別紙１

令和７年度ちば起業家育成事業 業務委託仕様書（公募用）

本仕様書は、当該業務委託の企画提案募集にあたり、業務の大要として、業務内容、要求事項、確認事項等を示すものであり、最終的な業務委託仕様書は、受託者決定後、協議の上、千葉県（以下「県」という。）が作成する。

１　事業目的

若年層を対象とした体験型の教育プログラムの実施を通じて、参加者のアントレプレナーシップ獲得を支援し、将来の職業選択の幅を広げるとともに、本県の若年層の起業機運を高める。

２　委託期間

契約締結日から令和８年３月 31 日（火曜日）まで

３　執行限度額

１８，０００，０００円（消費税及び地方消費税込み）

４　事業概要

（１）小学生・中学生を対象とした起業体験会の開催
（２）高校生・大学生等を対象としたビジネスプラン作成ワークショップの開催
（３）高校生等を対象とした起業家講演イベントの開催
（４）その他（１）（２）（３）の実施に係る広報の実施　等

５　委託内容

受託者は、主催者である県の指揮監督の下、各事業の企画・運営を行う。なお、参加者からは、プログラム実施に係る費用は徴収しないこととし、プログラム実施に必要となる機材（ＰＣ等）は受託者が用意する。

（１）小学生・中学生を対象とした起業体験会の開催

小中学生を対象にした早期教育の機会として、県、体験先企業等と協力しながら「BtoB 型の起業体験会」を運営し、参加者の起業への関心を高める。

①開催回数、時期

以下の時期を目安に 30 時間程度（昼休憩除く）のプログラムを 2 回開催する。なお、1 日あたりのプログラム時間については、企画提案を踏まえ決定する。

（開催時期）企画提案を踏まえ、県及び受託者の協議により決定する。

②体験先企業

企画提案を踏まえ、県及び受託者の協議により決定する。

③開催場所

県、受託者及び体験先企業による調整の上、決定する。

④参加者等

意欲的な県内在住または在学の小学 4 年生から中学 3 年生とし、1 会場あたり 30 名

を目安に上限を設定する。なお、応募多数の場合は、抽選により決定する。

⑤プログラムの概要

実施するプログラムの大要は以下のとおりとし、詳細については、企画提案を踏まえ、県、体験先企業及び受託者の協議の上決定する。

ア　起業体験プログラムの提供

以下の要素を盛り込んだ BtoB 型起業体験プログラムを構築し、参加者に提供する。

なお、プログラム構築においては、県、体験先企業等と十分調整の上、参加者がチームとなって BtoB 型のビジネスを体験するものとし、販売体験のような限定的な学びとならないよう配慮すること。

ⅰ　参加者による仮想企業（１チームあたり 5 名程度）の立ち上げを支援するとともに、参加者に仮想企業内の役職を意識させること。

ⅱ　本プログラム内で使用する通貨を設定し、参加者に仮想企業における企業活動とコストの関連を意識させる。

ⅲ　体験先企業から仮想企業に対し検討テーマを提示させる。提示される検討テーマは、体験先企業の意向も踏まえ、参加者の主体的な検討が可能なものとすること。

ⅳ　仮想企業は、体験先企業から提示を受けたテーマを踏まえてビジネスアイデアの検討を進めることとし、以下によりその支援を行うものとする。

・会社の仕組みなどを学ぶ「講習会」の開催
・体験先企業の協力のもと実施する「フィールドワーク」の設定
・参加者の検討の熟度が高まった段階で実施する「体験先起業との折衝体験（カベウチ)」の設定（２回以上）

ⅴ　プログラム最終日に、各仮想企業による体験先企業へのビジネスアイデア・プレゼンテーション会を開催する。各仮想企業は、体験先企業から評価を受け、当該評価を仮想企業の決算に反映させる。

イ　参加者の支援体制の構築

アのプログラムを効果的に運営するため、以下の支援体制を構築する。

・起業体験プログラムの統括・進行管理役（ファシリテーター）
・仮想企業の企画立案に対し助言を行うコンサルタント
・参加者に寄り添い気づきを与えることで更なる取組を促すチューター（チューターは、仮想企業１チームに対し必ず１名以上を設定すること。）

ウ　タブレット等の端末の提供

収支計算やアイデア検討に活用するため、プログラム開催期間中において、各チームにタブレット等の端末を１台貸与する。

なお、同端末の管理は、チューターによる管理を徹底させ、プログラム中の端末使用に係る一切の費用については委託料から支出するものとする。

（２）高校生・大学生等を対象としたビジネスプラン作成ワークショップの開催

高校生・大学生等を対象にした実践的な取組の場として、県、開催地域等と協力しながら「ビジネスプラン作成ワークショップ」を運営し、参加者の起業への関心や新事業創出の意欲を高める。

①開催回数、時期

以下の時期を目安に、36 時間程度（昼休憩除く）のプログラムを開催する。なお、1 日あたりのプログラム時間については、企画提案を踏まえ決定する。

（開催時期）県、受託者及び開催地域による調整の上、決定する。

②開催地域

県において決定した地域

③開催場所

県、受託者及び開催地域による調整の上、決定する。

④参加者等

意欲的な県内在住・在学の高校生（中等教育学校後期課程生を含む）・高専生・大学生・大学院生・専門学校生等または県内在住の 16 歳から 25 歳までの者を対象に 25 名程度を上限とし、複数名グループでの参加を可とする。

なお、応募多数の場合は、起業を志す人材の発掘・育成の観点から参加者の選定を行う。

⑤プログラムの概要

実施するプログラムの大要は以下のとおりとし、詳細については、企画提案を踏まえ、県、開催地域及び受託者の協議の上決定する。

ア　ビジネスプラン作成プログラムの提供

参加者が、フィールドワーク先の地域課題の解決に資するビジネスプランを提案するものとし、以下の要素を含むビジネスプラン作成支援プログラムを構築し、参加者に提供する。

なお、ビジネスアイデアの創出やプランのブラッシュアップのため、プログラム開催日以外のオンライン支援も含め、最終発表会までの間、可能な限り継続的な支援を実施するものとする。

ⅰ　起業に資する基礎講座の開催

参加者に対し、ビジネスプラン立案に資する知識の獲得を支援するための講座を複数開催する。なお、「ビジネスにおけるデジタル技術の活用」に関する講座を必ず盛り込むものとする。

ⅱ　フィールドワークの実施

参加者による地域に対する理解を深め、ビジネスプランの検討に資する取組として、開催地域の関係機関と連携の上、フィールドワークを実施する。

なおフィールドワークの実施にあたっては、参加者のために、受託者において貸切バスなどの交通手段を確保すること。

ⅲ　中間発表会及び最終発表会の開催

参加者の検討の熟度が高まった段階で中間発表会を、プログラム最終日にビジネスプランの提案を行うピッチイベントを開催し、メンター等による講評・フィードバックを受ける機会を設定する。

ⅳ　プロダクト紹介資料の作成

最終発表会までの間において、参加者に対し、ビジネスプランのプロダクトを紹介するホームページ等を作成させる。

イ　参加者の支援体制の構築

アのプログラムを効果的に運営するため、以下の支援体制を構築する。

・ワークショップの統括・進行管理役（ファシリテーター）
・参加者によるビジネスプラン作成に伴走する支援員（参加者数に応じて複数設定すること）
・中間発表会や最終発表会において参加者にフィードバックを行うメンター（メンターは、複数名設定することとし、ビジネスの実務家が 1 名以上いることが望ましい。）

ウ　参加者への活動支援費の設定

参加者による試作品の作成や関係者へのヒアリング等のために要する経費（実費相当）について、委託料から参加者への活動支援費を支出することを妨げない。なお、活動支援費の上限については、企画提案を踏まえ、県及び受託者の協議の上決定する。

⑥起業関係イベント等への参加促進

参加者への情報提供等により、県内外の関係機関が実施する各種ビジネスプランコンテストや起業セミナー、ワークショップ等への参加を促す。

特に、本プログラムを通じて優秀なビジネスプランを提案した者について、別に企画提案募集を行う「ちば起業家応援事業」において実施する予定の「CHIBA ビジコン」や「起業家大交流会」への参加を促すこと。

（３）高校生等を対象とした起業家講演会の開催

受託者は、起業家による講演イベントを開催し、起業という将来の選択肢を知る機会を設け、参加者及び視聴者のチャレンジ精神やリーダーシップ等を引き出す。

①開催回数、時期

時期は任意とし、開催回数は 1 回とする。

②開催場所

50 名以上の会場での開催とし、県と受託者の調整の上、決定する。

③開催形態等

・招聘する起業家の選定をはじめとする講演会に係る企画については、企画提案を踏まえ、県と受託者の協議の上決定する。
・講演会については、別途、県において県内高校に限定配信を行う。このため、講演の模様を録画することとし、開催後 1 月以内に県に録画データを提供する。
・受託者は、県と調整の上、参加者募集のための体制を構築するとともに、教育機関及び高校生等への情報周知に積極的に取り組むこと。

（４）情報発信

①リーフレットの作成

県内教育機関向けに配布する（１）から（３）の各事業に係る参加者募集のためのリーフレット（A4 カラー）を作成する。

なお、作成したリーフレットについては、委託事業者において県内の対象教育機関を通じて在校生へ配布する。

（参考）

令和 6 年度小中学校向け起業体験会に係るリーフレット配布枚数　約 10 万枚

令和 6 年度高校大学生向けワークショップに係るリーフレット配布枚数　約 3 万枚

②ホームページ等による情報発信の実施

参加者募集やイベント実施、事業実施結果の情報発信のため、WEB ページを作成すること。また、県と連携して、SNS 等を用いた効果的な情報発信を行うこと。

（５）独自提案（任意）

（１）～（４）の取組を効果的に実施するための独自提案を受け付ける。

なお、提案内容については、県、受託者及び体験先企業・開催地域等の関係機関と協議した上で、その実施の可否も含めて内容を決定する。

（６）プログラム実施に係る参加者アンケートの実施

プログラム実施後に参加者アンケートを実施し、集計・分析したデータを提出すること。なお、アンケートの内容や実施方法については、県と協議の上、決定することとし、集計・分析したデータに基づき作成した製作物の著作権は県に帰属する。

（７）報告書の作成

受託者は、業務の完了後、委託業務の事業内容及び成果が分かる実績報告書（様式任意・収支決算報告書を含む）を電磁的記録により作成し、令和 8 年 3 月 24 日（火曜日）までに県に提出し、3 月 31 日（火曜日）までに県の確認を受けること。

なお、報告書の作成にあたっては、提出期限の 2 週間前までに素案を作成し、予め県の確認を受けること。

また、本業務に係る制作物については、速やかに電磁的記録で納品を行うこととし、電磁的記録での納品は、納品データを用いて県ホームページで活用できるよう、必要なコンテンツの他、テキストデータ、画像データ等とすること。

６　その他基本事項

（１）情報管理体制

①体制及び情報取扱者

受託者は本事業で知り得た情報を適切に管理するため、別記 1「データ保護及び管理に関する特記仕様書」に記載する事項について遵守すること。

②確保すべき履行体制

契約を履行する一環として契約相手方が収集、整理、作成等した一切の情報が、県が保護を要さないと確認するまでは、情報取扱者名簿に記載のある者以外に伝達又は漏えいされないことを保証する履行体制を有していること。

県が個別に承認した場合を除き、親会社等の契約相手方に対して指導、監督、業務支援、助言、監査等を行う者を含む、一切の契約相手方以外の者に対して伝達又は漏えいされないことを保証する履行体制を有していること。

③情報の開示

本事業で知り得た一切の情報について、情報取扱者以外の者に開示してはならない。ただし、県の承認を得た場合は、この限りでない。

④体制及び情報取扱者の変更

上記①の情報セキュリティを確保するための体制を定めた書面又は情報取扱者名簿に変更がある場合は、予め県へ届出を行い、同意を得なければならない。

（２）その他業務管理上の留意事項

①運営体制の整備

・受託者は、本業務が円滑に実施される体制を構築するため、運営責任者及び主たる担当者を定めた上で、必要かつ適切な人員配置を行うこと。
・運営責任者は及び主たる責任者は、やむを得ない場合を除いて変更してはならない。
・緊急時における危機管理対応を含め、安全・確実に業務が実行できる対応とすること。また、偶発的な事故が発生した場合に備えるため、イベント等保険に加入すること。

②実施状況の管理

・受託者は、本業務を着手するに当たり、支援メニューごとに「実施計画書」及び「実施要領」等を作成し、事前に県の確認を受けること。
・受託者は、県と定期的に連絡をとり、その指示を受けること。
・受託者がマスコミ等からの取材を受けた場合は、原則として県に引き継ぐこと。

③経費

・県が実施するもの以外の本業務の実施に要する一切の費用（起業家・講師・メンター等への謝金、開催に係る費用（会場費ほか)、関係機関への協力金、リーフレット等の印刷費、タブレット等の支援機材の賃借料など）は、委託料に含むこと。
・ただし、備品等財産の取得に関わる費用は含めないものとする。

④著作権の譲渡等

・成果物の所有権は、全て県に帰属するものとする。
・成果物が、著作権法（昭和 45 年法律第 48 号）第 2 条第 1 項第 1 号に規定する著作物に該当する場合、受託者は、当該著作物に係る受託者の著作権（著作権法第 21 条から第 28 条までに規定する権利をいう）を、当該著作物の引渡時に県に無償で譲渡するものとする。
・受託者は、県の書面による事前の同意を得なければ、著作権法第 18 条（公表権）及び第 19 条（氏名表示権）を行使することができない。

⑤納入物品に関する責任

・本業務に係る全ての納入物品について、受託者が最終的な責任を負う。

⑥外部との交渉記録の作成

・受託者が直接やり取りをする相手との交渉過程及び合意事項等については、記録・保管すること。

・受託者から外部に発出する文書及び資料等については、内容等について事前に県の確認を受けること。

⑦各種資料等の作成

・受託者は、県が求める場合は、速やかに資料等を作成の上、紙媒体ないし電磁的記録で提出すること。

・受託者は、作成部数及びデータ形式等に関して、県の指示に従う。

⑧その他

・受託者は、本業務の処理上知り得た情報を他に漏らしてはならない。

・受託者は、契約期間満了後のホームページの保持について、契約期間終了後においても公開状態を継続するよう努めること。

・受託者は、本業務を通じて取得した全ての個人情報について、別記 2「個人情報等取扱特記事項」及び別記 3「特定個人情報等取扱特記事項」を遵守すること。また、本業務によって知り得た個人情報及び通常秘密とされる企業情報を本業務の目的以外に使用してはならない。委託期間が終了又は委託契約が解除された後においても同様とすること。

・原則として、受託者は委託業務の全部又は一部を第三者に再委託してはならない。ただし、再委託先や内容、理由を明記し、書面により県の承諾を事前に得た場合は、この限りでない。

・受託者は、本業務の経理を明確にするため、受託者は他の経理と明確に区分して会計処理を行うこと。

・委託業務の実施に伴い、第三者に与えた損害は、県の責に帰すべきものを除き、全て受託者の責任において処理すること。

・感染症の再拡大や天災等の想定外の事態が生じた場合は、県と協議のうえ対応を決定する。その際、中止または変更となる場合においては契約金額の範囲内で、県は、実際に要した経費をもとに県と受託者間で協議して取り決めた金額を支払う。

別記１

別記　データ保護及び管理に関する特記仕様書

第１ 目的

本契約において取り扱う各種データについて、適正なデータ保護・管理方策及び情報システムのセキュリティ方策ついて明確にすることを目的とする。

第２ 適用範囲

本契約を履行するに当たり、出版、報道等により公にされている情報を除き、千葉県（以下「発注者」という。）が交付若しくは使用を許可し、又は契約の相手方（以下「受注者」という。）が作成若しくは出力したものであって用紙に出力されたものを含む全ての情報（以下「電子データ等」という。）を対象とする。

第３ 対象とする脅威

本書において対象とする脅威は、次に掲げる情報セキュリティが侵害された又はそのおそれがある場合とする。

（１）不正プログラムへの感染（受注者におけるものを含む。）

（２）サービス不能攻撃によるシステムの停止（受注者におけるものを含む。）

（３）情報システムへの不正アクセス（受注者におけるものを含む。）

（４）書面又は外部記録媒体の盗難又は紛失（受注者におけるものを含む。）

（５）機密情報の漏えい・改ざん（受注者におけるものを含む。）

（６）異常処理等、予期せぬ長時間のシステム停止（受注者におけるものを含む。）

（７）発注者が受注者に提供した又は受注者にアクセスを認めた発注者の電子データ等の目的外利用又は漏えい

（８）アクセスを許可していない発注者の電子データ等への受注者によるアクセス

（９）意図しない不正な変更等（受注者におけるものを含む。）

第４ 本契約を履行する者が遵守すべき事項

受注者は、本契約の履行に関して、以下の項目を遵守すること。

４．１ 業務開始前の遵守事項

受注者は、以下の（1）から（6）までの各項目に定める事項及び契約内容を一部再委託する場合は（7）に定める事項を取りまとめた「データ管理計画書」を作成し、業務開始前までに発注者の承認を得ること。

なお、行政手続き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）による個人番号及び特定個人情報（以下「特定個人情報等」という。）を取扱う業務の場合は、他の電子データ等と明確に区分して管理することとし、特定個人情報の適正な取扱いに関するガイドラインに基づく安全管理措置について、「データ管理計画書」の各事項へ、追加で記載すること。

（1）データ取扱者等の指定

受注者は、電子データ等を取り扱う者（以下「データ取扱者」という。）及び、データ取扱者を統括する者（以下「データ取扱責任者」という。）を指定し、その所属、役職及び氏名等を記入した「データ取扱者等名簿」を作成すること。

また、特定個人情報等を扱う業務の場合は、特定個人情報等を明確に管理するため、特定個人情報等を取り扱う者（以下「特定個人情報ファイル取扱者」という。）及び特定個人情報ファイル取扱者を統括する者（以下「特定個人情報ファイル取扱責任者」という。）についても併せて指定し、「データ取扱者等名簿」に記載すること。

なお、データ取扱者、データ取扱責任者、特定個人情報ファイル取扱者及び特定個人情報ファイル取扱責任者（以下「データ取扱者等」という。）は、守秘義務等のデータの取扱いに関する社内教育、又はこれに準ずる講習等を受講した者とし、その受講実績も併せて「データ取扱者等名簿」に記入すること。

（2）データ取扱者等への教育・周知計画

受注者は、データ取扱者等を対象とした、本契約での電子データ等の取扱いや漏えい防止等の教育及び周知に関する「データ取扱者等への教育・周知計画」を作成すること。

（３）電子データ等の取扱いにおける情報セキュリティ確保の措置計画

受注者は、本契約に係る電子データ等の取扱いに関し、電子データ等の保存、運搬、複製及び破棄並びに電子データ等の保管場所を変更する場合において実施する措置を記載した「データ取扱計画」を作成すること。「データ取扱計画」には、以下に示す措置を含めること。

（ア）本契約の作業に係る電子データ等を取り扱うサーバ、パソコン、モバイル端末について、アクセス制御及び脅威に関する最新の情報を踏まえた不正プログラム対策及び脆弱性対策を行うこと。

（イ）機密性２以上の電子データ等の取扱いは、発注者又は受注者のいずれかの管理下にない情報システム等（データ取扱者等の個人所有物であるパソコン及びモバイル端末を含む。）を用いることを原則として禁止し、必要がある場合は発注者の許可を得て用いること。

（ウ）電子データ等名称、データ取扱者名、授受方法、使用目的、使用場所、保管場所、保管方法、返却方法、授受日時、返却日時、特定個人情報等の有無等を記録する「データ管理簿」を整備すること。

（エ）機密性２以上の電子データ等の保存に、発注者又は受注者のいずれかの管理下にない情報システム等又は電磁的記録媒体（データ取扱者等が私的に契約しているサービス及びデータ取扱者等の個人所有物である電磁的記録媒体を含む。）を用いることを原則として禁止し、必要がある場合は発注者の許可を得て用いること。

（オ）データ取扱責任者又は特定個人情報ファイル取扱責任者が、データ取扱者又は特定個人情報ファイル取扱者の作業に立ち会うなど適切な管理を行うこと。

（カ）データ取扱責任者又は特定個人情報ファイル取扱責任者が、データ取扱者又は特定個人情報ファイル取扱者が作業を終了し作業場所を離れる際は、データの持ち出しの有無を厳重に検査すること。

（キ）機密性２以上の電子データ等を電子メールにて送信する場合には、暗号化を行うこと。

（４）外部設置における情報セキュリティ確保の措置計画

受注者は、発注者が指定する場所以外に情報システム機器を設置（外部設置）し、本契約に係る電子データ等を取扱う場合は、情報セキュリティ確保のために、部外者

の侵入等の意図的な情報漏えい等を防止する措置を記載した「外部設置における情報セキュリティ措置計画」を作成すること。「外部設置における情報セキュリティ措置計画」には以下に示す措置を含めること。

（ア）情報システムにアクセス（一般向けに提供されているウェブページへのアクセスを除く。）する作業は、受注者の管理下にあり、部外者の立入りが制限された場所において行うこと。

（イ）電子データ等を取り扱うパソコン、モバイル端末等について、盗難、紛失、表示画面ののぞき見等による漏えいを防ぐための措置を講ずること。また、それらの措置を講じていないパソコン、モバイル端末等を用いた作業を制限すること。

（ウ）入退室記録、作業記録等を蓄積し、不正の検知、原因特定に有効な管理機能を備えること。

（５）外部接続における情報セキュリティ確保の措置計画

受注者は、発注者が指定するネットワーク以外のネットワークへ接続（以下「外部接続」という。）し、本契約に係る電子データ等を取扱う場合は、情報セキュリティ確保のために、外部のネットワークからの侵入や改ざんを防御する措置を記載した「外部接続におけるセキュリティ措置計画」を作成すること。「外部接続におけるセキュリティ措置計画」には、以下に示す措置を含めること。

（ア）外部接続箇所にファイアウォールを設置し、不要な通信の遮断を行うこと。

（イ）外部接続箇所に侵入検知システムを設置し、ネットワークへの不正侵入の遮断を行うこと。

（ウ）外部接続箇所で不正な通信を検出した場合、発注者へ通報を行うこと。

（６）情報セキュリティが侵害された又はそのおそれがある場合における対処手順

受注者は、本契約に係る業務の遂行において情報セキュリティが侵害された又はそのおそれがある場合に備え、事前に連絡体制を整備し、発生した場合の対処手順を記載した「情報セキュリティ侵害時対処手順」を作成すること。「情報セキュリティ侵害時対処手順」には、以下に示す対処を含めること。

（ア）作業中に、情報セキュリティが侵害された又はそのおそれがあると判断した場合には、直ちに、発注者に、口頭にてその旨第一報を入れること。発注者への第一報は、

情報セキュリティインシデントの発生を認知してから１時間以内に行うこと。

（イ）当該第一報が行われた後、発生した日時、場所、発生した事由、関係するデータ取扱者等を明らかにし、平日の午前９時から午後５時の間は１時間以内に、それ以外の時間帯は３時間以内に発注者に報告すること。また、当該報告の内容を記載した書面を遅延なく発注者に提出すること。

（ウ）発注者の指示に基づき、対応措置を実施すること。

（エ）発注者が指定する期日までに、発生した事態の具体的内容、原因、実施した対応措置を内容とする報告書を作成の上、発注者に提出すること。

（オ）再発を防止するための措置内容を策定し、発注者の承認を得た後、速やかにその措置を実施すること。

（７）再委託における情報セキュリティの確保の措置計画

受注者は、本契約内容について一部再委託（更に順次行われる再委託を含む。）する場合、受注者が業務を実施する場合に求められる水準と同一水準の情報セキュリティ対策を再委託先において確保させる必要があり、再委託先における情報セキュリティの十分な確保を受注者が担保するとともに、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、「再委託における情報セキュリティ措置計画」を作成すること。なお、特定個人情報等を取扱う業務を再委託したときは、発注者が行う再委託先の管理状況等の確認について、受注者は必要な協力を行うこと。

４．２ 業務実施中における遵守事項

（１）「データ管理計画書」に基づく情報セキュリティ確保

「データ管理計画書」に記載した、データ取扱者等への教育・周知、電子データ等の取扱い及び作業場所等の情報セキュリティ確保のための措置を実施すること。

（２）データ管理簿への記録

受注者は、データ取扱者等が電子データ等を取り扱う場合、「データ管理簿」に記録し、データ取扱責任者に確認させること。また、特定個人情報等を扱う業務の場合、特定個人情報ファイル取扱責任者に併せて確認させること。

（３）「データ管理計画書」の変更

（ア）受注者は、本契約に基づく請負作業中に、次の事項について作業開始前に提出した「データ管理計画書」の内容と異なる措置を実施する場合は、事前に「データ管理計画書」の変更について発注者に提出し、承認を得ること。また、承認された変更の内容を記録し保存すること。

・データ取扱者等の異動を行う場合

・データ取扱者等に対する教育・周知の計画を変更する場合

・電子データ等の取扱いに関する計画又は作業場所等の情報セキュリティ確保のための措置を変更する場合

・再委託先及び再委託先の情報セキュリティ対策を変更する場合

（イ）一時的に「データ管理計画書」とは異なる措置を実施する場合は、原則として事前にその旨を発注者へ提出し、承認を得ること。ただし、情報セキュリティが侵害された又はそのおそれがある場合など緊急を要する場合等の場合、受注者は、実施内容について事後速やかに発注者へ報告すること。

（４）業務の報告・監査等

（ア）受注者は、発注者へ業務実施中の「データ管理計画書」の遵守状況について定期的に報告すること。

（イ）受注者は、発注者が「データ管理計画書」に係る管理状況について監査を要請した時は、定期・不定期にかかわらず、これを受け入れること。

（ウ）受注者は、「データ管理計画書」の評価、見直しを行うとともに、必要な改善策等について、発注者へ提案すること。

（５）情報セキュリティ対策の履行が不十分であった場合の対応

受注者の本契約に係る作業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発注者が判断した場合、受注者は発注者と協議の上、必要な是正措置を講ずること。また、是正措置の内容を「データ管理計画書」に反映させること。

４．３ 業務完了時の遵守事項

（１）データ返却等処理

受注者は、本契約に基づく業務が完了したときは、「データ管理簿」に記録されている全てのデータについて、返却、消去、廃棄等の措置を行うものとし、処理の方法、日時、場所、立会者、作業責任者等の事項を記した、「データ返却等計画書」を事前に発注者へ提出し、承認を得た上で処理を実施すること。

また、特定個人情報等を扱う業務の場合は、特定個人情報等であることを「データ返却等計画書」に明示すること。

（２）作業後の報告

受注者は、「データ返却等計画書」に基づく処理が終了したときは、その結果を記載した「データ管理簿」を発注者へ提出すること。

（３）情報セキュリティ侵害の被害に関する記録類の引渡し

受注者は、本契約の業務遂行中に情報セキュリティが侵害された又はそのおそれがある事象が発生した場合、４．１（６）に基づいて取得し保存している記録類を発注者に引き渡すこと。

４．４ 記憶装置の修理及び廃棄等におけるデータ消去

受注者は、契約により発注者が利用する情報システム機器の修理及び廃棄、リース返却（以下、「廃棄等」という。）の場合、記憶装置から、全ての電子データ等を消去の上、復元不可能な状態にする措置（以下、「抹消措置」という。）を実施すること。

（１）抹消措置計画の作成

受注者は、「データ管理計画書」へ作業予定日時、作業予定場所、実施予定者氏名、データ完全消去区分、使用機材名・数量、データ消去対象記憶装置リスト、立会者などを記載した「抹消措置作業計画」を追加するとともに、必要に応じてその他の措置内容を変更したうえ、抹消措置実施日（賃貸借契約の場合は賃貸借期間満了日）の３０日前までに発注者に提出し、承認を得ること。

また、賃貸借契約の場合は賃貸借期間満了日から３０日以内に抹消措置実施日を設

定すること。

（２）抹消措置実施方法

ア マイナンバー利用事務系の領域において住民情報を保存する記憶媒体の抹消措置の方法

（ア）当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすること。なお、対象となる機器について、リース契約による場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行うこと。

（イ）職員が抹消措置の完了まで立ち会いによる確認を行う。ただし、庁舎外で抹消措置を行う場合は、庁舎内において、一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態までデータの消去を行い、職員が作業完了を確認した上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の証拠写真が添付された完了証明書により確認できること。

イ 機密性２以上に該当する情報を保存する記憶媒体（上記アに該当するものを除く。）の抹消措置の方法

（ア）一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うこと。

（イ）庁舎内において、一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態までデータの消去を行い、職員が作業完了を確認した上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認できること。

ウ 機密性１に該当する情報を保存する記憶媒体の抹消措置の方法

（ア）一般的に入手可能な復元ツールの利用によっても情報の復元が困難な状態に消去すること。

（イ）庁舎内においてデータの消去を実施し、職員が作業完了を確認するなど適正な方法により確認できること。

エ ＩｏＴ機器を含む特殊用途機器の抹消措置の方法

（ア）デジタル複合機などのＩｏＴ機器を含む特殊用途機器に保存された電子データ等の漏えいの対策について、国際標準に基づくセキュリティ要件と同等以上のセキュリティ要件とその要件に適合した第三者認証（「ＩＴ製品の調達におけるセキュリティ

要件リスト」適合製品など）を取得している機能を有する場合は、当該機能によるデータ消去をもって抹消措置とすることができる。

（イ）庁舎内においてデータの消去を実施し、職員が作業完了を確認するなど適正な方法により確認できること。

（３）抹消措置の報告

受注者は、抹消措置実施日から３０日以内に、作業日時、実施者氏名、データ完全消去区分、使用機材名・数量、データ消去対象記憶装置リスト、立会者及び全ての記憶装置について抹消措置前後の写真を添付した「抹消措置完了報告書」を発注者へ提出し、承認を得ること。

第５ 情報システムの情報セキュリティ要件

受注者は、本契約により情報システムを導入する場合は、対象となる以下の項目を遵守すること。

５．１ 侵害対策

（１）通信回線対策

（ア）通信経路の分離

不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを通信回線上で分離するとともに、業務目的、所属部局等の情報の管理体制に応じて内部のネットワークを通信回線上で分離すること。

（イ）不正通信の遮断

通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。

（ウ）通信のなりすまし防止

情報システムのなりすましを防止するために、サーバの正当性を確認できる機能を備えるとともに、許可されていない端末、サーバ装置、通信回線装置等の接続を防止する機能を備えること。

（エ）サービス不能化の防止

サービスの継続性を確保するため、情報システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減する機能を備えること。

（２）不正プログラム対策

（ア）不正プログラムの感染防止

不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。

（イ）不正プログラム対策の管理

システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該

機能の動作状況及び更新状況を一元管理する機能を備えること。

（３）脆弱性対策

（ア）構築時の脆弱性対策

情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。

（イ）運用時の脆弱性対策

運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。

５．２ 不正監視・追跡

（１）ログ管理

（ア）ログの蓄積・管理

情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、発注者が指定する期間保管するとともに、不正の検知、原因特定に有効な管理機能（ログの検索機能、ログの蓄積不能時の対処機能等）を備えること。

（イ）ログの保護

ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能及び消去や改ざんの事実を検出する機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざんの脅威の軽減）のための措置を含む設計とすること。

（ウ）時刻の正確性確保

情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。

（２）不正監視

（ア）侵入検知

不正行為に迅速に対処するため、情報システムで送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知する機能を備えること。

（イ）サービス不能化の検知

サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。

５．３ アクセス・利用制限

（１）主体認証

情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体の認証を行う機能として、ＩＤ／パスワードの方式を採用し、主体認証情報の推測や盗難等のリスクの軽減を行う機能として、パスワードの複雑性及び指定回数以上の認証失敗時のアクセス拒否などの条件を満たすこと。

（２）アカウント管理

（ア）ライフサイクル管理

主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。

（イ）アクセス権管理

情報システムの利用範囲を利用者の職務に応じて制限するため、情報システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。

（ウ）管理者権限の保護

特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。

５．４ 機密性・完全性の確保

（１）通信経路上の盗聴防止

通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信内容を暗号化する機能を備えること。

（２）保存情報の機密性確保

情報システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存できないようにすることに加えて、保存された情報を暗号化する機能を備えること。

（３）保存情報の完全性確保

情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。

５．５ 情報窃取・侵入対策

（１）情報の物理的保護

情報の漏えいを防止するため、記憶装置のパスワードロック、暗号化等によって、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。

（２）侵入の物理的対策

物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置すること。

５．６ 障害対策（事業継続対応）

（１）システムの構成管理

情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハード

ウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。

（２）システムの可用性確保

サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として１日を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。

５．７ サプライチェーン・リスク対策

（１）受注者（再委託先含む）において不正プログラム等が組み込まれることへの対策

情報システムの構築において、発注者が意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。当該品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。

（２）調達する機器等に不正プログラム等が組み込まれることへの対策

機器等の製造工程において、発注者が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。

５．８ 利用者保護

（１）情報セキュリティ水準低下の防止

情報システムの利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。

（２）プライバシー保護

情報システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。

別記２

個人情報等取扱特記事項

第１　基本的事項

乙は、個人情報等の保護の重要性を認識し、この契約による事務の実施に当たっては、個人の権利利益を侵害することのないよう、個人情報等の取扱いを適正に行う。

第２　事務従事者への周知及び監督

（事務従事者への監督）

１　乙は、この契約による事務を行うために取り扱う個人情報等の適切な管理が図られるよう、事務従事者に対して必要かつ適切な監督を行う。

（事務従事者への周知）

２　乙は、事務従事者に対して、次の事項等の個人情報等の保護に必要な事項を周知させるものとする。

(1) 事務従事者又は事務従事者であった者は、その事務に関して知り得た個人情報等をみだりに他人に知らせてはならないこと

(2) 事務従事者又は事務従事者であった者は、その事務に関して知り得た個人情報等を不当な目的に使用してはならないこと

第３　個人情報等の取扱い

（収集の制限）

１　乙は、この契約による事務を行うために個人情報等を収集するときは、当該事務の目的を達成するために必要な範囲内で、適法かつ公正な手段によりこれを行う。

（秘密の保持）

２　乙は、この契約による事務に関して知り得た個人情報等をみだりに他人に知らせてはならない。この契約が終了し、又は解除された後においても、同様とする。

（漏えい、滅失及びき損の防止等）

３　乙は、この契約による事務に関して知り得た個人情報等について、個人情報等の漏えい、滅失及びき損の防止その他の個人情報等の適切な管理のために必要な措置を講じる。

（持ち出しの制限）

４　乙は、甲が承諾した場合を除き、この契約による事務を甲が指定した場所で行い、個人情報等が記録された機器、記録媒体、書類等（以下「機器等」という。）を当該場所以外に持ち出してはならない。

（目的外利用及び提供の制限）

５　乙は、甲の指示がある場合を除き、個人情報等をこの契約の目的以外の目的のために利用し、又は甲の承諾なしに第三者に対して提供してはならない。

（複写又は複製の制限）

６　乙は、この契約による事務を処理するために甲から引き渡された個人情報等が記録された機器等を甲の承諾なしに複写又は複製してはならない。

第４　再委託の制限

乙は、甲が承諾した場合を除き、この契約による事務については自ら行い、第三者にその取扱いを委託してはならない。

第５　事故発生時における報告

乙は、この契約に違反する事態が生じ、又は生じるおそれのあることを知ったときは、速やかに甲に報告し、甲の指示に従うものとする。

第６　情報システムを使用した処理

乙は、情報システムを使用してこの契約による事務を行う場合には、この特記事項のほか、最高情報セキュリティ責任者（総務部デジタル改革推進局デジタル推進課が所管する千葉県情報セキュリティ対策基準（平成１４年３月１５日制定）５（１）アに規定する職にある者をいう。）の定める「データ保護及び管理に関する特記仕様書」等を遵守する。

第７　機器等の返還等

乙は、この契約による事務を処理するために、甲から提供を受け、又は乙自らが収集し、若しくは作成した個人情報等が記録された機器等は、この契約完了後直ちに甲に返還し、又は引き渡すものとする。ただし、甲が別に作業の方法を指示したときは、当該方法によるものとする。

第８　甲の調査、指示等

（調査、指示等）

１　甲は、乙がこの契約により行う個人情報等の取扱状況を随時調査し、又は監査することができる。この場合において、甲は、乙に対して、必要な指示を行い、又は必要な事項の報告若しくは資料の提出等を求めることができる。

（公表）

２　甲は、乙がこの契約により行う事務について、情報漏えい等の個人情報等を保護する上で問題となる事案が発生した場合には、個人情報等の取扱いの

態様、損害の発生状況等を勘案し、乙の名称等の必要な事項を公表することができる。

第９　契約の解除及び損害の賠償

甲は、次の各号のいずれかに該当するときは、この契約を解除し、及び乙に対して損害の賠償を請求することができる。

(1) 乙又は乙の委託先(順次委託が行われた場合におけるそれぞれの受託者を含む。）の責めに帰すべき事由による情報漏えい等があったとき

(2) 乙がこの特記事項に違反し、この契約による事務の目的を達成することができないと認められるとき

注

１　「甲」は実施機関を、「乙」は受託者を指す。

２　委託に係る事務の実態に則して、適宜必要な事項を追加し、不要な事項は省略することとする（例：仮名加工情報、行政機関等匿名加工情報等及び匿名加工情報を取り扱う事務を委託しない場合には、「個人情報等」の「等」の記述を削除する)。

別記３

特定個人情報等取扱特記事項

第１　総則

（基本的事項）

１　乙は、特定個人情報及び個人番号（以下「特定個人情報等」という。）の保護の重要性を認識し、この契約による事務の実施に当たっては、個人の権利利益を侵害することのないよう、特定個人情報等の取扱いを適正に行う。

（法令等の遵守）

２　乙は、この契約による事務の実施に当たっては、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）その他の法令、「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」（平成 26 年特定個人情報保護委員会告示第５号。以下「ガイドライン」という。）等（以下「法令等」という。）を遵守する。

（安全管理のための規程）

３　乙は、組織として特定個人情報等を適正に取り扱うため、次の事項等をその内容に含む基本方針を定める。

⑴ 法令等を遵守することの宣言

⑵ 特定個人情報等の漏えい、滅失及びき損（以下「情報漏えい等」という。）の防止その他の特定個人情報等の安全管理のために必要な措置（以下「安全管理措置」という。）に関する事項

⑶ 質問及び苦情処理の窓口

４　乙は、次の事項等をその内容に含む取扱規程等をあらかじめ定め、特定個人情報等を取り扱うための体制及び情報システムを整備する。

⑴ 取得、利用、保存、提供、削除又は廃棄等（以下「利用等」という。）の特定個人情報等の管理の段階に応じた特定個人情報等の取扱方法

⑵ 特定個人情報等を取り扱う事務の管理の責めに任ずべき者（以下「責任者」という。）及び責任者が取り扱う特定個人情報等の範囲

⑶ 特定個人情報等を取り扱う事務を担当する者（以下「事務取扱担当者」という。）及び当該事務並びに事務取扱担当者が取り扱う特定個人情報等の範囲

５　乙は、特定個人情報等についての秘密を保持するために必要な事項を、就業規則等に定める。

第２　管理体制

（事故発生時等のための体制及び手順等の整備）

１　乙は、この契約若しくは取扱規程等に違反する事態又は情報漏えい等の事案が生じ、又は生じるおそれを責任者、事務取扱担当者その他の乙の指揮監督を受けてその事務に

従事している者（以下「事務従事者」という。）が把握した場合に、適切かつ迅速に対応するための体制及び手順等を整備する。

（記録の整備）

２　乙は、特定個人情報ファイルの利用、出力及び削除、特定個人情報等を記録した書類及び記録媒体等の持ち出し並びに機器等の廃棄の記録その他の取扱規程等に基づく運用状況を確認するための記録を整備する。

第３　研修等

（事務従事者への監督）

１　乙は、この契約による事務を行うために取り扱う特定個人情報等の適切な管理が図られ、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務従事者に対して必要かつ適切な監督を行う。

（事務従事者への周知）

２　乙は、事務従事者に対して、次の事項等の特定個人情報等の保護及び適正な取扱いに必要な事項を周知させる。

⑴　事務従事者又は事務従事者であった者は、その事務に関して知り得た特定個人情報等をみだりに他人に知らせてはならないこと

⑵　事務従事者又は事務従事者であった者は、その事務に関して知り得た特定個人情報等を不当な目的に使用してはならないこと

（事務従事者への研修等）

３　乙は、定期に、事務従事者に対し、特定個人情報等を取り扱うに当たって留意すべき事項等に関する研修等を行う。

第４　特定個人情報等の取扱い

（収集の制限）

１　乙は、この契約による事務を行うために特定個人情報等を収集するときは、当該事務の目的を達成するために必要な範囲内で、適法かつ公正な手段によりこれを行う。

（秘密の保持）

２　乙は、この契約による事務に関して知り得た特定個人情報等をみだりに他人に知らせてはならない。この契約が終了し、又は解除された後においても、同様とする。

（安全管理措置等）

３　乙は、安全管理措置その他の特定個人情報等の適切な管理のために必要な措置を講じる。

（持ち出しの制限）

４　乙は、甲が承諾した場合を除き、この契約による事務を甲が指定した場所で行い、特定個人情報等が記録された機器、記録媒体、書類等（以下「機器等」という。）を当該

場所以外に持ち出してはならない。

（取扱区域）

５　乙は、特定個人情報等を取り扱う事務を実施する場所及び特定個人情報ファイルを取り扱う情報システムを管理する場所（以下「取扱区域」という。）を明確に定め、安全管理措置を講じる。

（持ち出し）

６　乙は、甲が承諾した範囲において、機器等を取扱区域から持ち出す場合には、機器等を紛失したときに第三者に個人番号が知られることがないように措置を講じ、持ち出した後に機器等の所在を特定できる手段を利用する等、安全な方法でこれを行う。

（目的外利用の禁止）

７　乙は、特定個人情報等を、この契約の目的以外の目的のために利用してはならない。

（複写又は複製の制限）

８　乙は、この契約による事務を処理するために甲から引き渡された特定個人情報等が記録された機器等を甲の承諾なしに複写又は複製してはならない。

（削除又は廃棄）

９　乙は、機器等を廃棄する場合には、廃棄した機器等に記録されていた特定個人情報等を復元することができないようにする。

10　乙は、特定個人情報ファイルのうち特定個人情報等の一部を削除する場合には、削除した特定個人情報等を容易に復元することができないようにする。

11　特定個人情報等の廃棄又は削除は、甲が承諾した場合に限り、その作業を第三者に委託することができる。この場合においては、乙は、当該第三者が削除又は廃棄したことを証する書類を徴する等により確認する。

第５　再委託

（再委託の制限）

１　乙は、甲が承諾した場合を除き、この契約による事務については自ら行い、第三者にその取扱いを委託してはならない。

（再委託の契約）

２　乙は、この契約による事務について、第三者にその取扱いを委託するときは、次の事項をその内容に含む契約を締結する。

⑴ 委託をしようとする者は、あらかじめ、甲の許諾を得なければならないこと

⑵ 委託を受けた者は、「第４　特定個人情報等の取扱い」に定める措置その他の甲が乙に対して委託するときの特定個人情報等の適切な管理のために必要な措置と同一の措置を講じること

⑶ 更に順次委託が行われる場合において、その順次行われたそれぞれの委託の委託をした者と委託を受けた者との間の契約について、上記⑴及び⑵の事項をその内容に

含む契約を締結しなければならないこととすること

（再委託についての通知）

３　乙は、この契約による事務について、第三者にその取扱いを委託したときは、その旨及び契約を締結したことを証する書類その他甲が求める書類を、甲に対して送付する。

（再委託先の監督）

４　乙は、この契約による事務について、第三者にその取扱いを委託したときには、当該第三者を適切に監督する責任を負う。当該第三者が再委託その他の順次行われる委託をしたときには、乙は、その受託者を適切に監督する責任を負う。

第６　安全確保上の問題への対応

（事故発生時における報告）

１　乙は、この契約に違反する事態が生じ、又は生じるおそれのあることを知ったときは、速やかに甲に報告し、甲の指示に従うものとする。

（情報漏えい等の事案の発生時における措置）

２　乙は、情報漏えい等の事案が生じ、又は生じるおそれのあることを知ったときは、当該事案による被害又は当該事案に類似する事案の発生を防止するため、次の措置を講じる。

⑴ 事実の調査及び原因の究明

⑵ 影響を受けるおそれのある者への連絡

⑶ 甲並びにガイドラインの「第 3-6　特定個人情報の漏えい事案等が発生した場合の対応」に従った個人情報保護委員会への報告

⑷ 再発を防止するための取り組み等（以下「再発防止策」という。）の検討及び決定

⑸ 事実、再発防止策及びその他必要な事項の公表

第７　監査及び点検の実施

（把握）

１　乙は、特定個人情報等の取扱いの状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない。

（監査及び点検）

２　乙は、特定個人情報等の取扱いの状況について、定期に又は随時、監査又は点検を実施する。ただし、乙は、乙以外のものに、監査を実施させることを妨げない。

第８　情報システムを使用した処理

乙は、情報システムを使用してこの契約による事務を行う場合には、この特記事項のほか、最高情報セキュリティ責任者（総務部デジタル改革推進局デジタル推進課が所管する千葉県情報セキュリティ対策基準（平成 14 年 3 月 15 日制定）5 ⑴ アに規定する職にあ

る者をいう。）の定める「データ保護及び管理に関する特記仕様書」等を遵守する。

第９　機器等の返還等

乙は、この契約による事務を処理するために、甲から提供を受け、又は乙自らが収集し、若しくは作成した特定個人情報等が記録された機器等は、この契約完了後直ちに甲に返還し、又は引き渡すものとする。ただし、甲が別に作業の方法を指示したときは、当該方法によるものとする。

第10　甲の調査、指示等

（調査、指示等）

１　甲は、乙がこの契約により行う特定個人情報等の取扱状況を随時調査し、又は監査することができる。この場合において、甲は、乙に対して、必要な指示を行い、又は必要な事項の報告若しくは資料の提出等を求めることができる。

（公表）

２　甲は、乙がこの契約により行う事務について、情報漏えい等の特定個人情報等を保護する上で問題となる事案が発生した場合には、特定個人情報等の取扱いの態様、損害の発生状況等を勘案し、乙の名称等の必要な事項を公表することができる。

第11　契約の解除及び損害の賠償

甲は、次の各号のいずれかに該当するときは、この契約を解除し、及び乙に対して損害の賠償を請求することができる。

⑴　乙又は乙の委託先（順次委託が行われた場合におけるそれぞれの受託者を含む。）の責めに帰すべき事由による情報漏えい等があったとき

⑵　乙がこの特記事項に違反し、この契約による事務の目的を達成することができないと認められるとき

注

１　「甲」は実施機関を、「乙」は受託者を指す。

２　委託に係る事務の実態に則して、及び当該事務において取り扱われる特定個人情報等の内容、当該特定個人情報等に係る本人（個人情報によって識別される特定の個人をいう。）の数、事務取扱担当者の数及び過去における情報漏えい等の有無等に照らして、適宜必要な事項を追加し、不要な事項は省略することとする。