の該当記載内容	分類 (意見/質問)	意見/質問内容
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

別紙６

資料閲覧申請書

申込日：　令和　　年　　月　　日

１　会 社 名：

２　住　　所：

３　担当者名：

４　電話番号：

５　E-mail アドレス：

６　閲覧日時：　　年　　月　　日　　時

７　閲覧者氏名：
：
：
：
：

別紙７

機密保持誓約書

「令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業」に係る資料閲覧に当たり、下記の事項を厳守することを誓約します。

記

１　農林水産省の情報セキュリティに関する規程等を遵守し、農林水産省が開示した情報（公知の情報を除く。）を本調達の目的以外に使用又は第三者に開示若しくは漏えいすることのないよう、必要な措置を講じます。

２　閲覧資料については、複製及び撮影を行いません。

３　本業務に係る調達の期間中及び終了後にかかわらず、守秘義務を負います。

４　上記１～３に反して、情報を本調達の目的以外に使用又は第三者に開示若しくは漏えいした場合、法的な責任を負うものであることを確認し、これにより農林水産省が被った一切の損害を賠償します。また、その際には秘密保持に関する農林水産省の監査を受けることとし、誠実に対応します。

令和　　年　　月　　日

住　　所

会 社 名

代表者名

委　託　契　約　書　（案）

支出負担行為担当官農林水産省大臣官房参事官（経理）須田　亙（以下「甲」という。）と○○○○○（以下「乙」という。）は、令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業（以下「委託事業」という。）の委託について、次のとおり委託契約を締結する。

【契約の相手方が共同事業体の場合】
支出負担行為担当官農林水産省大臣官房参事官（経理）須田　亙（以下「甲」という。）と■■共同事業体（以下「乙」という。）の構成員を代表する法人□□□□代表●●は、令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業（以下「委託事業」という。）の委託について、次のとおり委託契約を締結する。

（実施する委託事業）
第１条　甲は、次の委託事業の実施を乙に委託し、乙は、その成果を甲に報告するものとする。
（１）委託事業名 令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業
（２）委託事業の内容及び経費　別添委託事業計画書（別紙様式第１号）のとおり
（３）履行期限　令和９年３月３１日

（委託事業の遂行）
第２条　乙は、委託事業を、別添の委託事業計画書に記載された計画に従って実施しなければならない。当該計画が変更されたときも同様とする。

（委託費の限度額）
第３条　甲は、委託事業に要する費用（以下「委託費」という。）として、金　　円（うち消費税及び地方消費税の額○○円）を超えない範囲内で乙に支払うものとする。
（注）「消費税及び地方消費税の額」は、消費税法（昭和63年法律第108号）第28条第１項及び第29条並びに地方税法（昭和25年法律第226号）第72条の82及び第72条の83の規定により算出したもので、委託費の限度額に110分の10を乗じて得た金額である。
２　乙は、委託費を別添の委託事業計画書に記載された費目の区分に従って使用しなければならない。当該計画が変更されたときも同様とする。

（契約保証金）
第４条　会計法（昭和22年法律第35号）第29条の９第１項に規定する契約保証金の納付は、予算決算及び会計令（昭和22年勅令第165号）第100条の３第３号の規定により免除する。

（再委託の制限）
第５条　乙は、委託事業の全部を一括して、又は主たる部分を第三者に委任し、又は請け負わせてはならない。
なお、主たる部分とは、業務における総合的企画、業務遂行管理、手法の決定及び技術的判断等をいうものとする。
２　乙は、この委託事業の達成のため委託事業の一部を第三者に委任し、又は請け負わせること（以下「再委託」という。）を必要とするときは、あらかじめ再委託承認申請書（別紙様式第２号）に必要事項を記載して甲の承認を得なければな

らない。ただし、再委託ができる事業は、原則として委託費の限度額に占める再委託の金額の割合（以下「再委託比率」という。）が50パーセント以内の業務とする。

3　乙は、前項の再委託の承認を受けようとするときは、当該第三者の氏名又は名称、住所、再委託を行う業務の範囲、再委託の必要性及び契約金額について記載した書面を甲に提出しなければならない。

ただし、本委託事業の仕様書においてこれらの事項が記載されている場合にあっては、甲の承認を得たものとみなす。

4　乙は、前項の書面に記載した事項を変更しようとするときは、あらかじめ甲の承認を得なければならない。

5　乙は、この委託事業達成のため、再々委託又は再々請負（再々委託又は再々請負以降の委託又は請負を含む。以下同じ。）を必要とするときは、再々委託又は再々請負の相手方の氏名又は名称、住所及び業務の範囲を記載した書面を、第２項の承認の後、速やかに甲に届け出なければならない。

6　乙は、再委託の変更に伴い再々委託又は再々請負の相手方又は業務の範囲を変更する必要がある場合には、第４項の変更の承認の後、速やかに前項の書面を変更し、甲に届け出なければならない。

7　甲は、前２項の書面の届出を受けた場合において、この契約の適正な履行の確保のため必要があると認めるときは、乙に対し必要な報告を求めることができる。

8　再委託する業務が委託業務を行う上で発生する事務的業務であって、再委託比率が50パーセント以内であり、かつ、再委託する金額が100万円以下である場合には、軽微な再委託として第２項から前項までの規定は適用しない。

（再委託の制限の例外）

第６条　前条第１項及び第２項の規定に関わらず、再委託する業務が次の各号に該当する場合、乙は、委託事業の主たる部分及び再委託比率が50パーセントを超える業務を委任し、又は請け負わせることが出来るものとする。

（１）再委託する業務が海外で行われる場合

（２）広告、放送等の主たる業務を代理店が一括して請け負うことが慣習となっている場合

（３）会社法(平成17年法律第86号)第２条第３号の規定に基づく子会社若しくは財務諸表等の用語、様式及び作成方法に関する規則(昭和38年11月27日大蔵省令第59号)第８条第５項及び第６項に規定する関連会社に業務の一部を請け負わせる場合

2　前項の再委託がある場合において、再委託比率は、当該再委託の金額を全ての再委託の金額及び委託費の限度額から減算して計算した率とする。

（監督）

第７条　甲は、この委託事業の適正な履行を確保するために監督をする必要があると認めたときは、甲の命じた監督のための職員（以下「監督職員」という。）に監督させることができるものとする。

2　前項に定める監督は、立会い、指示その他の適切な方法により行うものとする。

3　乙は、甲（監督職員を含む。）から監督に必要な委託事業実施計画表等の提出を求められた場合は、速やかに提出するものとする。

（実績報告）

第８条　乙は、委託事業が終了したとき（委託事業を中止し、又は廃止したときを含む。）は、委託事業の成果を記載した委託事業実績報告書（別紙様式第３号）

を甲に提出するものとする。

（検査）

第９条　甲は、前条に規定する実績報告書の提出を受けたときは、これを受理した日から10日以内の日（当該期間の末日が休日（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。）に当たるときは、当該末日の翌日を当該期間の末日とする。）又は当該委託事業の履行期限の末日に属する年度の３月31日のいずれか早い日までに、当該委託事業が契約の内容に適合するものであるかどうかを当該実績報告書及びその他関係書類又は実地により検査を行うものとする。

２　甲が前項に規定する検査により当該委託事業の内容の全部又は一部が本契約に違反し又は不当であることを発見したときは、甲は、その是正又は改善を求めることができる。この場合においては、甲が乙から是正又は改善した給付を終了した旨の通知を受理した日から10日以内に、当該委託事業が契約の内容に適合するものであるかどうか再度検査を行うものとする。

（委託費の額の確定）

第10条　甲は、前条に規定する検査の結果、当該委託事業が契約の内容に適合すると認めたときは、委託費の額を確定し、乙に対して通知するものとする。

２　前項の委託費の確定額は、委託事業に要した経費の実支出額と第３条第１項に規定する委託費の限度額のいずれか低い額とする。

（委託費の支払）

第11条　甲は、前条の規定により委託費の額が確定した後、乙からの適法な精算払請求書（別紙様式第４号）を受理した日から30日以内にその支払を行うものとする。

ただし、乙が委託事業実績報告書（別紙様式第３号）の提出に併せて、委託費の精算払請求を行った場合は、前条第１項に規定する通知の日から30日以内にその支払を行うものとする。

２　甲は、概算払の財務大臣協議が調った場合においては、前項の規定にかかわらず、乙の請求により、必要があると認められる金額については、概算払をすることができるものとする。

３　乙は、前項の概算払を請求するときは、概算払請求書（別紙様式第４号）を甲に提出するものとし、甲は、乙からの適法な概算払請求書を受理した日から30日以内にその支払を行うものとする。

（過払金の返還）

第12条　乙は、既に支払を受けた委託費が、第10条第１項の委託費の確定額を超えるときは、その超える金額について、甲の指示に従って返還するものとする。

（委託事業の中止等）

第13条　乙は、天災地変その他やむを得ない事由により、委託事業の遂行が困難となったときは、委託事業中止（廃止）申請書（別紙様式第５号）を甲に提出し、甲乙協議の上、契約を解除し、又は契約の一部変更を行うものとする。

２　前項の規定により契約を解除するときは、前３条の規定に準じ精算するものとする。

（計画変更の承認）

第14条　乙は、前条に規定する場合を除き、別添の委託事業計画書に記載された委託事業の内容又は経費の内訳を変更しようとするときは、委託事業計画変更承認

申請書（別紙様式第６号）を甲に提出し、その承認を受けなければならない。
ただし、委託事業計画書２の収支予算の支出の部の区分欄に掲げる経費の相互間における30パーセント以内の金額の流用については、この限りではない。
２　甲は、前項の承認をするときは、条件を付すことができる。

（契約の解除等）
第15条　甲は、乙がこの契約に違反した場合、又は、正当な理由なく履行の全部又は一部が不能となることが明らかとなったときは、契約を解除し、又は変更し、及び既に支払った金額の全部又は一部の返還を乙に請求することができる。

（違約金）
第16条　次の各号のいずれかに該当する場合においては、甲は乙に対し、違約金として契約金額の100分の10に相当する額を請求することができる。
（１）前条の規定によりこの契約が解除された場合
（２）乙がその債務の履行を拒否し、又は、乙の責めに帰すべき事由によって乙の債務について履行不能となった場合
２　次の各号に掲げる者がこの契約を解除した場合は、前項第２号に該当する場合とみなす。
（１）乙について破産手続開始の決定があった場合において、破産法（平成16年法律第75号）の規定により選任された破産管財人
（２）乙について更正手続開始の決定があった場合において、会社更生法（平成14年法律第154号）の規定により選任された管財人
（３）乙について再生手続開始の決定があった場合において、民事再生法（平成11年法律第225号）の規定により選任された再生債務者等
３　甲は、前条の規定によりこの契約を解除した場合、これにより乙に生じる損害について、何ら賠償ないし補償することは要しないものとする。

（談合等の不正行為に係る解除）
第17条　甲は、この契約に関し、乙が次の各号の一に該当するときは、契約の全部又は一部を解除することができる。
（１）公正取引委員会が、乙又は乙の代理人に対して私的独占の禁止及び公正取引の確保に関する法律（昭和22年法律第54号。以下「独占禁止法」という。）第７条若しくは第８条の２（同法第８条第１号又は第２号に該当する行為の場合に限る。）の規定による排除措置命令を行ったとき、同法第７条の２第１項（同法第８条の３において読み替えて準用する場合を含む。）の規定による課徴金納付命令を行ったとき又は同法第７条の４第７項若しくは第７条の７第３項の規定による課徴金の納付を命じない旨の通知を行ったとき。
（２）乙又は乙の代理人（乙又は乙の代理人が法人にあっては、その役員又は使用人を含む。）が刑法（明治40年法律第45号）第96条の６若しくは第198条又は独占禁止法第89条第１項若しくは第95条第１項第１号の規定による刑の容疑により公訴を提起されたとき。
２　乙は、この契約に関して、乙又は乙の代理人が前項各号に該当した場合には、速やかに、当該処分等に係る関係書類を甲に提出しなければならない。

（談合等の不正行為に係る違約金）
第18条　乙は、この契約に関し、次の各号の一に該当するときは、甲が前条により契約の全部又は一部を解除するか否かにかかわらず、契約金額の100分の10に相当する額を違約金として甲が指定する期日までに支払わなければならない。
（１）公正取引委員会が、乙又は乙の代理人に対して独占禁止法第７条又は第８条の２（同法第８条第１号又は第２号に該当する行為の場合に限る。）の規定に

よる排除措置命令を行い、当該排除措置命令が確定したとき。
（２）公正取引委員会が、乙又は乙の代理人に対して独占禁止法第７条の２第１項（同法第８条の３において読み替えて準用する場合を含む。）の規定による課徴金納付命令を行い、当該納付命令が確定したとき。
（３）公正取引委員会が、乙又は乙の代理人に対して独占禁止法第７条の４第７項又は第７条の７第３項の規定による課徴金の納付を命じない旨の通知を行ったとき。
（４）乙又は乙の代理人（乙又は乙の代理人が法人にあっては、その役員又は使用人を含む。）に係る刑法第96条の６若しくは第198条又は独占禁止法第89条第１項若しくは第95条第１項第１号の規定による刑が確定したとき。
２　乙は、前項第４号に規定する場合に該当し、かつ、次の各号の一に該当するときは、前項の契約金額の100分の10に相当する額のほか、契約金額の100分の５に相当する額を違約金として甲が指定する期日までに支払わなければならない。
（１）前項第２号に規定する確定した納付命令について、独占禁止法第７条の３第１項の規定の適用があるとき。
（２）前項第４号に規定する刑に係る確定判決において、乙又は乙の代理人（乙又は乙の代理人が法人にあっては、その役員又は使用人を含む。）が違反行為の首謀者であることが明らかになったとき。
（３）乙が甲に対し、入札（又は見積）心得第３条（公正な入札（又は見積）の確保）の規定に抵触する行為を行っていない旨の誓約書を提出しているとき。
３　乙は、契約の履行を理由として、前２項の違約金を免れることができない。
４　第１項及び第２項の規定は、甲に生じた実際の損害の額が違約金の額を超過する場合において、甲がその超過分の損害につき賠償を請求することを妨げない。

（属性要件に基づく契約解除）
第19条　甲は、乙が次の各号の一に該当すると認められるときは、何らの催告を要せず、本契約を解除することができる。
（１）法人等（個人、法人又は団体をいう。）の役員等（個人である場合はその者、法人である場合は役員又は支店若しくは営業所（常時契約を締結する事務所をいう。）の代表者、団体である場合は代表者、理事等、その他経営に実質的に関与している者をいう。以下同じ。）が、暴力団（暴力団員による不当な行為の防止等に関する法律（平成３年法律第77号）第２条第２号に規定する暴力団をいう。以下同じ。）又は暴力団員（同法第２条第６号に規定する暴力団員をいう。以下同じ。）であるとき。
（２）役員等が、自己、自社若しくは第三者の不正の利益を図る目的、又は第三者に損害を加える目的をもって、暴力団又は暴力団員を利用するなどしているとき。
（３）役員等が、暴力団又は暴力団員に対して、資金等を供給し、又は便宜を供与するなど直接的あるいは積極的に暴力団の維持、運営に協力し、若しくは関与しているとき。
（４）役員等が、暴力団又は暴力団員であることを知りながらこれを不当に利用するなどしているとき。
（５）役員等が、暴力団又は暴力団員と社会的に非難されるべき関係を有しているとき。

（行為要件に基づく契約解除）
第20条　甲は、乙が自ら又は第三者を利用して次の各号の一に該当する行為をした場合は、何らの催告を要せず、本契約を解除することができる。
（１）暴力的な要求行為
（２）法的な責任を超えた不当な要求行為

（３）取引に関して脅迫的な言動をし、又は暴力を用いる行為
（４）偽計又は威力を用いて契約担当官等の業務を妨害する行為
（５）その他前各号に準ずる行為

（表明確約）
第21条　乙は、第19条の各号及び第20条各号のいずれにも該当しないことを表明し、かつ、将来にわたっても該当しないことを確約する。
２　乙は、前２条各号の一に該当する行為を行った者（以下「解除対象者」という。）を再受託者等（再委託の相手方及び再委託の相手方が当該契約に関して個別に契約する場合の当該契約の相手方をいう。以下同じ。）としないことを確約する。

（再委託契約等に関する契約解除）
第22条　乙は、契約後に再受託者等が解除対象者であることが判明したときは、直ちに当該再受託者等との契約を解除し、又は再受託者等に対し当該解除対象者（再受託者等）との契約を解除させるようにしなければならない。
２　甲は、乙が再受託者等が解除対象者であることを知りながら契約し、若しくは再受託者等の契約を承認したとき、又は正当な理由がないのに前項の規定に反して当該再受託者等との契約を解除せず、若しくは再受託者等に対し当該解除対象者（再受託者等）との契約を解除させるための措置を講じないときは、本契約を解除することができる。

（損害賠償）
第23条　甲は、第19条、第20条及び前条第２項の規定により本契約を解除した場合は、これにより乙に生じた損害について、何ら賠償ないし補償することは要しない。
２　乙は、甲が第19条、第20条及び前条第２項の規定により本契約を解除した場合において、甲に損害が生じたときは、その損害を賠償するものとする。

（不当介入に関する通報・報告）
第24条　乙は、自ら又は再受託者等が、暴力団、暴力団員、社会運動・政治運動標ぼうゴロ等の反社会的勢力から不当要求又は業務妨害等の不当介入（以下「不当介入」という。）を受けた場合は、これを拒否し、又は再受託者等をして、これを拒否させるとともに、速やかに不当介入の事実を甲に報告するとともに、警察への通報及び捜査上必要な協力を行うものとする。

（著作権等）
第25条　乙は、委託事業により納入された著作物に係る一切の著作権（著作権法（昭和45年法律第48号）第27条及び第28条に規定する権利を含む。）を、著作物の引渡し時に甲に無償で譲渡するものとし、甲の行為について著作者人格権を行使しないものとする。
２　乙は、第三者が権利を有する著作物を使用する場合は、原著作者等の著作権及び肖像権等の取扱いに厳重な注意を払い、当該著作物の使用に関して費用の負担を含む一切の手続きを行うものとする。
３　乙は、甲が著作物を活用する場合及び甲が認めた場合において第三者に二次利用させる場合は、原著作者等の著作権及び肖像権等による新たな費用が発生しないように措置するものとする。それ以外の利用に当たっては、甲は乙と協議の上、その利用の取り決めをするものとする。
４　この契約に基づく作業に関し、第三者と著作権及び肖像権等に係る権利侵害の紛争等が生じた場合、当該紛争等の原因が専ら甲の責めに帰す場合を除き、乙は

自らの責任と負担において一切の処理を行うものとする。この場合、甲は係る紛争等の事実を知ったときは、乙に通知し、必要な範囲で訴訟上の防衛を乙に委ねる等の協力措置を講じるものとする。

（著作権等の利用）

第26条　乙は、前条第１項の規定にかかわらず、委託事業により納入された著作物に係る著作権について、甲による当該著作物の利用に必要な範囲において、甲が利用する権利及び甲が第三者に利用を許諾する権利を、甲に許諾したものとする。

２　乙は、甲及び甲が許諾した第三者による利用について、著作者人格権を行使しないものとする。また、乙は、当該著作物の著作者が乙以外の者であるときは、当該著作者が著作者人格権を行使しないように必要な措置をとるものとする。

３　乙は、委託事業の成果によって生じた著作物及びその二次的著作物の公表に際し、委託事業による成果である旨を明示するものとする。

（委託事業の調査）

第27条　甲は、必要に応じ、乙に対し、実績報告書における委託費の精算に係る審査時その他の場合において、委託事業の実施状況、委託費の使途その他必要な事項について所要の調査報告を求め、又は実地に調査することができるものとし、乙はこれに応じなければならないものとする。

（帳簿等）

第28条　乙は、各委託事業の委託費については、委託事業ごとに、帳簿を作成・整備した上で、乙単独の事業又は国庫補助事業の経費とは別に、かつ、各委託事業の別に、それぞれ明確に区分して経理しなければならない。

２　乙は、委託費に関する帳簿への委託費の収入支出の記録は、当該収入支出の都度、これを行うものとする。

３　乙は、前項の帳簿及び委託事業実績報告書に記載する委託費の支払実績を証するための証拠書類又は証拠物（以下「証拠書類等」という。）を、乙の文書管理規程等の保存期限の規定にかかわらず、当該委託事業終了の翌年度の４月１日から起算して５年間、整備・保管しなければならない。

４　乙は、委託事業実績報告書の作成・提出に当たっては、帳簿及び証拠書類等と十分に照合した委託事業に要した経費を記載しなければならない。

５　乙は、前各項の規定のいずれかに違反し又はその他不適切な委託費の経理を行ったと甲が認めた場合には、当該違反等に係る委託費の交付を受けることができず、又は既にその交付を受けている場合には、甲の指示に従い当該額を返還しなければならない。

（旅費及び賃金）

第29条　乙は、委託費からの旅費及び賃金の支払については、いずれも各委託事業の実施要領等に定める委託調査等の実施と直接関係ある出張又は用務に従事した場合に限るものとする。

２　乙は、前項の規定に違反した不適切な委託費の経理を行ったと甲が認めた場合には、当該違反等に係る委託費の交付を受けることができず、又は既にその交付を受けている場合には、甲の指示に従い当該額を返還しなければならない。

（秘密の保持等）

第30条　乙は、この委託事業に関して知り得た業務上の秘密をこの契約期間にかかわらず第三者に漏らしてはならない。

（個人情報に関する秘密保持等）
第31条　乙及びこの委託事業に従事する者（従事した者を含む。以下「委託事業従事者」という。）は、この委託事業に関して知り得た個人情報（生存する個人に関する情報であって、当該情報に含まれる氏名、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。）を委託事業の遂行に使用する以外に使用し、又は提供してはならない。
２　乙及び委託事業従事者は、保有した個人情報の内容をみだりに他人に知らせ、又は不当な目的に利用してはならない。
３　前２項については、この委託事業が終了した後においても同様とする。

（個人情報の複製等の制限）
第32条　乙は、委託事業を行うために保有した個人情報について、毀損等に備え重複して保存する場合又は個人情報を送信先と共有しなければ委託事業の目的を達成することができない場合以外には、複製、送信、送付又は持ち出しをしてはならない。

（個人情報の漏えい等の事案の発生時における対応）
第33条　乙は、委託事業を行うために保有した個人情報について、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、甲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しなければならない。

（委託事業終了時における個人情報の消去及び媒体の返却）
第34条　乙は、委託事業が終了したときは、この委託事業において保有した各種媒体に保管されている個人情報については、直ちに復元又は判読不可能な方法により情報の消去又は廃棄を行うとともに、甲より提供された個人情報については、返却しなければならない。

（再委託の条件）
第35条　乙は、甲の承認を受け、この委託事業を第三者に再委託する場合は、個人情報の取扱いに関して必要かつ適切な監督を行い、第31条から第34条に規定する甲に対する義務を当該第三者に約させなければならない。

（疑義の解決）
第36条　前各条のほか、この契約に関して疑義を生じた場合には、甲乙協議の上、解決するものとする。

上記契約の証として、本契約書２通を作成し、双方記名の上、各１通を保有するものとする。

令和　　年　　月　　日

委託者（甲）　東京都千代田区霞が関１丁目２番１号
支出負担行為担当官
農林水産省大臣官房参事官（経理）
須田　亙

受託者（乙）　住　所
氏　名

（注）　電子契約書以外の場合は、甲乙それぞれ押印が必要。

（別紙様式第１号）

委　託　事　業　計　画　書

１　事業内容

ア　事業実施方針

令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業仕様書（以下「仕様書」という。）に基づき、事業を実施する。

イ　事業内容

仕様書のとおり。

ウ　事業実施期間

契約締結日～令和９年３月３１日

エ　担当者

オ　報告の方法

仕様書のとおり。

２　収支予算

収入の部

区　　分	予　算　額	備　　考
国 庫 委 託 費		うち消費税及び地方消費税の額〇〇円
計		

支出の部

区　　分	予　算　額	備　　考
計		

（注）備考欄には、各区分ごとの経費に係る算出基礎を記入し、必要がある場合は説明を付すこと。

一般管理費を経費として計上する場合は、原則、人件費及び事業費（再委託費を除く）の10%以内とし、これによりがたい場合は受託者の内部規程等で定められた率を使用すること。

備品（原型のまま比較的長期の反復使用に耐えうるもののうち取得価格が50,000円以上の物品）の購入は認めない。

３　再委託先等

氏名又は名称	住　　所	業務の範囲	必要性及び契約金額

（注）再委託先名及び金額が記載されている提案書が当該委託事業の仕様書として採用された場合に限る。

(契約の相手方が共同事業体の場合)

4　構成員の事業計画

ア　担当事業名	イ　構成員名		ウ　構成員の事業内容
	住所		
	名称		委託限度額：　　円
	住所		
	名称		委託限度額：　　円
	住所		
	名称		委託限度額：　　円

・代表機関を含む構成員の担当者は相互に連携し、十分確認の上、作成すること。

・1行目に代表機関の事業計画を記載すること。また、2行目以降は、参画する構成員の事業計画を記載すること。

・ア 担当事業名欄については、仕様書に示す事業内容のうち構成員が実施する課題名を記載すること。

・ウ 構成員の事業内容欄については、構成員が実施する事業内容の概略を記載すること。

（別紙様式第２号）

令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業再委託承認申請書

番　　号
年　　月　　日

支出負担行為担当官
農林水産省大臣官房参事官（経理）　殿

（受託者）
住　所
氏　名

令和　　年　　月　　日付け契約の令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業について、下記のとおり再委託したいので、委託契約書第５条第２項の規定により承認されたく申請します。

記

１　再委託先の相手方の氏名又は名称及び住所

２　再委託を行う業務の範囲

３　再委託の必要性

４　再委託金額

５　個人情報の取扱いに関する事項

６　その他必要な事項

（注）１　申請時に再委託先及び再委託金額（限度額を含む。）を特定できない事情がある場合には、その理由を記載すること。
　　なお、再委託の承認後に再委託先及び再委託金額が決定した場合には、当該事項をこの書類に準じて、報告すること。
２　再委託の承認後に再委託の相手方、業務の範囲又は再委託金額（限度額を含む。）を変更する場合には、あらかじめ甲の承認を受けなければならない。
３　契約の性質に応じて、適宜、様式を変更して使用すること。

（別紙様式第３号）

令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業実績報告書

番　　号
年　　月　　日

支出負担行為担当官
農林水産省大臣官房参事官（経理）　殿
（官署支出官
農林水産省大臣官房予算課経理調査官　殿）

（受託者）
住　所
氏　名

令和　年　月　日付け契約の令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業について、下記のとおり、事業を実施したので、委託契約書第８条の規定により、その実績を報告します。
（なお、併せて委託費金　　円也の支払を請求します。）

記

１　事業の実施状況
ア　事業内容
イ　事業実施期間
ウ　担当者
エ　事業の成果（又はその概略）
オ　事業成果報告書の配付実績等

２　収支精算
収入の部

区　分	精算額	予算額	比較増減		備　　考
			増	減	
国庫委託費 計					うち消費税及び地方消費税の額〇〇円

支出の部

区　分	精算額	予算額	比較増減		備　　考
			増	減	
  計					

（注）　備考欄には、精算の内訳を記載すること。

(契約の相手方が共同事業体の場合)

3　構成員の実績

ア　担当事業名	イ　構成員名		ウ　構成員の事業内容
	住所		
	名称		実績額：　　円
	住所		
	名称		実績額：　　円
	住所		
	名称		実績額：　　円

・代表機関を含む構成員の担当者は相互に連携し、十分確認の上、作成すること。

・1行目に代表機関の事業計画を記載すること。また、2行目以降は、参画する構成員の事業計画を記載すること。

・ア　担当事業名欄については、仕様書に示す事業内容のうち構成員が実施する課題名を記載すること。

・ウ 構成員の事業内容欄については、構成員が実施する事業内容の概略を記載すること。

（別紙様式第４号）

令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業委託費概算払・精算払　請求書

番　　号
年　　月　　日

官署支出官
農林水産省大臣官房予算課経理調査官　殿

（受託者）
住　所
氏　名

令和　年　月　日付け契約の令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業について、下記により、委託費
金　　円也を、　概算払・精算払　　により支払されたく請求します。

記

区　分	国庫委託費	既受領額		今回請求額		残　　額		事業完了予定年月日	備考
		金額	出来高	金額	出来高	金額	出来高		

（注）精算払請求の場合については、実績報告書に併記することにより請求書に代えることができるものとする。

(別紙様式第５号)

令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業中止（廃止）申請書

番　　号
年　　月　　日

支出負担行為担当官
農林水産省大臣官房参事官（経理）　殿

(受託者)
住　所
氏　名

令和　年　月　日付け契約の令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業について、下記により中止（廃止）したいので、委託契約書第13条第１項の規定により申請します。

記

１　委託事業の中止（廃止）の理由
２　中止（廃止）しようとする以前の事業実施状況
ア　事業について
イ　経費について

経費支出状況

経費の区分	○月○日現在 支出済額	残　額	支出予定額	中止（又は廃止）に伴う 不　用　額	備　考

３　中止（廃止）後の措置
ア　事業について
イ　経費について
ウ　経費支出予定明細

経費の区分	支出予定金額	算　　出　　基　　礎 （名称、数量、単価、金額）

（別紙様式第６号）

令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業計画変更承認申請書

番　　号
年　　月　　日

支出負担行為担当官
農林水産省大臣官房参事官（経理）　殿

（受託者）
住　所
氏　名

令和　年　月　日付け契約の令和８年度米穀流通事業者の届出・報告に関する業務のシステム化調査委託事業について、下記のとおり変更したいので、委託契約書第14条第１項の規定により承認されたく申請します。

記

１　変更の理由
２　変更する事業計画又は事業内容
３　変更経費区分

（注）記載方法は、別に定めのある場合を除き、委託事業計画書の様式を準用し、 当初計画と変更計画を明確に区分して記載のこと。