

機密情報の取扱いに関する標準特記仕様書チェックリスト

条項	条文	確認欄
第4条	受注者は、この契約による事務において個人情報を取り扱う場合は、個人情報の保護に関する法律等の法令に基づき、個人情報保護方針を公表していなければならない。	・ 公表場所（ホームページなど） 【補足】 随意契約の場合は、事業者が個人情報保護方針を公表している場所（URL等）を記入してください。競争入札の場合は、記入不要です。
第4条の2	受注者は、この契約による事務の履行のために機密情報を取り扱う場合において、発注者の指定があるときは、次に掲げるいずれかの認証制度の認証を取得していなければならない。 (1) I S M S（ISO/IEC27001（JIS Q 27001））認証取得 (2) プライバシーマーク（JIS Q 15001）取得 (3) その他発注者が適当と認める認証取得	☐ 次のいずれの認証等を指定しているか ☐ I S M S（ISO/IEC 27001（JIS Q 27001）） ☐ プライバシーマーク（JIS Q 15001） ☐ その他発注者が適当と認める認証取得 【補足】 随意契約の場合は、契約する事業者が取得している認証にチェックを入れてください。 競争入札の場合も認証の取得を指定する場合は、該当の認証にチェックを入れてください。 認証の取得状況は、一般財団法人日本情報経済社会推進協会（https://entity-search.jipdec.or.jp/pmark）や一般社団法人情報マネジメントシステム認定センター（https://isms.jp/lst/ind/index.html）で確認できます。

条項	条文	確認欄
第4条の3	受注者は、この契約による事務の履行のために利用するクラウドサービス（有料、無料にかかわらず、民間事業者等がインターネット上で提供する情報処理サービスで、約款への同意及び簡易なアカウントの登録等により当該機能が利用可能となるサービスのこと。以下同じ。）で機密情報を取り扱う場合であって、発注者の指定があるときは、次に掲げるいずれかの認証制度の認証を取得し、又は内部統制評価制度による審査を受けていなければならない。 (1) クラウドセキュリティ認証制度（I S M S 導入組織の場合） ア I S M S クラウドセキュリティ（ISO/IEC 27017）認証取得 イ パブリッククラウド上における個人情報保護（ISO/IEC 27018）認証取得 ウ プライバシー情報マネジメントシステム（ISO/IEC 27701）認証取得（サービス単位での場合） ・クラウド情報セキュリティ監査（C S）ゴールドマーク又はシルバーマーク（JASAクラウドセキュリティ推進協議会）取得（発注者が重要な情報システムとして特に指定したものの場合） ア 日本国政府情報システムのためのセキュリティ評価制度（I S M A P）認証取得 イ アメリカ合衆国政府機関におけるクラウドセキュリティ認証制度（F e d R A M P）認証取得	☐ クラウド化する ・クラウドサービスの形態は ☐ IaaS ☐ PaaS ☐ SaaS ☐ 次の認証等の指定をするか 1 I S M S クラウドセキュリティ（ISO/IEC 27017） ☐ IaaS ☐ PaaS ☐ SaaS 2 パブリッククラウド上における個人情報保護（ISO/IEC 27018） ☐ IaaS ☐ PaaS ☐ SaaS 3 プライバシー情報マネジメントシステム（ISO/IEC 27701） ☐ IaaS ☐ PaaS ☐ SaaS 4 クラウド情報セキュリティ監査（C S）ゴールドマーク又はシルバーマーク（JASAクラウドセキュリティ推進協議会） ☐ IaaS ☐ PaaS ☐ SaaS 5 日本国政府情報システムのためのセキュリティ評価制度（I S M A P） ☐ IaaS ☐ PaaS ☐ SaaS 6 アメリカ合衆国政府機関におけるクラウドセキュリティ認証制度（F e d R A M P） ☐ IaaS ☐ PaaS ☐ SaaS 7 受託業務に係る内部統制の保証報告書（S O C 2） ☐ IaaS ☐ PaaS ☐ SaaS 8 受託業務に係る内部統制の保証報告書（S O C 3） ☐ IaaS ☐ PaaS ☐ SaaS 9 業務全般にかかるシステムの内部統制の保証業務（SysTrust）審査報告書 ☐ IaaS ☐ PaaS ☐ SaaS 10 電子商取引認証局に対する保証業務（WebTrsuts）審査報告書 ☐ IaaS ☐ PaaS ☐ SaaS
第4条の3	(2) 内部統制評価制度 ア 受託業務に係る内部統制の保証報告書（S O C 2）（日本公認会計士協会IT7号） イ 受託業務に係る内部統制の保証報告書（S O C 3）（日本公認会計士協会IT2号） ウ 業務全般にかかるシステムの内部統制の保証業務（SysTrust）審査報告書（日本公認会計士協会IT2号） エ 電子商取引認証局に対する保証業務（WebTrsuts）審査報告書（日本公認会計士協会IT3号）	・上記認証の確認方法 ☐ 写しで確認：上記の番号： ☐ 審査機関等Webサイト等で確認：上記の番号： ☐ 事業者HPの掲載のマークで確認：上記の番号： ☐ その他：上記の番号： 【補足】 委託事業者がクラウドサービスを利用する場合は「クラウド化する」及び「クラウドサービスの形態」にチェックを入れてください。 また、随意契約の場合は、取得している認証にチェックを入れてください。競争入札の場合も認証の取得を指定する場合は、該当の認証をチェックを入れてください。

条項	条文	確認欄
第4条の4	受注者は、この契約による事務の履行のために利用するデータセンターで機密情報を取り扱う場合は、次に掲げる条件を満たすものを利用しなければならない。 (1) データセンターファシリティスタンダード（日本データセンター協会（JDCC））ティア3以上又はこれと同等レベルの安全性及び可用性の高さに関するサービス品質を保証するもの。 (2) 個人情報を含むデータは日本国内にあること。	☐ データセンターで機密情報を取り扱う - データセンターファシリティスタンダードを指定 ☐ ティア3相当と確認 ☐ ティア4相当と確認 - データの所在 ☐ データは国内所在であることを指定 確認方法： 【補足】 委託事業者がデータセンターで機密情報を取り扱う場合は、「データセンターで機密情報を取り扱う」にチェックを入れてください。 随意契約の場合は、委託事業者にティア3または4相当であること、データが日本国内にあることを確認し、その内容を記入してください。競争入札の場合は、記入不要です。
第6条	受注者は、この契約の締結後、次の文書を発注者に直ちに提出しなければならない。提出後に内容の変更があった場合も、同様とする。 (1) 情報セキュリティ及び機密情報保護に関する社内規程又は基準 (2) 次の内容を含む従事者名簿 ア 機密情報取扱いの責任者及び機密情報を取り扱う者の氏名、責任、役割及び事務執行場所 イ 機密情報に係る記録媒体の授受に携わる者の氏名並びに事務執行場所 ウ この契約による事務に関する緊急時連絡先一覧 (3) この契約による事務に関する実施スケジュールを明記した文書	- 提出の確認（契約締結後） ☐ 情報セキュリティ及び機密情報保護に関する社内規程又は基準 ☐ 従事者名簿 ☐ 実施スケジュール 【補足】 契約締結後の提出状況の確認欄として活用してください。（協議の際は記入不要です。）

条項	条文	確認欄
第6条	2 受注者は、この契約による事務の履行のために特定個人情報を取り扱う場合においては、この契約の締結後、次の文書を発注者に直ちに提出しなければならない。提出後に内容の変更があった場合も、同様とする。 (1) この契約による事務において使用する情報システムのネットワーク構成図（特定個人情報ファイル（コンピュータ等で検索することができるように体系的に構成した情報の集合物であって、個人番号をその内容に含むもの。以下同じ。）を取り扱う場合のみ。第24の3条の事項を証するもの。） (2) この契約による事務において使用する情報システムのセキュリティ仕様書（特定個人情報ファイルを取り扱う場合のみ。第24条の4の事項を証するもの。）	・ 提出の確認（契約締結後） ☐ 情報システムのネットワーク構成図 ☐ セキュリティ仕様書 ☐ クラウドサービスの利用に係るリスク対策文書 【補足】 契約締結後の提出状況の確認欄として活用してください。（協議の際は記入不要です。）
第6条	3 受注者は、この契約による事務の履行のためにクラウドサービスを利用する場合においては、この契約の締結後、クラウドサービスの利用に係るリスク対策文書（第24条の5の事項を証するもの）を発注者に直ちに提出しなければならない。提出後に内容の変更があった場合も、同様とする。 4 受注者は、前3項の規定により、発注者に届け出た従事者以外の者に、この契約による事務に係る機密情報を取り扱わせてはならない。	

条項	条文	確認欄
第7条	受注者は、この契約による事務の履行について、機密情報を取り扱う事務の全部又は一部を第三者（受注者の子会社（会社法（平成17年法律第86号）第2条第3号に規定する子会社をいう。）を含む。以下同じ。）に委託（以下「再委託」という。）してはならない。ただし、再委託をする事業者の名称及び所在地、再委託の内容及び理由並びに再委託をする事業者の機密情報に係る安全管理措置の状況等必要な事項を発注者に書面で提出し、その承諾を得た場合はこの限りではない。 2 前項ただし書の規定により再委託を受けた事業者は、この契約を受注した事業者とみなしてこの仕様書の規定が適用されるものとする。 3 受注者は、第1項ただし書の規定により再委託をする場合は、発注者に対し再委託をする業務に関する報告を行うとともに、再委託をする業務に関する全ての行為について、発注者に対し全ての責任を負うものとする。	☐ 再委託あり 【補足】 委託事業者が再委託する場合は、チェックを入れてください。 また、該当の場合は、必ず契約課への手続きも行ってください。
第9条	受注者は、発注者がこの契約による事務での使用を目的として受注者に提供し、又は貸与する機器等の情報資産を、当該事務以外の目的に使用してはならない。また、第三者に提供してはならない。	☐ 機器等の提供あり ・ 提供機器 ・ 管理方法 【補足】 委託事業者に提供等する機器がある場合は「機器等の提供あり」にチェックを入れ、その機器を記入してください。 随意契約の場合は、委託事業者における機器の管理方法について記入してください。

条項	条文	確認欄
第10条	受注者は、この契約による事務で取り扱う機密情報について、発注者の承認を得ずに複写、複製又は加工してはならない。当該事務を実施する上でやむを得ず複写、複製又は加工するときは、あらかじめ発注者に通知し、その承認を得なければならない。この場合において、当該事務の終了後（当該事務の終了後、引き続き発注者と受注者と当該事務に係る契約を締結する場合を除く。）、受注者は、直ちに複写、複製又は加工した機密情報を消去し、再生又は再使用できない状態にするとともに、機密情報を消去した日時、担当者及び処理内容を発注者に報告しなければならない。	☐ 複写、複製等をする機密情報あり 消去した日時（消去後） ☐ 担当者（消去後） ☐ 消去方法（事前指定・協議又は消去後） 【補足】 複写、複製等する機密情報がある場合は「複写、複製等をする機密情報あり」にチェックを入れてください。 機密情報の消去方法を指定する場合は、記入してください。 その他記入欄は、機密情報を消去した場合の確認欄として活用してください。
第11条	受注者は、この契約による事務開始前までに当該事務で機密情報を取り扱う事務執行場所及び機密情報の管理状況について、発注者に報告しなければならない。 2 受注者は、事前の発注者の承諾なく、この契約による事務で取り扱う機密情報を事務執行場所から持ち出してはならない。 3 受注者は、発注者の施設、事務執行場所等から機密情報を持ち出す必要がある場合には、暗号化、パスワード設定等の保護対策、鍵付きのケース等に格納する等機密情報の紛失や不正利用を防止するための安全管理措置及び運搬に当たってのセキュリティ便の使用等の紛失リスクの低減対策等を事前に発注者に協議しなければならない。 4 受注者は、実際に機密情報の持出しを行う場合には、運搬、保管・管理、廃棄等の各段階におけるその保護対策の状況、安全管理措置の状況等（以下「情報セキュリティ管理状況」という。）に関する記録及び適正な状況であることの確認を行った記録を残さなければならない。	☐ 持ち出しをする場合あり - 持ち出す場合の運搬方法、セキュリティ対策 【補足】 委託事業者による機密情報の持ち出しがある場合は「持ち出しをする場合あり」にチェックを入れてください。 随意契約の場合は、持ち出す場合の運搬方法、セキュリティ対策について記入してください。 ★複数の方法を実施する場合は、方法別に対策を記述のこと - 手交の場合は、双方で受領の確認ができる様式はあるか。 - 郵送の場合は、追跡確認ができる等の措置を施すか。 - 電磁的記録媒体を用いる場合は、どのようなセキュリティ対策を施すか。
第13条	受注者は、この契約による事務に係る発注者が運用する情報システムのサーバ等を区の施設外に設置する場合は、発注者の承認を得なければならない。 2 受注者は、前項のサーバ等について、定期的に情報セキュリティ対策状況について確認するとともに、発注者から要請があった場合は、その結果を発注者に報告しなければならない。	☐ 区の施設外にサーバ等の設置あり 【補足】 該当がある場合はチェックを入れてください。

条項	条文	確認欄
第19条	受注者は、従事者に対して、情報セキュリティ及び機密情報保護に関する教育並びに緊急時対応のための訓練を計画的に実施し、発注者にその教育の実施状況等を報告しなければならない。	- 報告の確認（契約締結後） ☐ 教育の実施状況等 【補足】 契約締結後に確認欄として活用してください。（協議の際は記入不要です。） 教育が第6条で報告を受けた従事者名簿に記載されている全員を対象に実施されているかを確認してください。
第22条	受注者は、情報システム等に記録された重要度の高い機密情報について、定期的にバックアップを取得しなければならない。また、バックアップの取得前にその手法を発注者に通知し、承認を得なければならない。	☐ バックアップを取るべき機密情報あり 手法、インターバル 【補足】 バックアップを取得するべき機密情報がある場合は「バックアップを取るべき機密情報あり」にチェックを入れ、その手法（外付けHDD、別クラウドサーバ等）・インターバル（対象期間・頻度等）などを記入してください。
第24条	受注者は、この契約による事務に使用する情報システムがネットワークに接続されている場合は、不正アクセスを防ぐため、常にセキュリティホールの発見に努め、メーカー等からのセキュリティ修正プログラムの提供があり次第、情報システムへの影響を確認し、発注者と協議の上、修正プログラムを適用しなければならない。また、不正プログラム対策を行い、不正プログラムの情報システムへの侵入及び拡散を防止しなければならない。	☐ ネットワークに接続あり - 不正アクセス対策等の確認 【補足】 情報システムがネットワークに接続されている場合は、「ネットワークに接続あり」にチェックを入れてください。 随意契約の場合は、委託事業者の不正アクセス対策等について記入してください。 記入にあたっては、次のことも確認してください。 - アンチウィルスソフトの導入、最新の定義ファイル適用等により、システム全般を検査し、不正プログラムの侵入がないことを定期的に確認しているか。 - 不正侵入探知、遮断のシステムを導入し、不正な通信は遮断する体制となっているか。
第24条 の3	受注者は、この契約による事務において特定個人情報ファイルを取り扱う場合は、当該特定個人情報ファイルをインターネットから物理的又は論理的に分離された環境にて取り扱わなければならない。	☐ 特定個人情報ファイルを取り扱うか - インターネットから分離方法 ☐ 物理的分離 ☐ 論理的分離 【補足】 特定個人情報ファイルの取扱いがある場合は、「特定個人情報ファイルを取り扱うか」にチェックを入れてください。 随意契約の場合は、該当する分離方法にチェックを入れてください。

条項	条文	確認欄
第24条 の4	受注者は、この契約による事務に使用する情報システムにおいて特定個人情報を取り扱う場合は、定期及び必要に応じ随時に当該情報システムのログ等の分析を行うなど不正アクセス等を検知する仕組みを講じるとともに、当該情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講じなければならない。	☐ 特定個人情報ファイルを取り扱うか 不正アクセス等対策、不正な構成変更対策について 【補足】 情報システムにおいて特定個人情報の取扱いがある場合は「特定個人情報ファイルを取り扱うか」にチェックを入れてください。 随意契約の場合は、不正アクセス等対策、不正な構成変更対策について記入してください。
第26条	受注者は、機密情報を電子メール、ファイル交換サービス等で送受信する場合は、事前に暗号化、パスワード設定等の保護対策を発注者に協議するとともに、実際に保護対策を講じなければならない。 2 受注者は、機密情報を郵送等で送付する場合は、送付状況を追跡できるサービスを活用する等の対策を講じなければならない。	☐ 電子メール、ファイル交換サービス等の使用あり 送受信方法及び保護対策の手法 【補足】 電子メール、ファイル交換サービス等を使用する場合は「電子メール～等の使用あり」にチェックを入れてください。 区または事業者が受け渡し方法を指定する場合は、送受信方法及び保護対策の手法について記入してください。なお、複数の方法を実施する場合は、方法別に対策を記述してください。 ※ファイル交換サービス等を利用する場合は、第4の4を参考にし、セキュリティ水準が高いサービスを利用してください。 ※個人情報をファイル交換サービスで送受信する場合は、別途個人情報処理の外部結合に係る協議が必要になる可能性があります。
第26条	3 受注者は、やむを得ず機密情報を使送する場合は、施錠可能なケースにより運搬する等の保護対策を講じるとともに、事前に運搬ルートを発注者に協議し、その運搬ルートを遵守しなければならない。	☐ 使送あり ☐ 運搬ルートの協議あり 【補足】 使送がある場合は、「使送あり」にチェックを入れてください。 また、「運搬ルートの協議あり」は、契約締結後に確認欄として活用してください。（協議の際には記入不要です。）

条項	条文	確認欄
第28条	受注者は、この契約による事務が終了したときは、発注者より受領し、又は受注者が当該事務を遂行する中で記録・作成した機密情報や機密情報に当たらない機器等の情報資産を速やかに発注者に返却しなければならない。 2 前項のほか、発注者に返却が不可能な機密情報又は発注者に返却をすることによりかえって機密情報が紛失する可能性がある場合には、発注者の了承のもと、機密情報及び情報資産を復元できないような処置をした上で廃棄し、日時、担当者及び処理内容を発注者に報告し、廃棄した記録を遅滞なく提出しなければならない。 3 この契約による事務を遂行していく中で、発注者から受領した機密情報を保持しておく必要性が乏しい場合については、前項と同様とする。	☐ 受注者に受け渡し等を行った機密情報あり ☐ 返却の確認 又は ☐ 返却を行わない場合 ・ 消去した日時（消去後） ・ 担当者（消去後） ・ 処理方法（事前指定・協議又は消去後） 【補足】 処理方法を指定している場合は「処理方法」にその方法を記入してください。その他は、機密情報を消去した場合の確認欄として活用してください。（協議の際には記入不要です。）
第30条	受注者は、この契約による事務で使用しているサーバ、パソコン等の機器（以下これらを「電子情報処理機器」という。）を修理又は廃棄する場合は、事前に当該電子情報処理機器に保存されている機密情報を消去し、再生又は再使用できない状態にするとともに、機密情報を消去した日時、担当者及び処理内容を発注者に速やかに報告しなければならない。	☐ 修理又は廃棄した電子情報処理機器あり ・ 消去した日時（消去後） ・ 担当者（消去後） ・ 処理方法（事前指定・協議又は消去後） 【補足】 処理方法を指定している場合は「処理方法」にその方法を記入してください。その他は、機密情報を消去した場合の確認欄として活用してください。（協議の際には記入不要です。）
第30条	2 前項の場合は、次に掲げる措置を行うものとし、受注者はその旨を発注者に事前に報告するものとする。ただし、当該措置を行うことが困難な場合には、発注者に協議し、承認を得るものとする。 (1) 記録装置の物理的又は電磁的な破壊 (2) 発注者が指定する場所で、発注者の職員の立会いの下における当該電子情報処理機器に保存されている機密情報を消去し、再生又は再使用できない状態にする措置 (3) 発注者が指定する場所で、発注者の職員の立会いの下における記録装置の物理的又は電磁的な破壊	☐ 以下の措置の対応あり（契約締結後・消去前） ☐ 記録装置の物理的又は電磁的な破壊 ☐ 職員の立会いの下での消去等 ☐ 職員の立会いの下での記録装置の物理的又は電磁的な破壊 【補足】 契約締結後に確認欄として活用してください。（協議の際には記入不要です。）

条項	条文	確認欄
第31条	受注者は、発注者に対し、機密情報の情報セキュリティ管理状況及びこの契約による事務の状況を定期的及びこの契約による事務の終了後に報告するものとする。ただし、発注者が必要と認めるときは、その都度報告するものとする。	◆ 報告の有無 年 月 日 【補足】 契約締結後に確認欄として活用してください。（協議の際には記入不要です。）
第34条	受注者は、この契約による事務において、事務上のトラブル、災害、事故、電子情報処理機器の不良、故障及び破損等が発生した場合は、速やかに発注者にその状況について報告し、発注者の指示に従わなければならない。	☐ 事務上のトラブルあり（契約締結後） 【補足】 契約締結後に確認欄として活用してください。（協議の際には記入不要です。）
第35条	受注者は、この契約による事務について次に掲げる事象が発生した場合は、速やかに、発注者にその状況を具体的に報告するとともに、発注者と協議の上、事故処理を行うものとする。 (1) 機密情報の紛失 (2) 機密情報の破壊 (3) 機密情報の改ざん (4) 機密情報の漏えい (5) 不正アクセス (6) 情報セキュリティ基本方針及びこの仕様書に定める事項の違反 (7) 前各号に掲げるもののほか、情報セキュリティに悪影響を及ぼす事象	☐ 次に掲げる事象の発生あり（契約締結後） ☐ 機密情報の紛失 ☐ 機密情報の破壊 ☐ 機密情報の改ざん ☐ 機密情報の漏えい ☐ 不正アクセス ☐ 情報セキュリティ基本方針及びこの仕様書に定める事項の違反 ☐ その他情報セキュリティに悪影響を及ぼす事象 【補足】 契約締結後に確認欄として活用してください。（協議の際には記入不要です。）