別紙様式第２３号

情報セキュリティ対策実施確認事項

令和　　年　　月　　日

国立研究開発法人

農業・食品産業技術総合研究機構

農業機械研究部門　所長　殿

コンソーシアム名：

* ***管理運営機関を設置している場合は、***

***管理運営機関***

代表機関名：

報告機関名：

報告者（役職）：

氏名：

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「情報セキュリティ基準」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。 |  |  |
| 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（国立研究開発法人農業・食品産業技術総合研究機構（以下、「農研機構」という。）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研機構に届け出ること。  ④情報セキュリティ対策に関して農研機構が行う調査（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。 |  |  |
| 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研機構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研機構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、開示先において情報セキュリティ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、農研機構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）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）事前に農研機構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研機構に協議を求めることができることを定めていること。 |  |  |
| 12 | 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。 |  |  |
| 13 | 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。 |  |  |
| 14 | 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。 |  |  |
| 15 | 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、農研機構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研機構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。 |  |  |
| 16 | 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。  ・農研機構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。 |  |  |
| 17 | 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研機構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。 |  |  |
| 18 | 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。 |  |  |
| 19 | 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。 |  |  |
| 20 | ８（１）ア　取扱施設の指定  ・取扱施設を定めていること。 |  |  |
| 21 | 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。 |  |  |
| 22 | 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。 |  |  |
| 23 | 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。 |  |  |
| 24 | 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。 |  |  |
| 25 | 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。 |  |  |
| 26 | 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。 |  |  |
| 27 | 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。 |  |  |
| 28 | 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。 |  |  |
| 29 | 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） |  |  |
| 30 | 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。 |  |  |
| 31 | 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。 |  |  |
| 32 | 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。 |  |  |
| 33 | 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。 |  |  |
| 34 | 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。 |  |  |
| 35 | 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。 |  |  |
| 36 | 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。 |  |  |
| 37 | 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。）。 |  |  |
| 38 | 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。 |  |  |
| 39 | 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。 |  |  |
| 40 | 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。 |  |  |
| 41 | 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。 |  |  |
| 42 | 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。 |  |  |
| 43 | 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。 |  |  |
| 44 | 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。 |  |  |
| 45 | 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。 |  |  |
| 46 | 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。 |  |  |
| 47 | 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。 |  |  |
| 48 | 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。 |  |  |
| 49 | 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。）。 |  |  |
| 50 | 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。 |  |  |
| 51 | 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。 |  |  |
| 52 | 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。）。 |  |  |
| 53 | 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。 |  |  |
| 54 | 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。 |  |  |
| 55 | 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）。 |  |  |
| 56 | 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。 |  |  |
| 57 | 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。 |  |  |
| 58 | 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。 |  |  |
| 59 | 11（１）　情報セキュリティインシデントの報告  ・情報セキュリティインシデント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　情報セキュリティインシデントが発生したときは、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　情報セキュリティインシデントの疑い又はインシデント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。 |  |  |
| 60 | 11（２）ア　対処体制及び手順  ・情報セキュリティインシデント（情報セキュリティインシデント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。 |  |  |
| 61 | 11（２）イ　証拠の収集  ・情報セキュリティインシデントが発生した場合（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。 |  |  |
| 62 | 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、情報セキュリティインシデント及び事象を反映することを定めていること。 |  |  |
| 63 | 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。 |  |  |
| 64 | 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。 |  |  |
| 65 | 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。 |  |  |
| 66 | 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。 |  |  |
| 67 | 12（４）農研機構による調査  ・農研機構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。 |  |  |
| 68 | 12（５）サービスレベルの保証  ・業務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は業務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報を取り扱う場合には、セキュリティ確保の観点から、システムの可用性、通信速度及び安定性、データの保存期間及び方法、データ交換の安全性及び信頼性確保のための方法、情報セキュリティインシデントの対処方法等を決定し、当該サービスレベルに関して保証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）： 　　　　　　　　　　　　印 | | | |

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。

***※　赤字の部分を削除し、情報管理統括責任者が確認の上、代表機関等を通じて提出すること***

**（管理運営機関を設置している場合は、「代表機関」を「管理運営機関」とし、管理運営機関を通じて提出すること）**