Ⅱ－4　情報管理の適正化

（※本取扱いは令和2年1月以降、新たに公募するものから適用となります。）

(1)概要

受注企業のグローバル化が進む中、情報管理の徹底を図る観点から、農林水産省において「農林水産省が行う調達における情報管理の適正化について」を策定し、農林水産省大臣官房参事官（経理）、同検査・監察部長名で令和元年9月に発出され、本通知の趣旨を踏まえ、各法人の調達における情報管理の強化を図ることを要請されました。

この通知を受け、次の①～④を主な内容とする生研支援センターが行う調達における情報管理の適正化について、新たに通知を定め、調達における情報管理の強化を図ることとしました。

① 情報管理の必要な調査研究等に係る契約について、入札者の情報管理体制の事前スクリーニング
② 契約時に受注者の情報セキュリティ実施手順の作成や除法取扱者名簿の提出
③ 保護すべき情報について人的、物理的、環境的セキュリティの確保
④ 契約の履行中及び履行後を問わず、必要に応じて調査・監査の実施

(2)本業務に関する要求

① 本業務の実施体制

構成員は、本業務の実施に当たって次の体制を確保し、これを変更する場合には、事前に生研支援センターと協議するものとします。

ア 契約の履行に必要な情報を取り扱うにふさわしい、契約を履行する業務に従事する情報管理統括責任者又は情報管理責任者（以下「情報管理責任者等」という。）を確保すること

イ 情報管理責任者等が業務の要求する特定の経験、資格、業績等を有すること

ウ 情報管理責任者等が、イに掲げるもののほか、契約の履行に必要若しくは有用な、又は背景となる経歴、知見、資格、語学（母語及び外国語能力）、文化的背景（国籍等）、業績等を有すること

エ 情報管理責任者等が他の手持ち業務等との関係において契約の履行に必要な業務所要に対応できる体制にあること

② 情報保全

構成員は、本業務に係る契約の履行に際し知り得た保護すべき情報（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、特に構成員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。以下同じ。）の取扱いに当たっては、「調達における情報セキュリティ基準」（以下「本基準」という。）及び【特記事項】「調達における情報セキュリティの確保に関する特約事項」（以下「情報セキュリティ特約条項」という。）に基づき、適切に管理するものとします。この際、特に、保護すべき情報の取扱いについては、次の情報管理実施体制を確保し、これを変更した場合には、遅滞なく生研支援センターに通知するものとします。

ア 契約を履行する一環として構成員が収集、整理、作成等した一切の情報が、生研支援センターが保護を要さないと確認するまでは保護すべき情報として取り扱われることを保障す

る履行体制

イ 生研支援センターの同意を得て指定した取扱者以外の者に取り扱わせないことを保障する履行体制

ウ 生研支援センターが書面により個別に許可した場合を除き、構成員に係る親会社等(本基準第2項第 14 号に規定する「親会社等」をいう。)、兄弟会社(本基準第2項第 15 号に規定する「兄弟会社」をいう。)、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構成員に対して指導、監督、業務支援、助言、監査等を行う者を含む一切の構成員以外の者に対して伝達又は漏えいされないことを保障する履行体制

③ 構成員に要求される事項

構成員は、上記①及び②の事項を踏まえて「情報管理実施体制(様式Ⅵ－2)」、「情報管理経歴書(様式Ⅵ－3)」を生研支援センターへ提出するものとします。

また、本基準及び情報セキュリティ特約条項第8条に規定する「情報セキュリティ実施手順」(情報セキュリティ対策実施確認事項(様式Ⅵ－1))については、契約締結後にその遵守状況について確認し、生研支援センターへ提出するものとします。

なお、構成員は、提出した資料に関し、説明、質問への回答、追加資料の提出、及び生研支援センターとの協議等に応じる義務を負うものとします。

(1) 業務従事者リストの提出(「情報管理統括責任者」「情報管理責任者」)
…… ……「(様式Ⅵ-2)情報管理実施体制」

(2) (1)に係る経歴資料の提出 ……「(様式Ⅵ-3)情報管理経歴書」

(3) 情報セキュリティ実施手順の作成 ‥「(様式Ⅵ-1)情報セキュリティ対策実施確認事項」

	情報管理統括責任者	情報管理責任者	経 歴 書	情報セキュリティ実施手順作成
代表機関	○	○	○	○
構成員	不要	○	○	○
提出様式	様式Ⅵ-2		様式Ⅵ-3	様式Ⅵ-1
根拠条文	第 1 条 第 1 項 (調達における情報セキュリティ基準)			
(特記事項3)	5.組織のｾｷｭﾘﾃｨ － ｲ.責任の割当て)			4.情報ｾｷｭﾘﾃｨ実施手順

(情報管理適正化に係る提出資料の補足説明((2)③関係))

ア 【様式Ⅵ－1】[構成員で作成、代表機関等を通じて提出]

・契約締結(変更契約含む)後に、その遵守状況の確認を行い、作成の上、生研支援センターへ提出してください。

イ 【様式Ⅵ－2】[代表機関等で作成]

契約締結(変更契約含む)時に、情報管理実施体制を作成の上、生研支援センターへ提出してください。

・情報管理統括責任者は代表機関等の職員で当該プロジェクト全体の情報管理の総責任者であり、情報管理責任者は各構成員が担当する研究課題の情報管理全般の責任者です。いずれも日頃情報管理を担当している職員を想定しています。

・情報管理統括責任者と情報管理責任者を兼ねることは可能です。
・情報管理責任者等については、各構成員における組織上の然るべき職員であれば、特別な資格、条件は必要ありません。

ウ【様式Ⅵ－3】[構成員で作成、代表機関等を通じて提出]

契約締結(変更契約含む)時に、情報管理実施体制で定めた情報管理責任者等の情報管理経歴書を作成の上、生研支援センターへ提出してください。
・特別な資格、条件は必要ありませんが、情報管理に関する資格や経歴等を有している場合は記載してください。
・情報管理統括責任者が情報管理責任者を兼ねる場合は、情報管理経歴書に「○○(構成員)の情報管理責任者を兼ねる」旨を明記してください。

（別添1）

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事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。

【特記事項】 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　乙構成員は、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乙代表機関を通じ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　乙構成員は、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乙代表機関を通じて甲の確認を受けなければならない。
3　甲は、乙構成員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　乙構成員は、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　乙構成員は、乙構成員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（乙構成員を除く。）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　乙構成員は、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「情報セキュリティ対策実施確認事項（様式Ⅵ－1）」に定める確認事項により確認した上で、書面により乙代表機関を通じて甲の許可を受けなければならない。
2　乙構成員は、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　乙構成員は、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、「情報セキュリティ対策実施確認事項（様式Ⅵ－1）」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、その結果を乙代表機関を通じて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構成員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、委託業務におけ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構成員の事業所、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、乙構成員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　乙構成員は、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　乙構成員は、甲が乙構成員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、乙構成員は、乙構成員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乙代表機関を通じ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　乙構成員は、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乙代表機関を通じて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、乙構成員は、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乙代表機関を通じて甲に報告しなければならない。
　一　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
　二　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、乙構成員は、適切な措置を講じるとともに、速やかにその詳細を乙代表機関を通じて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構成員の内部又は外部から指摘があったときは、乙構成員は、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乙代表機関を通じて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　乙構成員は、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構成員の責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、乙構成員の負担とする。
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、乙構成員の責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9条、第10条、第12条及び第13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、乙構成員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　乙構成員は、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、その理由を添えて乙代表機関を通じて甲に協議を求めることができる。

（様式Ⅵ－１（情報管理関係））

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。		
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、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。）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、生研支援センターに届け出ること。 ④情報セキュリティ対策に関して生研支援センターが行う調査（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、生研支援センターに報告すること。		

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。

情報セキュリティ対策実施確認事項

（事業名：　　）

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、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。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、生研支援センターが、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、生研支援センター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。		
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）事前に生研支援センターの許可を得る手続を定めていること。 ・契約終了後、生研支援センター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、生研支援センター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。		

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。

情報セキュリティ対策実施確認事項

（事業名：　　）

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、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、生研支援センター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。 ・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、生研支援センター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。		
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。		

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。

情報セキュリティ対策実施確認事項

（事業名：　　）

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
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。		
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）		
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。		

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。

情報セキュリティ対策実施確認事項

（事業名：　　）

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。		
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。		

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。

情報セキュリティ対策実施確認事項

（事業名：　　）

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
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。		
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。		
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。		

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。

情報セキュリティ対策実施確認事項

（事業名：　　）

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
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生研支援センター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、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、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生研支援センターに報告しなければならない。		
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、速やかに生研支援センター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。		

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。

情報セキュリティ対策実施確認事項

（事業名：　　）

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
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。		
68	**12（4）生研支援センターによる調査** ・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）：

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。

（**様式Ⅵ－２（情報管理関係）**）

情報管理実施体制

【代表機関：　　】
情報管理統括責任者
役職：
氏名：

情報管理責任者
役職：
氏名：

- 【共同研究機関：　　】
  情報管理責任者
  役職：
  氏名：
- 【共同研究機関：　　】
  情報管理責任者
  役職：
  氏名：
- 【共同研究機関：　　】
  情報管理責任者
  役職：
  氏名：

（様式Ⅵ－３（情報管理関係））

情報管理経歴書

氏　名		生年月日	年　月　日 （　歳）
①所属及び役職			
②学歴及び職歴 ・ ・ ・ ・			
③情報管理に関する業務経験、研修実績、専門的知識・知見（資格等）、 その他特筆すべき事項 ・ ・ ・			