機密情報の取扱いに関する標準特記仕様書

（基本的事項）

第１条　受注者は、この契約による事務の実施に当たり、個人情報（特定個人情報を含む。以下同じ。）を取り扱うときは、その保護の重要性を認識し、個人の権利利益を侵害することのないよう、個人情報の保護に関する法律（平成１５年法律第５７号）（特定個人情報を取り扱う場合は、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号）を含む。）その他の関係法令を遵守し、個人情報の漏えい、滅失又は毀損の防止その他の個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

２　受注者は、この契約による事務の実施に当たっては、目黒区情報セキュリティ基本方針を遵守し、機密情報（個人情報のほか、この契約に基づき発注者から提供を受ける技術情報及び行政の運営上の情報のうち、秘密である旨を示された機器等の情報資産（メモ及びバックアップ等を含む。）をいう。以下同じ。）を適正に取り扱わなければならない。

（秘密保持義務）

第２条　受注者は、この契約による事務により知り得た機密情報をいかなる理由があっても第三者に漏らしてはならず、この旨を当該事務に従事する者（以下「従事者」という。）へ周知徹底しなければならない。この契約が終了し、又は解除となった後においても同様とする。

（書面主義の原則）

第３条　受注者は、この仕様書に定める事項により通知、報告、提出等が求められている事項については、特段の定めがない限り、書面により行うものとする。

（個人情報保護方針の公表）

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。

参考：個人情報保護方針の公表項目

１　取得する個人情報の利用目的

２　保有個人データに関する事項

３　開示等の請求に応じる手続

４　問い合わせ及び苦情の窓口

５　オプトアウトにより個人情報を第三者へ提供する場合は、次に掲げる事項

・第三者への提供を利用目的とすること

・第三者に提供される個人データの項目

・第三者への提供の手段又は方法

・本人の求めに応じて第三者への提供を停止すること

６　個人情報を共同利用する場合は、次に掲げる事項

・利用する者の名称

・利用目的
・利用する個人情報の項目

（情報セキュリティ及び個人情報保護に関する認証等）

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) ＩＳＭＳ（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

（クラウドサービスに関する認証等）

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

（ＩＳＭＳ導入組織の場合）

ア　ＩＳＭＳ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（ＣＳ）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（ＩＳＭＡＰ）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（ＦｅｄＲＡＭＰ）認証取得

(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（ＳＯＣ２）（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（ＳＯＣ３）（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）

（データセンターに関する情報セキュリティ対策）

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、原則日本国内にあること。

ただし、当該データセンターに関する契約において、準拠法が日本法であり、管轄裁判所が日本国内の裁判所と定められている場合で、かつ発注者が適当と認めたときは、データを国外に保管することを認めることができる。

（収集の制限）

第５条　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収集するときは、その業務の目的を達成するために必要な範囲で、適法かつ公正な手段によって収集しなければならない。

（管理体制等の通知）

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

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条の３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。）

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。

（再委託の制限等）
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。
（目的外使用及び外部提供の禁止）
第８条　受注者は、この契約による事務で取り扱う機密情報を当該事務の目的以外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。
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。
（複写及び複製等の制限）
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。
（機密情報の持出制限）
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。

（物的セキュリティ対策）

第１２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に係る装置の取付けを行う場合は、できる限り、火災、水害、埃、振動、温度、湿度、磁気、紫外線、直射日光等の影響を受けない場所に設置するものとし、施錠等容易に取り外すことができないよう必要な措置を講じなければならない。

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。

第１４条　受注者は、その従事者に名札等の着用及び身分証明書等の携帯を義務付け、発注者のサーバ管理施設その他の発注者の管理区域に立ち入る場合において発注者から求められたときは、身分証明書等を提示するよう指導しなければならない。

第１５条　受注者は、この契約による事務で使用するパソコン等の盗難を防止するため、当該パソコン等をセキュリティワイヤーで固定し、又は従事者が事務執行場所を離れる間において施錠可能なロッカー等に収納させるなどの措置を講じなければならない。

（人的セキュリティ対策）

第１６条　受注者は、この契約による事務において、発注者に提出した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を遵守しなければならない。

２　受注者は、情報セキュリティ対策について疑義がある場合、遵守することが困難な点等がある場合は、速やかに発注者に報告し、代替策について協議しなければならない。

第１７条　受注者は、情報資産を適切に保管するものとし、パソコン等により情報資産を使用する場合は、第三者に使用され、又は閲覧されることがないように、離席時にパスワードロック又はログオフ等を行わなければならない。

第１８条　受注者は、従事者に情報システムの保守又は運用業務に関し、次の事項を遵守させなければならない。

(1) 自己が利用しているＩＤは、他人に利用させないこと（ＩＤの共用を指定されている場合は除く。）。

(2) 共用ＩＤを利用する場合は、共用ＩＤ の利用者以外の者に利用させないこと。

(3) パスワードを秘密にし、パスワードの照会等には一切応じないこと（パスワード発行業務を除く。）。

(4) パスワードのメモの不用意な作成等により、パスワード流出の機会を作らない

こと。

(5) パスワードは、十分な長さとし、想像し難い文字列とすること。

(6) 複数の情報システムを取り扱う場合は、パスワードを情報システム間で共有しないこと。

(7) パソコン等のパスワードの記憶機能を利用しないこと。

(8) 従業者間でパスワードを共有しないこと（ＩＤの共用を指定されている場合を除く。）。

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。

（技術的及び運用におけるセキュリティ対策）

第２０条　受注者は、情報システムの保守又は運用業務を遂行するに当たり、情報システムの変更記録、作業日時及び実施者を記録するとともに、各種アクセス記録及び情報セキュリティの確保に必要な記録を全て取得し、発注者が指定する期間保存しなければならない。

第２１条　受注者は、アクセスログ等を取得するサーバについて、正確な時刻設定を行わなければならない。自動的にサーバ間の時刻同期が可能な場合は、その措置を講じなければならない。

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。

第２３条　受注者は、情報システムの開発及び導入に当たり、開発及び導入前に発注者と協議の上、情報セキュリティに係る検証事項を定め、検証を実施しなければならない。

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。

第２４条の２　受注者は、情報システムを開発する場合は、システム開発及びテスト環境と、本番運用環境を分離しなければならない。

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。

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、ソフトウエ

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。

第２４条の５　受注者は、この契約による事務において利用するクラウドサービスで機密情報を取り扱う場合は、当該クラウドサービスの利用に伴い想定される情報セキュリティ上のリスクを回避するために必要な措置を講じなければならない。

（その他のセキュリティ対策）

第２５条　受注者は、この契約による事務に関し、発注者より機密情報を受領した場合は、預かり証を発注者に対して交付しなければならない。

２　前項の場合において受注者は、当該機密情報を適切に管理するため、機密情報の受領日時、受領者名、受領した機密情報の種類等の記録簿を作成するとともに、発注者から要請があった場合は、速やかに当該記録簿を発注者に提示しなければならない。

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。

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。

第２７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、厳格にアクセス制御を行うとともに、当該機密情報を施錠可能な金庫、ロッカー等に適切に保管する等善良な管理者の注意をもって当たり、機密情報の取扱いには十分注意し、機密情報の紛失並びに情報の改ざん、漏えい等の防止に努めなければならない。

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。

第２９条　受注者は、機密情報の作成業務を終了したときは、直ちに当該機密情報を発注者があらかじめ指定した職員に引き渡さなければならない。

（電子情報処理機器の修理又は廃棄）

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。

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

（委託業務の報告）

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。

（監査、施設への立入検査の受入れ）

第３２条　受注者は、機密情報の情報セキュリティ管理状況について、発注者の求めに応じて報告するものとする。

２　発注者は、受注者によるこの契約による事務の履行に伴う機密情報の取扱いについて、必要があると認めるときは、受注者に対して必要な指示を行うことができる。

３　発注者が必要に応じて監査又は検査を実施する場合は、受注者は受け入れなければならない。

第３３条　受注者は、発注者が必要とする場合は、業務執行場所へ発注者の職員の立入りを認めるものとする。

（緊急時の対応）

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。

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

（契約の解除）

第３６条　発注者は、受注者の責に帰すべき理由により、この契約による事務の履行に関し前条各号に掲げる事象が発生したときは、この契約を解除することができる。

（サービスレベルの保証）

第３７条　受注者は、この契約による事務のサービスレベルについて、事前に発注者と合意している場合は、そのサービスレベルを保証するものとする。

（損害賠償）

第３８条　受注者は、この仕様書に定める事項に違反し、又はこの仕様書に定める事項を履行しなかったことにより、発注者又は第三者に損害が生じた場合には、発注者又は第三者に対しこれを賠償するものとする。

（公表措置）

第３９条　発注者は、受注者がこの契約による事務の履行により知り得た機密情報の紛失、漏えい、滅失、毀損及び改ざん等の事故を発生させたときは、その事実を公表することができる。

（疑義等）

第４０条　この仕様書に定める事項について疑義が生じたとき又は定めのない事項については、発注者及び受注者双方協議の上定める。

以　　上