外部委託における情報セキュリティ要件について

仕様書別添２

　本委託業務の実施に当たり、以下の情報セキュリティ要件を満たしたうえで、機密保持を遵守するための措置を講じること。

１　機密保持に関する情報管理等について

（１）受注者は、政府機関統一基準群、厚生労働省情報セキュリティポリシー及び関係規程等を遵守すること。なお、厚生労働省情報セキュリティポリシー及び関係規程等は非公表であるため、政府機関統一基準群を必要に応じ参照すること。ポリシー及び関係規程等の開示については、契約締結後に開示する。

政府機関統一基準群：https://www.nisc.go.jp/active/general/kijun30.html

（２）受注者は、本業務において取扱う情報について、下記２から９の項目を記載した情報セキュリティ管理計画書を提出し、事業を開始するまでに当局の承認を得ること。また、当局は措置状況について、随時、実地調査できるものとする。

２　情報管理のための体制整備等について

1. 情報管理のための体制

ア　受注者は、受注者組織全体のセキュリティを確保するとともに、当局から求められた当該業務の実施において情報セキュリティを確保するための管理体制を整備すること。

イ　本体制には、経営者が関与し、経営者の責任の明確化を図ること。

ウ　当局が提供した業務上の情報を適正に管理するために、情報管理責任者（当該業務の情報取扱いの全てに責任を有する者）をおくこと。

エ　情報管理責任者は、事務の一部を担当させるため、情報取扱管理担当者（当該業務の進捗管理等を行い当該業務の情報を取扱う可能性のある者）を指定すること。

オ　当該業務の実施に当たり、受注者又はその従業員、本調達の役務内容の一部を再委託する先、若しくはその他のものによる意図せざる不正な変更が情報システムのハードウェアやソフトウェア等に加えられないための管理体制を整備すること。

1. 情報管理のための体制確保について

ア　受注者は、本業務で知り得た情報を適切に管理する必要があることから、次に掲 げる体制を確保し、当該体制を確保していることを証明するため、当局に対し、以下の書面を提出すること。（下記（ウ）は、研究開発及び調査、コンピュータサービス並びに電気通信サービスに関する調達の場合にのみ必要。）

1. 情報取扱者名簿

当該業務に従事する者のうち、保護を要する情報を取り扱う可能性のある者の名　　簿をいう。業務の一部を再委託する場合は再委託先も含む。情報取扱者名簿には、情報管理責任者、情報取扱管理者、その他保護を要する情報を取り扱う可能性のある者について、氏名、住所、生年月日、所属 部署、役職等を、業務の一部を再委託する場合は再委託先も含めて記載すること。

1. 情報セキュリティを確保するための体制を定めた書面

情報管理体制図、情報管理に関する社内規則のほか、受注者等の資本関係・役員等の情報、業務の実施場所が確認できる資料をいう。業務の一部を再委託する場合　は再委託先も含む。

1. 業務従事者名簿

当該業務に従事する者の名簿をいう。業務従事者名簿には、当該業務に従事す　る者について、氏名、所属部署、 役職、学歴、職歴、業務経験、研修実績その他の経歴、専門的知識その他の知見、母語及び外国語能力、国籍等を記載すること。

イ　受注者は、「情報取扱者名簿」、「情報セキュリティを確保するための体制を定め　た書面」及び「業務従事者名簿」に変更がある場合は、あらかじめ当局に申請を行い、承認を得なければならない。

1. その他

ア　情報管理責任者は、受注者側組織内で作業を行う場合の情報の取扱いに関して、 情報セキュリティが侵害され又はそのおそれがある場合等の非常時における対策を定めると共に、その内容を従事者に徹底すること。

イ　本調達の役務内容を一部再委託する場合は、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に情報セキュリティ管理計画 書に記載された措置の実施を担保すること。

３　取り扱う情報の目的外利用等について

（１）当局から提供する情報の目的外利用を禁止すること。

（２）受注者は、本業務で知り得た情報について、当局が承認した場合を除き、受注者の役員等を含め、情報取扱者以外の者に伝達又は漏えいしてはならないこと。受注者は、本業務で知り得た情報について、当局が承認した場合を除き、受注者の親会社、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 その他の受注者に対して指導、監督、業務支援、助言、監査等を行う者を含め、受注者以外の者に伝達又は漏えいしてはならないこと。

４　情報の受領・管理・廃棄等について

（１）当局から情報を受領する場合は、情報セキュリティに配慮した受領方法にて行うこと。 例えば、メールや ＣＤ等で情報のやりとりをする場合には、ファイルに設定するパスワードを委託先と事前に決定し、当該ルールに基づき実施すること。

（２）受注者が個人情報等を電子メール、ＦＡＸ、郵送により送付する、又はインターネット等にアップロードする作業を行う場合は、送付手順書・アップロード手順書（別添２－１）を作成し当局へ速やかに提出すること。

（３）本業務において当局から受領した情報（資料等を含む。）及び作成された情報については、業務の終了に伴い不要となった場合又は当局から返却又は廃棄若しくは抹消の指示があった場合は、速やかに返却する又は廃棄・抹消する場合は回復が困難な方法により速やかに対応すること。なお、実施方法等については、作業実施計画書（別添２－２）により当局の承認を得た上で速やかに実施し、実施後においては作業完了報告書（別添２－３）を当局へ速やかに提出すること。情報の返却又は廃棄若しくは抹消は、契約期間内に確実に終了することとし、特に、契約の終期が年度末となっている場合、抹消等が契約期間内までに確実に完了する必要があることに留意すること。

（４）本業務を実施する住所を示すこと。

（５）当該業務の日々の活動場所は、受注者側組織内であることに鑑み、情報を受注者組織内に移送する際は、暗号化や施錠等適切な方法により、情報セキュリティを確保すること。また、受注者側組織内へ移送した情報は、当局との調整等に必要な場合及び返却時以外は原則として、受注者組織外に持ち出さないこと。

（６）個人情報等の重要な情報が記載された情報に関しては、原則として社外に持ち出さないこと。

（７）受注者側組織内で作業を行う場合には、作業を行う施設は、IC カード等の電磁的管理又はこれに準じた方法による入退館管理がなされていること。

（８）同様に、上記作業施設内の作業実施場所は、IC カード等の電磁的管理又はこれに準じた方法による入退室管理がなされていること。

（９）電磁的に情報を保管する場合には、当該業務に係わる体制以外の者がアクセスできないようアクセス制限を行うこと。また、アクセスログにより不審なアクセスがないか等の確認を行うこと。

（10）当局から受領した情報を保管する端末やサーバ装置等は、受注者の情報セキュリティポリシー等により、サイバー攻撃に備え、ウイルス対策ソフト、脆弱性対応及び検知・監視等の技術的対策が講じられ、適切に管理・運用される必要があるため、 政府統一基準群や厚生労働省情報セキュリティポリシーに準拠し、管理等することとし、 準拠した対応ができない場合は、代替のリスク軽減策を講じ、当局の承認を得ること。

(11) 情報セキュリティ対策に関する履行状況を定期的に確認し、当局へ報告すること。

５　情報セキュリティが侵害された場合の対処について

（１）情報セキュリティインシデントへの対処方法が確立されていること。

（２）本業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、業務の履行中・履行後を問わず、速やかに当局に報告すること。なお、受注者自ら検知したものに限らず、報道等の外部からの指摘により認知した場合を含む。

（３）本調達に係る業務の遂行において、情報セキュリティ対策の履行状況を定期的に当局に報告すること。なお、情報セキュリティ対策の履行状況に問題がある場合は、 情報セキュリティインシデントに該当する可能性もあることから、速やかに当局に報告すること。

（４）被害の程度を把握するため、受注者は必要な記録類を事案対応終了時まで保存し、 当局の求めに応じて成果物と共に当局に引き渡すこと。

６　情報セキュリティ対策の履行が不十分な場合の対処について

本調達に係る業務の遂行において、受注者における情報セキュリティ対策の履行が不 十分であると認められる場合には、速やかに改善策を提出し、当局の承認を受けた上で 実施すること。

７　ファイル共有サービス等の外部サービスの活用における遵守事項について

　　受注者は、インターネット上のファイル共有サービス等 (オンラインストレージ、クラウドサービス等を含む。)を活用する場合、以下の項目を遵守すること。

（１）受注者は、重要情報をインターネットから直接参照できないよう、適切なアクセス制御を行うこと。（主体認証やIP アドレスでの制限など、サービスにて利用可能な各種制御機能を用いて、アクセス可能な者が必要最小限となるよう限定する。）

（２）受注者は、アクセス権（ファイル等を閲覧可能なユーザー等）の設定について、不適切なもの（初期設定のまま、あるいは、誰もが閲覧可能となっている等）となっていないか、情報のアップロード前に確認すること。（確認手順の策定や、ダブルチェックを徹底するなど、人為的ミスの発生リスクを低減する。）

（３）受注者は、主体認証に係る情報（ID/PASS）や保存場所へのアクセスに必要なURL 等は、第三者に窃取されないよう厳重に管理すること。（可能な場合は多要素認証を用いる。）

（４）受注者は、情報を十分な強度を持つ暗号化形式（AES-256bit など）で暗号化して保存すること。（例：アップロード前にファイルを暗号化し、暗号化したファイルをストレージに送信(保存)する等。）

（５）受注者は、通信経路における盗聴及び情報の改ざん等の対策として、通信内容の秘匿性を確保するためTLS（SSL）、IPsec 等による暗号化を行うこと。

（６）受注者は、主体認証や暗号化などに用いるパスワードは、推定されないよう十分な長さや複雑さを持たせること。

（７）受注者は、ファイル共有サービス等に保存した情報について、業務上不要となった時点で速やかに削除すること。

（８）受注者は、約款による外部サービスで個人情報を含む要機密情報を取り扱わないこと。

８　情報セキュリティ監査の実施について

（１）本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、当局が情報セキュリティ監査の実施を必要と判断した場合は、当局がその実施内容（監査内容、対象範囲、実施者等）を定めて、情報セキュリティ監査を行う （当局が選定した事業者による外部監査を含む。）。

（２）受注者は、当局から監査等の求めがあった場合に、速やかに情報セキュリティ監査を受け入れる部門、場所、時期、条件等を「情報セキュリティ監査対応計画書」 等により提示し、監査を受け入れること。

（３）受注者は自ら実施した外部監査についても当局へ報告すること。

（４）情報セキュリティ監査の実施については、これらに記載した内容を上回る措置を講ずることを妨げるものではない。

（５）業務履行後において当該業務に関する情報漏えい等が発生した場合であっても、 監査を受け入れること。

９　報告の義務について

当局から求めがあった場合には、以上の状況について書面等での報告を行うこと。