情報セキュリティ要件

令和８年１月１日

国立研究開発法人物質・材料研究機構
情報基盤統括部門

改訂履歴

版*	改訂年月日(yyyy/mm/dd)	改訂箇所(p. 内容)	改訂内容
1.0.0	2026/1/1	全般	全面改訂

目次

1.目的・趣旨

1.1 目的

機構外の者に、調査・研究等の業務を委託、あるいは情報システムやアプリケーションプログラムの開発・運用・保守等を委託する際に、委託先に提供する要保護情報等を適切に保護するための情報セキュリティ対策が確実に実施されるよう、委託する業務の範囲や委託先の責任範囲等を明確化し、要求事項を調達仕様書等に定め契約条件とすることを目的とする。

1.2 対象となる業務委託

調査・研究等の業務を委託、あるいは情報システムやアプリケーションプログラムの開発・運用・保守など以下を例とした業務委託とする。

＜業務委託の例＞

- 情報システムの開発及び構築業務の委託
- アプリケーション・コンテンツの開発業務の委託
- 情報システムの運用業務の委託
- 業務運用支援業務（統計、集計、データ入力、媒体変換等）の委託
- プロジェクト管理支援業務の委託
- 調査・研究業務（調査、研究、検査等）の委託
- ウェブサイトの運用業務の委託
- この他、機構の要機密情報を取り扱う業務の委託

1.3 守秘義務

受注者は、本業務の内容及び本業務に関連して開示を受けた又は知り得た相手方の技術的もしくは事業運営に係る一切の情報（以下、「機密情報」という。）につき最大限の注意をもって秘密を保持し、事前に機構の書面による承諾を受けることなく、本業務の目的外で使用し、又は第三者に開示・漏えいしてはならない。また、受注者は、自社の従業員を含む本業務に従事する関係者（以下、「関係者」という。）にのみ機密情報を開示するものとし、本業務に関与しない者には、いかなる手段においても一切機密情報を開示し又は使用させてはならない。なお、受注者が機構より機密情報を受け取り、取り扱う場合には、本業務の実施完了後、本業務に関する情報を返却又は確実に破棄すること。

1.4 個人情報の取扱い

本業務の実施にあたっては、個人情報の保護に関する法令や規範を遵守するとともに、個人情報の保護の重要性を認識し、個人の権利又は利益を侵害することのないよう、個人情報の取扱いを適正に行うこと。

2.情報セキュリティ管理

受注者は、以下の情報セキュリティ管理事項を遵守すること。

2.1 要求事項

本業務に関する情報セキュリティについては、受注者において、設定不可能な場合や意味をなさない項目を除き、下記事項の実施、又は対策を行うこと。また、機構の求めに応じ対策内容を提出しその承認を得ること（要機密情報を取り扱う場合には必須とする）。

(1) 受注者に提供する情報の目的外利用の禁止

(2) 受注者における情報セキュリティ対策の実施及び管理体制の構築

① 委託業務の実施にあたり、受注者又はその従業員、再委託先、もしくはその他の者による意図せざる変更が加えられないための管理体制の構築

② 受注者、受注作業実施場所、及び受注業務従事者に関する情報提供

③ 受注者の資本関係・役員等の情報、委託業務の実施場所、委託業務従事者の所属・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提供

(3) 情報セキュリティインシデントへの対処方法

① 情報セキュリティインシデント対応のための実施体制、連絡先

(4) 再委託先における情報セキュリティ対策

① 受注者が本調達に係る業務を一部再委託する場合、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、受注者に求める情報セキュリティ対策と同等の措置内容を再委託にも実施させるとともに、機構の求めに応じて再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機構に提供し承認を受けること。

② 「再委託先」には、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、多段階の委託が行われる場合の委託先を含む。

2.2 情報セキュリティ監査、及び対策状況の確認と対処

(1) 情報セキュリティ監査、および情報セキュリティ対策とその他の契約の履行状況の確認

① 機構は、本調達に係る機構情報に関するセキュリティ対策の履行状況を確認するため、必要と判断した場合、情報セキュリティ監査を実施できるものとする。監査内容、対象範囲、実施方法（監査基準の概要、実施場所等）は、要求担当者と受注者が事前に調整したうえで要求担当者が定める。

② 受注者が、上記履行状況の確認を含む第三者による監査を実施した場合、当該監査結果のうち該当部分を機構に報告することで、機構による監査に代えることができる。

③ 監査の対象範囲、実施者（機構指定の第三者、受注者選定の第三者、または両者の独立部門）、実施方法等については、受注者の負担や機構の情報セキュリティ規程、及び情報セキュリティ対策基準との整合性を考慮し、事前に機構と受注者が協議の上、合意するものとする。

④ 委託先への立入検査または情報セキュリティ監査を実施する場合、対象範囲、実施者、

方法等を、事前に機構と受注者が協議の上、定めるものとする。

(2) 情報セキュリティ対策の履行が不十分な場合の対処

① 受注者は、本調達に係る機構情報のセキュリティ対策の履行状況について、機構が改善を求めた場合には、機構と協議の上、必要な改善策を立案し速やかに実施すること。

2.3 セキュリティ管理実施内容

(1) 本業務において使用する機器、およびソフトウェア等

① 受注者は、本調達で機構に納める（又は履行で用いる）機器やソフトウェアについて、また、役務の履行を行う場合はそれらに関わる者について、日本の国益を損なう国の諜報活動や情報収集活動に関与していないことを保証できるものを受注者の責任において選定及び採用すること。

② 本調達において利用、もしくは機構に納める機器やソフトウェアについては、既知の脆弱性が存在しない、又は存在しても製造元より無償で対策等が提供されるものとすること。

(2) 私物端末及び私物媒体等の使用禁止

① 受注者は、本調達に係る業務を実施するすべての関係者に対し、原則、私物（関係者個人の所有物等、受注者管理外のものを指す。）のコンピュータ等端末及び電子記録媒体（USBメモリ等）に機構の情報を保存すること、及び本調達に係る業務を私物コンピュータ等端末において実施することを禁止すること。また、機構の情報を取り扱う端末や媒体等を管理し、機構が要求した場合には管理簿を提出すること。

(3) 外部とのデータ授受（メール、インターネット、媒体等）

① 本業務でデータを授受するにあたっては、授受手順を明確化したうえで機構に申請し、承認を得た上で作業を実施すること。

② データの授受にあたっては、データ暗号化、パスワード設定およびウイルスチェックの実施等のセキュリティ対策を施こすこと。

(4) クラウドサービス等の利用について

① 本業務遂行にあたりクラウドサービス等を利用する場合は、事前に利用するクラウドサービス名、その使用目的、業務内容、利用者などを機構に申請し、承認を得た上で使用すること。

② クラウドサービス等の利用に係る遵守状況を定期的に確認し、機構の求めに応じてその結果を報告すること。

③ ChatGPT等生成AIを使用する場合は以下を遵守し、生成された回答内容は受注者が責任を負うこと。

1) 要機密情報を入力しないこと。

2) 入力した情報を学習させる設定を無効にすること。

(5) 外部電磁記憶媒体の管理について

① 本業務遂行にあたり、外部電磁記憶媒体（USBメモリ、スマホ、SDカード、DVD等）の使用は禁止する。ただし業務上不可欠な場合に限り、機構の承認を受けることおよび外部電磁記憶媒体自体又はデータにパスワードを設定することを条件として使用を認める。使用範囲は本業務及び本業務において使用するPCのみとし、使用後は当該データを削除すること。

② 管理責任者は、外部電磁記憶媒体を施錠したキャビネット等で保管すること。

③ 関係者への貸出し、返却にあたって、貸出管理簿に、貸出（返却）日時、貸出者、可搬型外部記憶媒体の識別Noを記載すること。

(6) アクセスを認められた機構が管理する情報システムについて、アクセス者は本業務の関係者のみとし、認められていない者へのアクセス権限の提供は行わないこと。

(7) 情報へアクセスする主体の識別とアクセスの制御、およびログの取得・監視について

① 取り扱う情報について、主体認証やその属性ごとにアクセス制御を行い、管理者権限を持つ場合には必要最低限の権限と利用に制限した上で、ログを取得すること。

② 可能な限り特権アカウントへのアクセスには多要素主体認証を採用すること。

③ リモートアクセス時や無線LAN利用時には、通信の暗号化、認証、監視などの対策を行うこと。

④ 強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用すること、初期パスワードを必ず変更するなど主体認証情報に関する対策を行うこと。

(8) データの持ち出し

① PCおよび可搬型外部記憶媒体などによりデータを外部に持ち出す場合は、機構に申請し承認を受けること。その際、データ暗号化、パスワード設定等のセキュリティ対策を施すこと。

② 個人情報については、原則持ち出すことを禁止とする。

③ 調査・解析等において、ログ情報は海外に開示しないこと。海外での調査・分析が必要な場合は、機構の了承を得ること。

(9) 納品物

① 電子ファイル等については、納品時点における最新版コンピュータウイルス検索用パターンファイル（DATファイル、定義ファイル、シグネチャ）を実装したコンピュータウイルス検知ソフトウェアを用いて、コンピュータウイルス混入についてチェックを行い、納品物の健全性を確保すること。

(10) 貸与品

① 情報を含む機構からの貸与品は、責任者を定めて適切に管理し、紛失や破損のないように留意すること。不要となった情報を含む貸与品は確実に返却又は抹消すること。また、本件作業が完了次第、全ての情報を含む貸与品を速やかに確実に返却又は抹消し、報告すること。

2.4 その他

① 情報セキュリティインシデントの発生や兆候を発見した場合は、機構に速やかに報告すること。

② 機構が情報セキュリティ対策の履行状況の点検及び現地確認を行う際は、機構の要請に応じて対応すること。

③ この要項に記載の要件を満足しない場合は、その代替方法を検討・提案し、機構の承認を受けること。

④ 要求仕様書に記載されている情報セキュリティに係る要件との齟齬が確認された場合には、本情報セキュリティ要件の記載内容を正として取り扱う。

2.5 提出物

① 2.1要求事項(2)②、(4)
情報セキュリティ対策の実施及び管理体制 説明資料（再委託先を含めた実施体制図等）

② 2.1要求事項(3)
情報セキュリティインシデント体制 説明資料（連絡先を含めた実施体制図）

以上