別紙９

調達における情報セキュリティ基準

１　趣旨

調達における情報セキュリティ基準（以下「本基準」という。）は、国立研究開発法人農業・食品産業技術総合研究機構生物系特定産業技術研究支援センター（以下「生研支援センター」という。）が行う調達を受注した法人（以下「受注者」という。）において当該調達に係る保護すべき情報の適切な管理を目指し、生研支援センターとして求める対策を定めるものであり、受注者は、情報セキュリティ対策を本基準に則り実施するものとする。

なお、従来から情報セキュリティ対策を実施している場合は、本基準に則り、必要に応じ新たに追加又は拡充を実施するものとする。また、本基準において示されている対策について、合理的な理由がある場合は、適用の除外について、生研支援センターの確認を受けることができる。

２　定義

本基準において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

（１）「保護すべき情報」とは、生研支援センターの業務に係る情報であって公になっていないもののうち、生研支援センター職員以外の者への漏えいが生研支援センターの試験研究又は業務の遂行に支障を与えるおそれがあるため、特に受注者における情報管理の徹底を図ることが必要となる情報をいう。

（２）「保護すべき文書等」とは、保護すべき情報に属する文書（保護すべきデータが保存された可搬記憶媒体を含む。）、図画及び物件をいう。

（３）「保護すべきデータ」とは、保護すべき情報に属する電子データをいう。

（４）「情報セキュリティ」とは、保護すべき情報の機密性、完全性及び可用性を維持することをいう。

（５）「機密性」とは、情報に関して、アクセスを許可された者だけがこれにアクセスできる特性をいう。

（６）「完全性」とは、情報が破壊、改ざん又は消去されていない特性をいう。

（７）「可用性」とは、情報へのアクセスを許可された者が、必要時に中断することなく、情報にアクセスできる特性をいう。

（８）「情報セキュリティ実施手順」とは、本基準に基づき、受注者が受注した業務に係る情報セキュリティ対策についての実施手順を定めたものをいう。

（９）「情報セキュリティ事故」とは、保護すべき情報の漏えい、紛失、破壊等

の事故をいう。
(10)「情報セキュリティ事象」とは、情報セキュリティ実施手順への違反のおそれのある状態及び情報セキュリティ事故につながるおそれのある状態をいう。
(11)「経営者等」とは、経営者又は生研支援センターが行う調達を処理する部門責任者をいう。
(12)「下請負者」とは、契約の履行に係る作業に従事する全ての事業者（生研支援センターと直接契約関係にある者を除く。）をいう。
(13)「第三者」とは、法人又は自然人としての生研支援センターと直接契約関係にある者以外の全ての者をいい、親会社等、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生研支援センター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。
(14)「親会社等」とは、会社法（平成 17 年法律第 86 号）第２条第４号の２に規定する「親会社等」をいう。
(15)「兄弟会社」とは、同一の会社を親会社とする子会社同士をいい、当該子会社は会社法第 847 条の２第２号に規定する「完全子会社」、会社計算規則（平成 18 年法務省令第 13 号）第２条第３項第 19 号に規定する「連結子会社」及び同項第 20 号に規定する「非連結子会社」をいう。
(16)「可搬記憶媒体」とは、パソコン又はその周辺機器に挿入又は接続して情報を保存することができる媒体又は機器のうち、可搬型のものをいう。
(17)「情報システム」とは、ハードウェア、ソフトウェア（プログラムの集合体をいう。）、ネットワーク又は記憶媒体で構成されるものであって、これら全体で業務処理を行うものをいう。
(18)「取扱施設」とは、保護すべき情報の取扱い及び保管を行う施設をいう。
(19)「保護システム」とは、保護すべき情報を取り扱う情報システムをいう。
(20)「利用者」とは、情報システムを利用する者をいう。
(21)「悪意のあるコード」とは、情報システムが提供する機能を妨害するプログラムの総称であり、コンピュータウイルス、スパイウェア等をいう。
(22)「伝達」とは、知識を相手方に伝えることであって、有体物である文書等の送達を伴わないものをいう。
(23)「送達」とは、有体物である文書等を物理的に移動させることをいう。
(24)「電子メール等」とは、電子メールの送受信、ファイルの共有及びファイルの送受信をいう。
(25)「電子政府推奨暗号等」とは、電子政府推奨暗号リストに記載されている暗号等又は電子政府推奨暗号選定の際の評価方法により評価した場合に電

子政府推奨暗号と同等以上の解読困難な強度を有する秘匿化の手段をいう。

(26)「秘匿化」とは、情報の内容又は情報の存在を隠すことを目的に、情報の変換等を行うことをいう。

(27)「管理者権限」とは、情報システムの管理（利用者の登録及び登録削除、利用者のアクセス制御等）をするために付与される権限をいう。

3　対象

（1）対象とする情報は、受注者において取り扱われる保護すべき情報とする。

（2）対象者は、受注者において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、派遣職員、契約社員、パート、アルバイト等を含む。この場合において、当該者が、自らが保護すべき情報に接しているとの認識の有無を問わない。以下「取扱者」という。）とする。

4　情報セキュリティ実施手順

（1）情報セキュリティ実施手順の作成受注者は、5から１２までの内容を含んだ情報セキュリティ実施手順を作成するものとし、その際及び変更する場合は、本基準との適合性について、生研支援センターの確認を受けるものとする。

（2）情報セキュリティ実施手順の周知

経営者等は、情報セキュリティ実施手順を、保護すべき情報を取り扱う可能性のある全ての者（取扱者を含む。）に周知しなければならない。また、保護すべき情報を取り扱う下請負者に周知しなければならない。

（3）情報セキュリティ実施手順の見直し

受注者は、情報セキュリティ実施手順を適切、有効及び妥当なものとするため、定期的な見直しを実施するとともに、情報セキュリティに係る重大な変化及び情報セキュリティ事故が発生した場合は、その都度、見直しを実施し、必要に応じて情報セキュリティ実施手順を変更しなければならない。

5　組織のセキュリティ

（1）内部組織

ア　情報セキュリティに対する経営者等の責任

経営者等は、情報セキュリティの責任に関する明瞭な方向付け、自らの関与の明示、責任の明確な割当て及び情報セキュリティ実施手順の承認等を通して、組織内における情報セキュリティの確保に不断に努めるものとし、組織内において、取扱者以外の役員、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ず、かつ、職務上の下級者等に対してその提供を要求してはならない。

イ　責任の割当て

受注者は、保護すべき情報に係る全ての情報セキュリティの責任を明確化するため、保護すべき情報の管理全般に係る総括的な責任者及び保護すべき情報ごとに管理責任者（以下「管理者」という。）を指定しなければならない。

ウ　守秘義務及び目的外利用の禁止

受注者は、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ものとし、要求事項の定期的な見直しを実施するとともに、情報セキュリティに係る状況の変化及び情報セキュリティ事故が発生した場合は、その都度、見直しを実施した上、必要に応じて要求事項を修正しなければならない。

エ　情報セキュリティの実施状況の調査

受注者は、情報セキュリティの実施状況について、定期的及び情報セキュリティの実施に係る重大な変化が発生した場合には、調査を実施し、その結果を保存しなければならない。また、必要に応じて是正措置を取らなければならない。

（２）保護すべき情報を取り扱う下請負者

受注者は、当該契約の履行に当たり、保護すべき情報を取り扱う業務を下請負者に委託する場合、本基準に基づく情報セキュリティ対策の実施を当該下請負者との間で契約し、当該業務を始める前に、生研支援センターが定める確認事項に基づき、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た後、生研支援センターに届け出なければならない。

（３）第三者への開示の禁止

ア　第三者への開示の禁止

受注者は、第三者（当該保護すべき情報を取り扱う業務に係る契約の相手方を除く。）に保護すべき情報を開示又は漏えいしてはならない。やむを得ず保護すべき情報を第三者（当該保護すべき情報を取り扱う業務に係る契約の相手方を除く。）に開示しようとする場合には、あらかじめ、生研支援センターが定める確認事項に基づき、開示先において情報セキュリティが確保されることを確認した後、書面により生研支援センターの許可を受けなければならない。

イ　第三者の取扱施設への立入りの禁止

受注者は、想定されるリスクを明確にした上で、当該リスクへの対策を講じた場合を除き、取扱施設に第三者を立ち入らせてはならない。

6　保護すべき情報の管理

（１）分類の指針

受注者は、保護すべき情報を明確に分類することができる情報の分類体系を定めなければならない。

（２）保護すべき情報の取扱い

ア　保護すべき情報の目録

受注者は、保護すべき情報の現状（保管場所等）が分かる目録を作成し、維持しなければならない。

イ　取扱いの管理策

（ア）受注者は、保護すべき情報を接受、作成、製作、複製、持出し（貸出しを含む。）、破棄又は抹消する場合は、その旨を記録しなければならない。

（イ）受注者は、保護すべき情報を個人が所有する情報システム及び可搬記憶媒体において取り扱ってはならず、やむを得ない場合は、あらかじめ、書面により生研支援センターの許可を得なければならない。

（ウ）受注者は、生研支援センターから特段の指示がない限り、契約終了後、保護すべき情報を返却、提出、破棄又は抹消しなければならない。ただし、当該情報を引き続き保有する必要があるときは、その理由を添えて生研支援センターに協議を求めることができる。

ウ　保護すべき情報の保管等

受注者は、保護すべき情報を施錠したロッカー等に保管し、その鍵を適切に管理しなければならない。また、保護すべき情報を保護すべきデータとして保存する場合には、暗号技術を用いることを推奨する。

エ　保護すべき情報の持出し

受注者は、経営者等が持出しに伴うリスクを回避することができると判断した場合を除き、保護すべき情報を取扱施設外に持ち出してはならない。

オ　保護すべき情報の破棄及び抹消

受注者は、接受、作成、製作又は複製した保護すべき情報を復元できないように細断等確実な方法により破棄又は抹消し、その旨を記録するものとする。なお、保護すべきデータを保存した可搬記憶媒体を廃棄する場合も同様とする。

カ　該当部分の明示

（ア）受注者は、保護すべき情報を作成、製作又は複製した場合は、下線若しくは枠組みによる明示又は文頭及び文末に括弧を付すことによる明示等の措置を行うものとする。

（イ）受注者は、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、生研支援センター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わなければならない。ただし、保護すべき情報の指定を解除する必要がある場合には、その理由を添えて生研支援センターに協議を求めることができる。

7　人的セキュリティ

（1）経営者等の責任

経営者等は、保護すべき情報の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なければならない。また、生研支援センター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と認める者としてはならない。

（2）取扱者名簿

受注者は、取扱者名簿（取扱者の氏名、生年月日、所属する部署、役職、国籍等が記載されたものをいう。以下同じ。）を作成又は更新し、その都度、保護すべき情報を取り扱う前に生研支援センターに届け出て同意を得なければならない。また、受注者は、下請負者及び保護すべき情報を開示する第三者の取扱者名簿についても、同様の措置を取らなければならない。

（3）取扱者の責任

取扱者は、在職中及び離職後において、契約の履行において知り得た保護すべき情報を第三者（当該保護すべき情報を取り扱う業務に係る契約の相手方を除く。）に漏えいしてはならない。

（4）保護すべき情報の返却等

受注者は、取扱者の雇用契約の終了又は取扱者との契約合意内容の変更に伴い、保護すべき情報に接する必要がなくなった場合には、取扱者が保有する保護すべき情報を管理者へ返却又は提出させなければならない。

8　物理的及び環境的セキュリティ

（1）取扱施設

ア　取扱施設の指定

受注者は、保護すべき情報の取扱施設（日本国内に限る。）を明確に定めなければならない。

イ　物理的セキュリティ境界

受注者は、保護すべき情報及び保護システムのある区域を保護するために、物理的セキュリティ境界（例えば、壁、カード制御による入口、有人

の受付）を用いなければならない。

ウ　物理的入退管理策

受注者は、取扱施設への立入りを適切な入退管理策により許可された者だけに制限するとともに、取扱施設への第三者の立入りを記録し、保管しなければならない。

エ　取扱施設での作業

受注者は、保護すべき情報に係る作業は、機密性に配慮しなければならない。また、取扱施設において通信機器（携帯電話等）及び記録装置（ボイスレコーダー及びデジカメ等）を利用する場合は、経営者等の許可を得なければならない。

（２）保護システムの物理的保全対策

ア　保護システムの設置及び保護

受注者は、保護システムを設置する場合、不正なアクセス及び盗難等から保護するため、施錠できるラック等に設置又はワイヤーで固定する等の措置を取らなければならない。

イ　保護システムの持出し

受注者は、経営者等が持出しに伴うリスクを回避することができると判断した場合を除き、保護システムを取扱施設外に持ち出してはならない。

ウ　保護システムの保守及び点検

受注者は、第三者により保護システムの保守及び点検を行う場合、必要に応じて、保護すべき情報を復元できない状態にする、又は取り外す等の処置をしなければならない。

エ　保護システムの破棄又は再利用

受注者は、保護システムを破棄する場合は、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た上、記憶媒体を物理的に破壊した後、破棄し、その旨を記録しなければならない。また、再利用する場合は、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た後でなければ再利用してはならない。

９　通信及び運用管理

（１）操作手順書

受注者は、保護システムの操作手順書を整備し、維持するとともに、利用者が利用可能な状態にしなければならない。

（２）悪意のあるコードからの保護

受注者は、保護システムを最新の状態に更新されたウイルス対策ソフトウェア等を用いて、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しなければならない。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ものとする。

（３）保護システムのバックアップの管理

受注者は、保護システムを可搬記憶媒体にバックアップする場合、可搬記憶媒体は（４）に沿った取扱いをしなければならない。

（４）可搬記憶媒体の取扱い

ア　可搬記憶媒体の管理

受注者は、保護すべきデータを保存した可搬記憶媒体を施錠したロッカー等において集中保管し、適切に鍵を管理しなければならない。また、可搬記憶媒体は、保護すべき情報とそれ以外を容易に区別できる処置をしなければならない。

イ　可搬記憶媒体への保存

受注者は、保護すべきデータを可搬記憶媒体に保存する場合、暗号技術を用いなければならない。ただし、生研支援センターへの納入又は提出物件等である場合には、生研支援センターの指示に従うものとする。

ウ　可搬記憶媒体の廃棄又は再利用

受注者は、保護すべきデータの保存に利用した可搬記憶媒体を廃棄する場合、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た上、可搬記憶媒体を物理的に破壊した後、廃棄し、その旨を記録しなければならない。また、再利用する場合は、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た後でなければ再利用してはならない。

（５）情報の伝達及び送達

ア　保護すべき情報の伝達

受注者は、通信機器（携帯電話等）を用いて保護すべき情報を伝達する場合、伝達に伴うリスクを経営者等が判断の上、必要に応じそのリスクから保護しなければならない。

イ　伝達及び送達に関する合意

受注者は、保護すべき情報を伝達又は送達する場合には、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わなければならない。

ウ　送達中の管理策

受注者は、保護すべき文書等を送達する場合には、送達途中において、許可されていないアクセス及び不正使用等から保護しなければならない。

エ　保護すべきデータの伝達

受注者は、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。ただし、漏えいのおそれがないと認められる取扱施設内において、有線で伝達が行われる場合は、この限りでない。

（６）外部からの接続

受注者は、保護システムに外部から接続（モバイルコンピューティング、テレワーキング等）を許可する場合は、利用者の認証を行うとともに、暗号技術を用いなければならない。

（７）電子政府推奨暗号等の利用

受注者は、暗号技術を用いる場合、電子政府推奨暗号等を用いなければならない。なお、電子政府推奨暗号等を用いることが困難な場合は、その他の秘匿化技術を用いる等により保護すべき情報を保護しなければならない。

（８）ソフトウェアの導入管理

受注者は、保護システムへソフトウェアを導入する場合、あらかじめ当該システムの管理者によりソフトウェアの安全性の確認を受けなければならない。

（９）システムユーティリティの使用

受注者は、保護システムにおいてオペレーティングシステム及びソフトウェアによる制御を無効にすることができるシステムユーティリティの使用を制限しなければならない。

(10) 技術的脆弱性の管理

受注者は、技術的脆弱性に関する情報について時期を失せず取得し、経営者等が判断の上、適切に対処しなければならない。

(11) 監視

ア　ログの取得

受注者は、保護システムにおいて、保護すべき情報へのアクセス等を記録したログを取得しなければならない。

イ　ログの保管

受注者は、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、定期的に点検しなければならない。

ウ　ログの保護

受注者は、ログを改ざん及び許可されていないアクセスから保護しなければならない。

エ　日付及び時刻の同期

受注者は、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なければなら

ない。

オ　常時監視

受注者は、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。）から物理的又は論理的に分離されていない場合は、常時監視を行わなければならない。

10　アクセス制御

（1）利用者の管理

ア　利用者の登録管理

受注者は、取扱者による保護システムへのアクセスを許可し、適切なアクセス権を付与するため、保護システムの利用者としての登録及び登録の削除をしなければならない。

イ　パスワードの割当て

受注者は、保護システムの利用者に対して初期又は仮パスワードを割り当てる場合、容易に推測されないパスワードを割り当てるものとし、機密性に配慮した方法で配付するものとする。なお、パスワードより強固な手段（生体認証等）を採用又は併用している場合は、本項目の適用を除外することができる。

ウ　管理者権限の管理

保護システムの管理者権限は、必要最低限にとどめなければならない。

エ　アクセス権の見直し

受注者は、保護システムの利用者に対するアクセス権の割当てについては、定期的及び必要に応じて見直しを実施しなければならない。

（2）利用者の責任

ア　パスワードの利用

受注者は、容易に推測されないパスワードを保護システムの利用者に設定させ、当該パスワードを複数の機器やサービスで再使用させないとともに、流出時には直ちに変更させなければならない。なお、パスワードより強固な手段（生体認証等）を採用又は併用している場合は、本項目の適用を除外することができる。

イ　無人状態にある保護システム対策

受注者は、保護システムが無人状態に置かれる場合、機密性に配慮した措置を取らなければならない。

（3）ネットワークのアクセス制御

ア　機能の制限

受注者は、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

を制限し提供しなければならない。

イ　ネットワークの接続制御

受注者は、保護システムの共有ネットワーク（インターネット等）への接続に際しては、接続に伴うリスクから保護しなければならない。

（４）オペレーティングシステムのアクセス制御

ア　セキュリティに配慮したログオン手順

受注者は、利用者が保護システムを利用する場合、セキュリティに配慮した手順により、ログオンさせなければならない。

イ　利用者の識別及び認証

受注者は、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）を保有させなければならない。

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（パスワードの再使用を防止する機能等）を有さなければならない。

11　情報セキュリティ事故等の管理

（１）情報セキュリティ事故等の報告

ア　受注者は、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、直ちに把握しうる限りの全ての内容を、その後速やかに詳細を生研支援センターに報告しなければならない。

イ　次に掲げる場合において、受注者は、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、その後速やかに詳細を生研支援センター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、受注者は、適切な措置を講じるとともに、速やかにその詳細を生研支援センター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受注者の内部又は外部から指摘があったときは、受注者は、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

細を生研支援センターに報告しなければならない。

（２）情報セキュリティ事故等の対処等

ア　対処体制及び手順

受注者は、情報セキュリティ事故、その疑いのある場合及び情報セキュリティ事象に対処するため、対処体制、責任及び手順を定めなければならない。

イ　証拠の収集

受注者は、情報セキュリティ事故が発生した場合、その疑いのある場合及び（１）イ（ア）の場合は証拠を収集し、速やかに生研支援センターに提出しなければならない。

ウ　情報セキュリティ実施手順への反映

受注者は、発生した情報セキュリティ事故、その疑いのある場合及び情報セキュリティ事象を情報セキュリティ実施手順の見直し等に反映しなければならない。

12 遵守状況等

（１）遵守状況の確認等

ア　遵守状況の確認

受注者は、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を確認しなければならない。

イ　技術的遵守状況の確認

受注者は、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しなければならない。

（２）情報セキュリティの記録

受注者は、保護すべき情報に係る重要な記録（複製記録、持出記録、監査記録等）の保管期間（少なくとも契約履行後１年間）を定めた上、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により厳密に保護するとともに、適切に鍵を管理しなければならない。

（３）監査ツールの管理

受注者は、保護システムの監査に用いるツールについて、悪用を防止するため必要最低限の使用にとどめなければならない。

（４）生研支援センターによる調査

ア　調査の受入れ

受注者は、生研支援センターによる情報セキュリティ対策に関する調査の要求があった場合には、これを受け入れなければならない。

イ　調査への協力

受注者は、生研支援センターが調査を実施する場合、生研支援センター

の求めに応じ必要な協力（職員又は生研支援センターの指名する者の取扱施設への立入り、書類の閲覧等への協力）をしなければならない。