別添２

調達における情報セキュリティの確保に関する特約条項

（情報セキュリティ実施手順の確認）

第１条　乙は、契約締結後、速やかに情報セキュリティ実施手順（甲の定める「調達における情報セキュリティ基準」（以下「本基準」という。）第２項第８号に規定する「情報セキュリティ実施手順」をいう。以下同じ。）を作成し、甲の定める本基準に適合していることについて甲の確認を受けなければならない。ただし、既に甲の確認を受けた情報セキュリティ実施手順と同一である場合は、特別な指示がない限り、届出をすれば足りる。

２　乙は、前項により甲の確認を受けた情報セキュリティ実施手順を変更しようとするときは、あらかじめ、当該変更部分が甲の定める本基準に適合していることについて甲の確認を受けなければならない。

３　甲は、乙に対して情報セキュリティ実施手順及びそれらが引用している文書の提出、貸出し、又は閲覧を求めることができる。

（保護すべき情報の取扱い）

第２条　乙は、前条において甲の確認を受けた情報セキュリティ実施手順に基づき、この契約に関する保護すべき情報（甲の定める本基準第２項第１号に規定する「保護すべき情報」をいう。以下同じ。）を取り扱わなければならない。

（保護すべき情報の漏えい等に関する乙の責任）

第３条　乙は、乙の従業員又は下請負者（契約の履行に係る作業に従事する全ての事業者（乙を除く。）をいう。）の故意又は過失により保護すべき情報の漏えい、紛失、破壊等の事故があったときであっても、契約上の責任を免れることはできない。

（第三者への開示及び下請負者への委託）

第４条　乙は、やむを得ず保護すべき情報を第三者に開示する場合には、あらかじめ、開示先において情報セキュリティが確保されることを別紙様式に定める確認事項により確認した上で、書面により甲の許可を受けなければならない。

２　乙は、第三者との契約において乙の保有し、又は知り得た情報を伝達、交換、共有その他提供する約定があるときは、保護すべき情報をその対象から除く措置を講じなければならない。

３　乙は、契約の履行に当たり、保護すべき情報を下請負者に取り扱わせる場合には、あらかじめ、別紙様式に定める確認事項によって、当該下請負者において情報セキュリティが確保されることを確認し、その結果を甲に届け出なければならない。ただし、輸送その他の保護すべき情報を知り得ないと乙が認める業務を委託する場合は、この限りではない。

（調査）

第５条　甲は、仕様書等に定める情報セキュリティ対策に関する調査を行うことができる。

２　甲は、前項に規定する調査を行うため、甲の指名する者を乙の事業所、工場その他の関係場所に派遣することができる。

３　甲は、第１項に規定する調査の結果、乙の情報セキュリティ対策が情報セキュリティ実施手順を満たしていないと認められる場合は、その是正のため必要な措置を講じるよう求めることができる。

４　乙は、前項の規定による甲の求めがあったときは、速やかにその是正措置を講じなければならない。

５　乙は、甲が乙の下請負者に対し調査を行うときは、甲の求めに応じ、必要な協力を行わなければならない。また、乙は、乙の下請負者が是正措置を求められた場合、講じられた措置について甲に報告しなければならない。

（事故等発生時の措置）

第６条　乙は、保護すべき情報の漏えい、紛失、破壊等の事故が発生したときは、適切な措置を講じるとともに、直ちに把握しうる限りの全ての内容を、その後速やかにその詳細を甲に報告しなければならない。

２　次に掲げる場合において、乙は、適切な措置を講じるとともに、直ちに把握しうる限りの全ての内容を、その後速やかにその詳細を甲に報告しなければならない。

（１）保護すべき情報が保存されたサーバ又はパソコン（以下「サーバ等」という。）に悪意のあるコード（本基準第２項第21号に規定する「悪意のあるコード」をいう。以下同じ。）への感染又は不正アクセスが認められた場合

（２）保護すべき情報が保存されているサーバ等と同一のイントラネットに接続されているサーバ等に悪意のあるコードへの感染又は不正アクセスが認められ、保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染又は不正アクセスのおそれがある場合

３　第１項に規定する事故について、それらの疑い又は事故につながるおそれ

のある場合は、乙は、適切な措置を講じるとともに、速やかにその詳細を甲に報告しなければならない。

4　前３項に規定する報告のほか、保護すべき情報の漏えい、紛失、破壊等の事故が発生した可能性又は将来発生する懸念について乙の内部又は外部から指摘があったときは、乙は、直ちに当該可能性又は懸念の真偽を含む把握しうる限りの全ての内容を、速やかに事実関係の詳細を甲に報告しなければならない。

5　前各項に規定する報告を受けた甲による調査については、前条の規定を準用する。

6　乙は、第１項に規定する事故がこの契約及び関連する物品の運用に与える影響等について調査し、その措置について甲と協議しなければならない。

7　第１項に規定する事故が乙の責めに帰すべき事由によるものである場合には、前項に規定する協議の結果取られる措置に必要な経費は、乙の負担とする。

8　前項の規定は、甲の損害賠償請求権を制限するものではない。

（契約の解除）

第７条　甲は、乙の責めに帰すべき事由により前条第１項に規定する事故が発生し、この契約の目的を達することができなくなった場合は、この契約の全部又は一部を解除することができる。

2　前項の場合においては、主たる契約条項の契約の解除に関する規定を準用する。

（契約履行後における乙の義務等）

第８条　第２条、第３条、第５条及び第６条の規定は、契約履行後においても準用する。ただし、当該情報が保護すべき情報でなくなった場合は、この限りではない。

2　甲は、本基準第６項第２号イ（ウ）の規定によるほか、業務に支障が生じるおそれがない場合は、乙に保護すべき情報の返却、提出、破棄又は抹消を求めることができる。

3　乙は、前項の求めがあった場合において、保護すべき情報を引き続き保有する必要があるときは、その理由を添えて甲に協議を求めることができる。

別紙様式

情報セキュリティ対策実施確認事項

（事業名：　　）

1　下請負者名又は開示先事業者名等

(1) 事業者名：
(2) 委託又は開示予定年月日：
(3) 業務の実施予定場所※：

※（下請負事業者又は開示先事業者の業務の実施予定場所を記入）

2　下請負者又は開示先事業者に対する確認事項

※　確認事項欄の冒頭の番号及び用語の定義は、「調達における情報セキュリティ基準」（以下「本基準」という。）による。

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
1	**４（２）情報セキュリティ実施手順の周知** ・保護すべき情報を取り扱う可能性のある全ての者に周知することを定めていること。 ・下請負者へ周知することを定めていること。		
2	**４（３）情報セキュリティ実施手順の見直し** ・情報セキュリティ実施手順を定期的並びに重大な変化及び事故が発生した場合、見直しを実施し、必要に応じて変更することを定めていること。		
3	**５（１）ア　情報セキュリティに対する経営者等の責任** ・経営者等が情報セキュリティ実施手順を承認することを定めていること。 ・取扱者以外の役員（持分会社にあっては社員を含む。以下同じ。）、管理職員等を含む従業員その他の全ての構成員について、取扱者以外の者は保護すべき情報に接してはならないことを定めていること。 ・職務上の下級者等に対して、保護すべき情報の提供を要求してはならないことを定めていること。		
4	**５（１）イ　責任の割当て** ・総括責任者を置くことを定めていること。 ・管理責任者を置くことを定めていること。		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
5	**５（１）ウ　守秘義務及び目的外利用の禁止** ・取扱者との間で守秘義務及び目的外利用の禁止を定めた契約又は合意をすることを定めていること。 ・定期的並びに状況の変化及び事故が発生した場合、要求事項の見直しを実施し、必要に応じて修正することを定めていること。		
6	**５（１）エ　情報セキュリティの実施状況の調査** ・情報セキュリティの実施状況について、定期的及び重大な変化が発生した場合、調査を実施し、必要に応じて是正措置を取ることを定めていること。		
7	**５（２）保護すべき情報を取り扱う下請負者** ・保護すべき情報を取り扱う業務を他の業者に再委託する場合には、以下の事項を定めていること。 ①本基準に基づく情報セキュリティ対策の実施を契約上の義務とすること ②下請負者がその実施の確認をした上で、発注者（農林水産省との直接契約関係にある者をいう。以下同じ。）の確認を得た上で、発注者を経由して農林水産省に届け出ること。 ④情報セキュリティ対策に関して農林水産省が行う調査（職員又は指名する者の立入り、資料の閲覧等）に協力すること。 ⑤調査の結果、是正措置を求められた場合、速やかに当該措置を講じ、発注者に報告すること。		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
8	**５（３）ア　第三者への開示の禁止** ・第三者（法人又は自然人としての農林水産省と直接契約関係にある者以外の全ての者をいい、親会社、兄弟会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の農林水産省と直接契約関係にある者に対して指導、監督、業務支援、助言、監査等を行うものを含む。以下同じ。）への開示又は漏えいをしてはならないことを定めていること。 ・保有し、又は知り得た情報を第三者との契約において伝達、交換、共有その他提供する約定があるときは、保護すべき情報をその対象から除く措置を定めていること。 ・やむを得ず開示しようとする場合には、発注者が、開示先において本基準と同等の情報セキュリティが確保されることを確認した上で、農林水産省の許可を得ることを定めていること。		
9	**５（３）イ　第三者の取扱施設への立入りの禁止** ・第三者の取扱施設への立入りを認める場合、リスクを明確にした上で対策を定めていること。		
10	**６（１）　分類の指針** ・保護すべき情報を明確に分類できる分類体系を定めていること。		
11	**６（２）ア　保護すべき情報の目録** ・目録の作成及び維持を定めていること。		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
12	**６（２）イ　取扱いの管理策** ・取扱施設で取り扱うことを定めていること。 ・接受等を記録することを定めていること。 ・個人が所有する情報システム及び可搬記憶媒体で取り扱ってはならないことを定めていること。 ・（やむを得ない場合）事前に農林水産省の許可を得る手続を定めていること。 ・契約終了後、発注者から特段の指示がない限り、保護すべき情報を返却、提出、破棄又は抹消することを定めていること。 ・契約終了後も引き続き保護すべき情報を保有する必要がある場合には、その理由を添えて、発注者を経由して農林水産省に協議を求めることができることを定めていること。		
13	**６（２）ウ　保護すべき情報の保管等** ・保護すべき情報は、施錠したロッカー等において保管することを定めていること。 ・ロッカー等の鍵を適切に管理(無断での使用を防止)することを定めていること。		
14	**６（２）エ　保護すべき情報の持出し** ・持出しに伴うリスクを回避することができると判断する場合の判断基準を定めていること。 ・持ち出す場合は記録することを定めていること。		
15	**６（２）オ　保護すべき情報の破棄**及び抹消 ・復元できない方法による破棄又は抹消を定めていること。 ・破棄又は抹消したことを記録することを定めていること。		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
16	**６（２）カ　該当部分の明示** ・保護すべき情報を作成、製作又は複製した場合、保護すべき情報である旨の表示を行うことを定めていること。 ・契約の目的物が保護すべき情報を含むものである場合には、当該契約の履行の一環として収集、整理、作成等した一切の情報について、農林水産省が当該情報を保護すべき情報には当たらないと確認するまでは、保護すべき情報として取り扱うことを定めていること。 ・保護すべき情報の指定を解除する必要がある場合には、その理由を添えて、発注者を経由して農林水産省に協議を求めることができることを定めていること。 ・保護すべき情報を記録する箇所を明示する及び明示の方法を定めていること。		
17	**７（１）　経営者等の責任** ・経営者等は取扱者の指定の範囲を必要最小限とするとともに、ふさわしいと認める者を充て、情報セキュリティ実施手順を遵守させることを定めていること。 ・農林水産省との契約に違反する行為を求められた場合にこれを拒む権利を実効性をもって法的に保障されない者を当該ふさわしい者と認めないことを定めていること。		
18	**７（２）　取扱者名簿** ・以下の内容の取扱者名簿を作成又は更新し、発注者を経由して農林水産省に届け出て同意を得ることを定めていること。 ①取扱者名簿には、取扱者の氏名、生年月日、所属する部署、役職、国籍等が記載されていること。 ②取扱者名簿には、保護すべき情報に接する全ての者（保護すべき情報に接する役員（持分会社にあっては社員を含む。以下同じ。）、管理職員、派遣社員、契約社員、パート、アルバイト等を含む。この場合において、自らが保護すべき情報に接しているとの当該者の認識の有無を問わない。）が記載されていること。		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
19	**７（３）　取扱者の責任** ・在職中及び離職後においても、知り得た保護すべき情報を第三者に漏えいしてはならないことを定めていること。		
20	**７（４）　保護すべき情報の返却等** ・保護すべき情報に接する必要が無くなった場合は、管理者へ返却又は提出することを定めていること。		
21	**８（１）ア　取扱施設の指定** ・取扱施設（国内に限る。）を定めていること。		
22	**８（１）イ　物理的セキュリティ境界** ・物理的セキュリティ境界を用いることを定めていること。		
23	**８（１）ウ　物理的入退管理策** ・取扱施設への立入りは、許可された者だけに制限することを定めていること。		
24	**８（１）エ　取扱施設での作業** ・機密性に配慮し作業することを定めていること。 ・通信機器及び記録装置を利用する場合は、経営者等の許可を得ること定めていること。		
25	**８（２）ア　保護システムの設置及び保護** ・保護システムへの保護措置を実施することを定めていること。		
26	**８（２）イ　保護システムの持出し** ・持出しに伴うリスクを回避することができると判断する場合の基準を定めていること。 ・持出しする場合は記録することを定めていること。		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
27	**８（２）ウ　保護システムの保守及び点検** ・第三者による保守及び点検を行う場合は、必要な処置を実施することを定めていること。		
28	**８（２）エ　保護システムの破棄又は再利用** ・保護すべきデータが復元できない状態であることを点検し、物理的に破壊したのち、破棄し、その旨を記録することを定めていること。 ・復元できない状態であることを点検した後、再利用することを定めていること。		
29	**９（１）　操作手順書** ・操作手順書を整備し、維持することを定めていること。 ・操作手順書には、①可搬記憶媒体へ保存時の手順②可搬記憶媒体及び保護システムの破棄又は再利用の手順③電子メール等での伝達の手順④セキュリティに配慮したログオン手順についての記述又は引用がなされていること。		
30	**９（２）　悪意のあるコードからの保護** ・保護システムを最新の状態に更新されたウィルス対策ソフト等を用いて、少なくとも週１回以上フルスキャンを行うことなどにより、悪意のあるコードから保護することを定めていること。（なお、１週間以上電源の切られた状態にあるサーバ又はパソコン（以下「サーバ等」という。）については、再度の電源投入時に当該処置を行うことで可）		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
31	**９（３）　保護システムのバックアップの管理** ・可搬記憶媒体へのバックアップを実施する場合、調達における情報セキュリティ基準９（４）に添った取扱いをすることを定めていること。		
32	**９（４）ア　可搬記憶媒体の管理** ・保護すべき情報を保存した可搬記憶媒体を施錠したロッカー等により集中保管することを定めていること。 ・ロッカー等の鍵を適切に管理することを定めていること。 ・保護すべき情報とそれ以外を容易に区別できる処置をすることを定めていること。		
33	**９（４）イ　可搬記憶媒体への保存** ・可搬記憶媒体へ保存する場合、暗号技術を用いることを定めていること。		
34	**９（４）ウ　可搬記憶媒体の廃棄又は再利用** ・保護すべきデータが復元できない状態であることを点検し、物理的に破壊したのち、廃棄し、その旨を記録することを定めていること。 ・復元できない状態であることを点検した後、再利用することを定めていること。		
35	**９（５）ア　保護すべき情報の伝達** ・伝達に伴うリスクから保護できると判断する場合の基準を定めていること。		
36	**９（５）イ　伝達及び送達に関する合意** ・保護すべき情報の伝達及び送達は、守秘義務を定めた契約又は合意した相手に対してのみ行うことを定めていること。		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
37	**９（５）ウ　送達中の管理策** ・保護すべき文書等を送達する場合、許可されていないアクセス及び不正使用等から保護する方法を定めていること。		
38	**９（５）エ　保護すべきデータの伝達** ・保護すべきデータを伝達する場合には、保護すべきデータを既に暗号技術を用いて保存していること、通信事業者の回線区間に暗号技術を用いること又は電子メール等に暗号技術を用いることのいずれかによって、保護すべきデータを保護しなければならないことを定めていること（漏えいのおそれのない取扱施設内で有線での伝達をする場合を除く。）。		
39	**９（６）　外部からの接続** ・外部からの接続を許可する場合は、利用者の認証を行い、かつ、暗号技術を用いることを定めていること。		
40	**９（７）　電子政府推奨暗号等の利用** ・暗号技術を用いる場合には、電子政府推奨暗号等を用いることを定めていること。 ・やむを得ず電子政府推奨暗号等を使用できない場合は、その他の秘匿化技術を用いることを定めていること。		
41	**９（８）　ソフトウェアの導入管理** ・導入するソフトウェアの安全性を確認することを定めていること。		
42	**９（９）　システムユーティリティの使用** ・システムユーティリティの使用を制限することを定めていること。		
43	**９（10）　技術的脆弱性の管理** ・脆弱性に関する情報を取得すること及び適切に対処することを定めていること。		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
44	**9（11）ア　ログ取得** ・利用者の保護すべき情報へのアクセス等を記録したログを取得することを定めていること。		
45	**9（11）イ　ログの保管** ・取得したログを記録のあった日から少なくとも3か月以上保存するとともに、定期的に点検することを定めていること。		
46	**9（11）ウ　ログの保護** ・ログを改ざん及び許可されていないアクセスから保護することを定めていること。		
47	**9（11）エ　日付及び時刻の同期** ・保護システム及びネットワークを通じて保護システムにアクセス可能な情報システムの日付及び時刻を定期的に合わせることを定めていること。		
48	**9（11）オ　常時監視** ・保護システムがインターネットやインターネットと接点を有する情報システム（クラウドサービスを含む。）から物理的論理的に分離されていない場合には、常時監視を行うことを定めていること。		
49	**10（1）ア　利用者の登録管理** ・保護システムの利用者の登録及び登録削除をすることを定めていること。		
50	**10（1）イ　パスワードの割当て** ・初期又は仮パスワードは、容易に推測されないものとするとともに、機密性を配慮した方法で配付することを定めていること（パスワードより強固な手段を併用又は採用している場合はこの限りでない。）。		
51	**10（1）ウ　管理者権限の管理** ・管理者権限の利用は必要最低限とすることを定めていること。		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
52	**10（1）エ アクセス権の見直し** ・保護システムの利用者のアクセス権の割当てを定期的及び必要に応じて見直すことを定めていること。		
53	**10（2）ア　パスワードの利用** ・保護システムの利用者は、容易に推測されないパスワードを選択しなければならないことを定めていること（パスワードより強固な手段を併用又は採用している場合はこの限りでない。）。		
54	**10（2）イ　無人状態にある保護システム対策** ・保護システムが無人状態に置かれる場合、機密性を配慮した措置を実施することを定めていること。		
55	**10（3）ア　機能の制限** ・保護システムの利用者の職務内容に応じて、利用できる機能を制限することを定めていること。		
56	**10（3）イ　ネットワークの接続制御** ・保護システムを共有ネットワークへ接続する場合、接続に伴うリスクから保護することを定めていること（FW設置など）。		
57	**10（4）ア　セキュリティに配慮したログオン手順** ・保護システムの利用者は、セキュリティに配慮した手順でログオンすることを定めていること。		
58	**10（4）イ　利用者の識別及び認証** ・保護システムの利用者ごとに一意な識別子（ユーザーID、ユーザー名等）を保有させることを定めていること。		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
59	**10（4）ウ　パスワード管理システム** ・保護システムは、パスワードの不正使用を防止する機能を有さなければならないことを定めていること。		
60	**11（1）　情報セキュリティの事故等の報告** ・情報セキュリティ事故等に関する下記のそれぞれの事項について、以下のことが規定されていること。 ア　情報セキュリティ事故が発生したときは、適切な措置を講じるとともに、直ちに把握し得る限りの全ての内容を、その後速やかにその詳細を発注者に報告しなければならない。 イ　次の場合において､適切な措置を講じるとともに、直ちに把握し得る限りの全ての内容を、その後速やかにその詳細を発注者に報告しなければならない。 （ア）保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染又は不正アクセスが認められた場合 （イ）保護すべき情報が保存されているサーバ等と同一のイントラネットに接続されているサーバ等に悪意のあるコードへの感染又は不正アクセスが認められ、保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染又は不正アクセスのおそれがある場合 ウ　情報セキュリティ事故の疑い又は事故につながるおそれのある場合は、適切な措置を講じるとともに、速やかに､その詳細を発注者に報告しなければならない。 エ　アからウまでに規定する報告のほか、保護すべき情報の漏えい、紛失、破壊等の事故が発生した可能性又は将来発生する懸念について、内部又は外部から指摘があったときは、直ちに当該可能性又は懸念の真偽を含む把握し得る限りの全ての内容を、速やかに事実関係の詳細を発注者に報告しなければならない。		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
61	**11（2）ア　対処体制及び手順** ・情報セキュリティ事故（情報セキュリティ事故の疑いのある場合を含む。以下同じ。）及び事象に対処するため、対処体制、責任及び手順を定めていること。		
62	**11（2）イ　証拠の収集** ・情報セキュリティ事故が発生した場合（保護すべき情報が保存されたサーバ等に悪意のあるコードへの感染が認められた場合を含む。）、証拠を収集し、速やかに発注者へ提出することを定めていること。		
63	**11（2）ウ　情報セキュリティ実施手順への反映** ・情報セキュリティ実施手順の見直しに、情報セキュリティ事故及び事象を反映することを定めていること。		
64	**12（1）ア　遵守状況の確認** ・管理者の責任の範囲において、情報セキュリティ実施手順の遵守状況の確認を定めていること。		
65	**12（1）イ　技術的遵守状況の確認** ・保護システムの管理者の責任の範囲において、情報セキュリティ実施手順への技術的遵守状況を確認することを定めていること。		
66	**12（2）情報セキュリティの記録** ・保護すべき情報に係る重要な記録の保管期間を定めていること。 ・重要な記録は、施錠したロッカー等において保管又は暗号技術を用いる等厳密に保護することを定めていること。 ・適切に鍵を管理することを定めていること。		
67	**12（3）監査ツールの管理** ・保護システムの監査に用いるツールは、悪用を防止するため、必要最低限の使用にとどめることを定めていること。		

番号	確認事項	実施／未実施	実施状況の確認方法 又は未実施の理由
68	**12（4）農林水産省による調査** ・農林水産省による情報セキュリティ対策に関する調査を受け入れること及び必要な協力（職員又は指名する者の立入り、書類の閲覧等）をすることを定めていること。		
確認年月日： 確認者（企業名、所属、役職、氏名）：			

注：未実施の理由については、実施する必要がないと認められる合理的な理由を記すこと。