令和５年度経済産業省デジタルプラットフォーム構築事業（次期 RESAS システム構築・運用保守業務）

仕様書

令和４年１２月

経済産業省地域経済産業グループ地域経済産業調査室

1.プロジェクトの背景と目的

1.1 背景・目的

- 我が国の経済発展に向け、地域経済の活性化は非常に重要な課題である。この課題解決のためには、地域経済の現状を把握し、そこから得られた地域特性に応じた施策の立案及び適切な執行が欠かせない。上記の問題意識の下、産業構造、ヒト・モノ・カネの流れなど地域経済の実態を把握するためのツールとして平成27年４月より「地域経済分析システム(RESAS)（以下「本システム」という。）を運用している。
- 本システムは令和４年 12 月現在、84 のメニューより地域経済にかかわる様々なビッグデータを可視化しており、主に地方自治体における政策立案等の用途を中心に利用されている。それと同時に、地方自治体以外のユーザー層も拡大しつつあり、多様なニーズが生まれている。引き続き、地方自治体からのニーズを充足しつつ、地方自治体以外のユーザーへのニーズへも的確に応えていくために、新たな機能やユーザーインターフェースの向上等を実現するシステムのアーキテクチャの改革を検討、実行する必要がある。
- また、デジタル・ガバメント推進方針（平成 29 年５月 30 日）も踏まえつつ、行政コストの更なる省力化に加え、利用者の利便性向上に対応するべく、本システムのデータを常に最新の状況に保ち、データ更新の一層の迅速化を図り、地方自治体のみならず経済産業省（以下「当省」という。）をはじめとする中央省庁において効果的かつ効率的な政策立案を推進していく上で必要なシステム改修を行っていくことが必要である。
- 第２期まち・ひと・しごと創生総合戦略ではRESASについて次のように言及されている。
  - 地域経済分析システム（以下「RESAS」という。）について、データ拡充やシステム周知等を中心に取り組んできた結果、データの充実等について評価を得た一方で、地方公共団体の政策立案時の RESAS の利活用においては改善の余地があるとされた。これを踏まえ、今後は、更に政策立案等に資するよう、RESAS の機能拡充に加え利活用の促進等を図る。
  - 地域経済の実態を踏まえた政策立案や地域企業の経営に資するため、RESAS のデータ拡充やシステム改善等を行うことでユーザービリティを高めるなど、一層の利活用に向けた環境整備を図る。

1.2 本事業の目的

運用開始から８年が経過したRESASは、以下の課題を抱えている。

（１）中長期的なRESASの在り方を考慮したシステム見直し

- 現状の描画処理に対して、開発当初の設計思想で構築された作り込みのプログラム構造のため、描画の速度改善検討が技術的に限界となっている。最新技術を踏まえた抜本的な構造見直しが必要。
- GIS 機能を搭載していない等、新たなニーズや変化に即応する基盤が無いため、機能変更が難しい。
- データ絶対量の増加による DB 拡張費などシステム維持コストの抑制。
- システム全体の統制コストの抑制。(画面ごとの独立した描画プログラムによるコスト、一部機能改善が他に及ぼす影響が検証できないなど)
- データの自動更新など将来的に想定される機能拡充への配慮が必要。

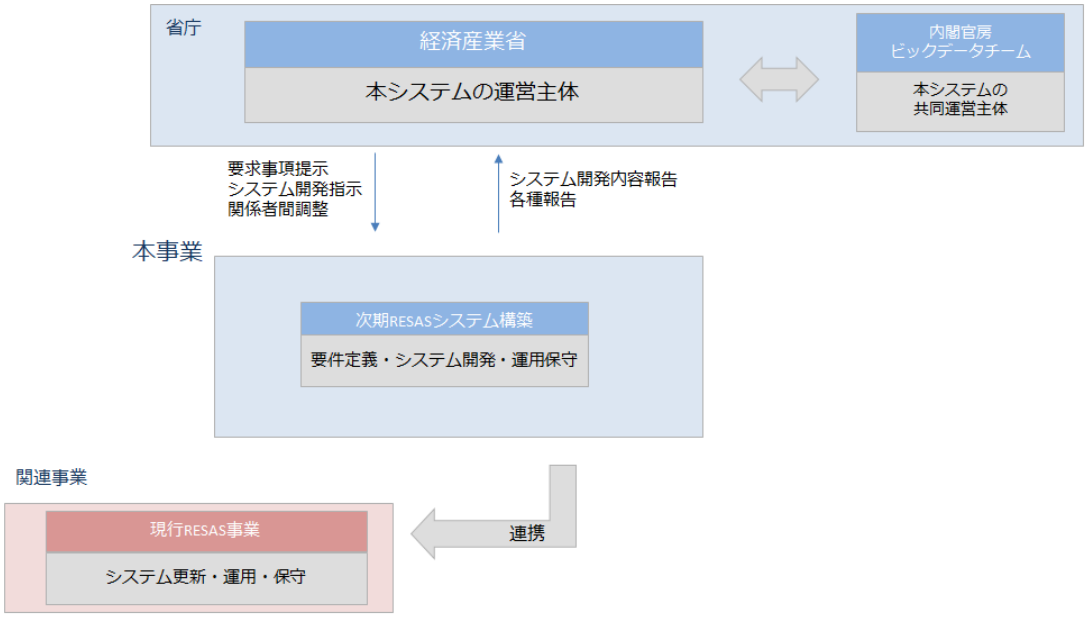
（２）ユーザーの拡大

- 自治体関係者をターゲットとしたデータ整備となっており、国（EBPM を踏まえた政策立案）や企業（効率的なマーケティング）等には有効活用されていない。
- 利用者がデータを利用・加工することが困難な仕様となっており、利用が伸び悩んでいる。既存ユーザー層に対してもニーズを的確に捉えて、ユーザーの幅だしを図る必要がある。
- 第２期まち・ひと・しごと創生総合戦略において、「政策立案や地域企業の経営に資するため（中略)、一層の利活用に向けた環境整備を図る」とされたことも踏まえ、地方自治体等の公共機関に加え、民間企業・支援機関等の幅広いユーザー層による利活用を促していくことが必要。

これらの課題を踏まえて、システムの見直しが必要となっている。令和４年度事業では、RESAS の将来的なシステム更改（以下「次期 RESAS」という。）に向けたシステムの基盤検証及び設計を行った。令和５年度ではその結果を元に、次期 RESAS システムの構築及び本番リリース後の運用保守を行う。

1.3 関係者

・ 本事業における関係者を以下に示す。



RESAS システム及び関連アプリケーションは、内閣官房デジタル田園都市国家構想実現会議事務局ビッグデータチーム（以下「内閣官房ビッグデータチーム」という。）との共同開発を行っている。内閣官房ビッグデータチームにおいては、RESAS の利活用促進のための各種アプリケーション構築・運用を実施している。本事業を遂行するにあたり、必要に応じて内閣官房ビックデータチームとの連携を図る。また、現在稼働中の RESAS システム（以下「現行 RESAS」という。）に対する事業とも連携を図る。

2. 事業内容

2.1 事業全体に係る作業

（１）業務計画書の作成

受託者は、作業体制、作業内容及び業務スケジュール等について記載した業務計画書を作成し、委託契約締結日から 10 営業日以内に当省に提出すること。作業体制には、作業責任者、個人情報取扱責任者及び作業担当者の氏名、所属、担当作業、指揮命令系統、情報セキュリティ対策に係る管理・連絡体制、連絡先を記載すること。

（２）定例会議等の開催

当省と各業務担当間の連絡調整のため、オンライン又は当省を会場として事業の進捗報告等を行う会議を定期に開催する。開催頻度については、当省

と相談し決定することとするが、週１回の開催を基本とすること。また、その議事録については、会議実施の翌日から起算して２営業日以内に作成の上、当省に提示し了承を得ること。なお、オンラインによる定例会議等の開催の際は当省が指定するコミュニケーションツールを使用すること。

2.2 次期 RESAS 構築に向けた要件定義業務

（別添）「令和５年度経済産業省デジタルプラットフォーム構築事業（次期 RESAS システム構築)」に記載された要求事項を満たす機能要件を検討すること。詳細な対応スケジュールを立案した上で当省に提示すること。

2.3 次期 RESAS システム開発業務

「令和４年度次期 RESAS 構築に向けた基盤検証事業」で検討された機能及び、「2.2 次期 RESAS 構築に向けた要件定義業務」にて検討した機能について、システム開発を行う。「8.主なスケジュール」に従い、次期 RESAS システムの本番リリースまでを行う。本番リリースまでの各工程における詳細な対応スケジュールを立案した上で当省に提示すること。

2.3.1 システム開発対象マップ

次期 RESAS システム開発は、現行 RESAS のデータを移行して構築を行う。次期 RESAS システム構築対象は 20 メニューを見込むこととし、詳細な移行対象については、「11.入札に係る資料の閲覧について」を参照すること。

2.4 次期 RESAS システム運用・保守業務

「2.3 次期 RESAS システム開発業務」で本番リリースした次期 RESAS システムの運用・保守を行う。

(1)システム稼働環境の整備と稼働

システム稼働に必要なシステム基盤を整備し、適切に稼働させること。システムの稼働要件等については、「**エラー！ 参照元が見つかりません。**」や「11.入札に係る資料の閲覧について」を参照すること。

なお、令和６年度事業における受託者（受託予定者）にシステム稼働環境を引き継ぐ必要が生じる場合を想定し、本事業の受託者は、システム稼働環境の利用者としての権利、及び運用・保守業務を行うに当たり作成、使用した手順書、ツール、業務遂行のために有効なノウハウ等まとめた資料などの一式を電子データにてまとめ、次年度受託事業者へ円滑に引き継

ぐために必要な手続等の業務引継ぎ作業を契約期間終了時までに行うこと。

(2)システム運用・保守の定期作業（日次・週次・月次）の実施

以下に定める作業を実施する。以下に定める作業は契約期間中、土曜日、日曜日、国民の祝日に関する法律（昭和 23 年法律第 178 号）に定める休日及び令和５年 12 月 29 日から令和６年１月３日以外のすべての日（以下、「営業日」という。）において実施すること。日次作業においてリソースの逼迫や緊急対応の必要などが予見される場合、当省へ通知し、事前の対応策について合意の上、対策を行うこと。

なお、夜間、休日等においては、システムの自動監視などを活用し、業務時間外におけるシステム障害やアラートなどを検知できる仕組みを整え、障害や不具合の発生時には「2.4(7)障害時対応、緊急時対応」に定める障害対応フローを取れるよう体制を整備すること。

対象は「2.3 次期 RESAS システム開発業務」で本番リリースした次期 RESAS システムとし、現行 RESAS は対象外とする。

作業時期	作業項目	詳細
日次作業	システム稼働確認	本システムが正常に稼働していることを確認すること。
	パッチ検証調査	本システムで使用しているソフトウェア、ミドルウェア等について、パッチ検証調査を実施する。影響度及び緊急度等を勘案して緊急で適用すべきパッチか否かを２営業日以内に判断する。特に緊急を要する場合は即時関係者へ電話及びメールで連絡し対策を協議すること。 なお、契約末日及びその前日に公開されたパッチについては、適用の必要性について判断の上、次年度の受注者にその情報を引き継ぐこと。
	各リソースの使用量、状況確認	ディスク、メモリ、CPU 使用率などを確認し、必要に応じて拡張対応や縮小対応を行うこと。
	ウイルス定義ファイルの更新	ウイルス定義ファイルの更新を確認し、正常に自動更新されていない場合には手動更新を実施すること。

	ログ確認	本システムのログを確認し、異常や不正アクセスが発生していないかチェックを行うこと。
週次作業	運用状況週次報告書（各リソースの週次使用量、状況確認）の提出	ディスク、メモリ、CPU 使用率、ページビュー（以下「PV」という。）数などの週間推移を確認し、必要に応じて拡張・縮小検討や抜本的な対応等の要否について検討すること。
	システムメンテナンス	本システムで使用しているソフトウェア、ミドルウェア等について、パッチ適用調査を実施する。影響度及び緊急度等を勘案して適用すべき対応等がある場合は、影響調査及び適用確認試験等を実施した上で、システム稼働環境に適用する。また、適用後の動作確認試験についても実施する。
月次作業	PV 数等の集計、Web アクセス月次報告書の提出	本システムへのアクセス回数、ユニークユーザー数、ユーザーの属性等を集計する。月次報告書には上記の月次確認結果を取りまとめ、当省に報告を行うこと。
事業終了時までの作業	システム概要ドキュメントの更新	本システムのサーバ構成や利用技術、アプリケーションの連関等を示したドキュメントを最新の状態に更新すること。
	セキュリティ診断作業	第三者のセキュリティ診断を受診し、指摘事項について対応を行うこと。セキュリティ診断及び指摘事項への対応は、事業終了時までに実施すること。 なお、セキュリティ診断の第三者性を担保するため、受託者自身やその関連会社等、第三者性が認められないセキュリティ診断の実施は不可とする。ツール等の活用により客観性が保たれる場合については、ツール等による結果の診断についても客観性が保たれることを条件に、その実施方法や概要について当省に相談し、当省の合意の上で利用すること。
	変更管理の取	システム変更や障害、障害対応等について

	りまとめ報告書	取りまとめ、当省に報告を行うこと。

(3)アプリケーションの保守作業

アプリケーションについて、ウェブブラウザやシステム基盤のソフトウェア、OS 等のアップデート、システム更新、サービス不具合等に伴い仕様通りに動作しない事象が発見された場合は、当省と協議し、必要に応じて仕様通りに動作するよう修正作業や更新作業を実施すること。

(4)システム運用・保守業務及び関連する問合せ対応

ユーザーからの本システムの運用・保守に関する問合せへの対応及びユーザーからの問合せ対応において効率化の検討を行う。問合せ対応は管理表にて一元管理し、それぞれの対応状況について進捗管理を行い、漏れなく対応を行うこと。ユーザーからの問合せについて、ユーザーとの直接の連絡は当省が行うが、技術的課題の解決において受託者からの直接の連絡が有効な場合にはこの限りではない。効率化の検討に当たっては、効率化の実現に必要となる事項や課題等を検討し、当省と協議の上、必要となる対応を実施すること。

(5)システム基盤の最適化に向けた検討・実施

本システムのシステム構成、ネットワーク構成、サーバ構成の資料を基に、定期的に現状のシステム状態について詳細に調査し、サーバ、OS、ミドルウェア、ソフトウェア、ネットワーク等の構成において最適化すべき事項、システム更改の必要性等及び実装に向け必要となる事項、工数等を整理し取りまとめ、当省と協議の上、最適化に向けた必要な実装を行うこと。また、運用上においてオペレーションの効率化が図れる事項なども合わせて検討し、当省の了承の上で必要な改善を図ること。

(6)システムセキュリティ施策の実行と運用

システム全体や搭載データを保護するためのセキュリティ施策を講じて、ぜい弱性への対応やシステム監視等を適切に実行すること。不正な通信やアクセス、システム改ざん、ウイルス感染等のインシデントが発生した場合には、計画書に明記した緊急対応体制と対応方法に従い、直ちに当省に通知を行い、対策を立案し、速やかに適切な措置を行うこと。

(7)障害時対応、緊急時対応

本項に定める作業は契約期間中、受託者が不具合発生を認識した時点又は当省から通知があった時点から速やかに対応すること。また、年度当初に提出する業務計画書へ、具体的な対応フローや体制について記載すること。

対応事項	内容
緊急時一次受けエスカレーション	本システムの不具合発生に伴い検知又は連絡を受け付け、速やかに当省へ連絡、エスカレーションを実施する。
一次報告	障害内容について、発生日時、障害種別（インフラ障害、アプリケーション障害、セキュリティインシデント等)、原因、影響範囲、暫定対応、恒久対応案等の中から判明している事象について記載し、不具合発生の検知又は連絡を受けてから６時間以内に関係者全体へメールにて連絡を行う。
不具合解析と報告	システムの不具合について原因を解析し、対応策を検討する。緊急度に応じた頻度で関係者へ周知する。
不具合復旧対応	不具合復旧のための対策を実施し、復旧後に関係者への報告等を実施する。
障害報告書の作成	障害内容について、発生日時、障害種別（インフラ障害、アプリケーション障害、セキュリティインシデント等)、原因、影響範囲、暫定対応、恒久対応、再発防止策等を取りまとめた報告書を作成し、障害発生日から３営業日以内に当省へ提出する。

(8)システム更新作業に伴うテスト及びリリース作業の支援

本番リリース対応後に発生する不具合対応や、ユーザーからの問合せに対する改修によって生じるシステム更新作業において、本番環境への更新データの投入や改修項目の反映を行う際には、事前に検証環境（以下「ステージング環境」という。）を準備し、総合テスト及び受入れテストの支援を実施の上、本番環境へのリリース作業を行い、リリース作業が完了した旨を当省に連絡すること。また、リリース作業にてステージング環境、本番環境への変更が行われる際、変更概要については都度変更管理、構成管理を行い、履歴を残すこと。

2.5 遵守すべきガイドライン等

・ 本事業の実施に当たっては、原則として「デジタル・ガバメント推進標準ガイドライン」（https://www.digital.go.jp/resources/standard_guidelines/）等に記載された事項を遵守すること。また、今後契約期間中に当該文書が改定された場合にはそれに従うこととするが、より良い作業の進め方あるいは開発手法について提案がある場合には、当省に提示し、協議の上認められたものについては実施することができる。

3. 機能要件

次期 RESAS システムにおける機能要件について、詳細な内容については、「11. 入札に係る資料の閲覧について」に記載のある資料を閲覧すること。

3.1 データ基本要件

本システムでは、次期 RESAS システム開発は、現行 RESAS のデータを移行して構築を行うため、データ仕様は現行 RESAS を踏襲し、以下の通りと定義する。なお現行 RESAS からの移行に際して、以下の定義で変更の必要が生じた場合は当省と協議の上、方針を決定することとする。

3.1.1 データルールの定義

・ 以下の定義に従い、現行 RESAS で扱うデータが作成されるが、このデータを次期 RESAS システム上でも正しく表示できるよう設計すること。

項目	内容	データの状態
値について	小数点以下の表示	小数点以下の数値を表示させている場合、小数点以下２桁を基本的にシステム上で表示させること。（小数点以下３桁目を四捨五入） ※マップによっては表示が異なるため、マップの仕様に従うこと。
	原典データにおいて、データがない場合	ブランク（空白の状態）となる。システム上は、表示データがない旨のメッセージを表示すること。
	原典データにおいて、秘匿処理がされて	ｘ（小文字のエックス）となる。システム上は表示データがない旨のメッセージを表示する。

	いる場合	秘匿処理がなされている地域を合算機能で合算した場合、どの地域が秘匿のために合算されていないのかをシステム上で示せることが望ましい。
	計算不可（0÷0など）	ハイフンとなる。システム上は表示データがない旨のメッセージを表示する。
	%の表記	数値とする。%等の文字列はシステム側で表示させること。
コード	市区町村コード、業種コードなどの数値でなるコード	公的機関にて公表されているコード体系に従ったデータとなるため、これを踏襲しシステム側で活用すること。
ファイル形式	改行コード	CRLF
	拡張子	CSV 形式のデータで作成。文字列の記述は、ダブルクォーテーションで囲まない形式で納品される。
エリアの表記方法	都道府県名、市区町村名の表記	データ形式は以下。 都道府県：都道府県名付き（例：東京都） 市区町村名：市区町村名付き（例：札幌市中央区） ※○○郡△△町などの郡名は除外される ＝「△△町」と記載 ※東京都特別区については区名のみとする
	コードと名称	コードと名称は併記される。システム上においてエリアコードは表示させていない。
	政令指定都市	市のデータも作成される（例：札幌市は札幌市の値と、各区の値がそれぞれ作成される） ※システムの表示原則としては現行のマップ別の仕様に従うこと。
	世界の地域区分	アジア、ヨーロッパ等の地域区分が各マップで異なる場合があるため注意すること。 例： 輸出入統計…貿易統計に基づく地域区分（アジア州、北アメリカ州、ヨーロッパ州、南アメリカ州、アフリカ州、大洋州）

		免税取引…独自体系（アジア、北米、欧州、中南米、アフリカ、大洋州、中東）
ファイルの区分方法	納品ファイルの集計単位（地域区分）	全国、都道府県、市区町村はそれぞれファイルを分けて作成される。
エリアの表記方法	座標⇒コードと名称付加	貿易統計、特許については都道府県コードと名称、市区町村コードと名称が記載されている。
項目名	項目名の記載方法	データ仕様書に基づいて、項目名と並びが設定されている。
増減率	増減率のデータ形式	例：北海道で人口が 2010 年⇒2015 年で３%増加の場合、カラムは都道府県コード、都道府県名、年（2015）、増減率（0.03000）となる。 ※原則としては現行のマップ別の仕様に従うこと。
増減率、平均値	増減率、平均値	対象マップにより異なるため、データ仕様書に基づいて作成されている。
単位	金額	対象マップにより単位が異なるため、データ仕様書に基づいて作成されている。
値について	市区町村合併	最新の市区町村コードに基づき作成されている。 （2012 年にＡ市とＢ市が合併してＸ市になった場合、Ｘ市の人口などは 2011 年以前もＡ市＋Ｂ市の値とする）
増減率	算出方法	（本年－前年）/前年　※値は 0.2、-0.2 などとなる。
文字コード	Shift JIS/UTF-8 の取扱い	ダウンロードデータは Shift-JIS とする。システム側の文字コードは UTF-8 とする。

3.2 Web 要件

本システムにおける Web 要件を以下に示す。

3.2.1 デザイン

・ 本システムの Web デザインの基本要件を以下に記す。

HTML5 で整備すること。

レスポンシブデザインを基本に、スマートフォン等の多用な端末に対応できるようにすること。（レスポンシブデザインが必須ではないが、スマートフォンやタブレット等でも画面が確認できるようにすること）

以下のブラウザに対応すること。

ア Microsoft Edge

イ Google Chrome

ウ Safari

- 文字コード指定等で文字が正しく表示されること。
- Schema.org に対応可能なページは対応すること。
- 画面上のマップのプロットやグラフにおいて、色覚多様性を考慮し識別しやすい配色とすること。
- マップやグラフが印刷資料等に使用される際に、文字つぶれ等が起きないフォントサイズとすること。また、グラフや文字の色、太さについて、識別しやすい色とすること。
- Web デザインの詳細に関しては、デジタル庁が提供する各種目的別 Web サイトガイドを参照すること。
（https://www.digital.go.jp/resources/standard_guidelines/）

3.2.2 ドメイン

・ 本システムのドメインの基本要件を以下に記す。

- ドメイン取得と管理については、ドメイン管理ガイドライン（https://www.digital.go.jp/resources/standard_guidelines/）を参照すること。

3.2.3 外部サービスの利用

・ 本システムの外部サービスの利用の基本要件を以下に記す。

- マップ・グラフ画面、データ出典一覧画面においてデータ出典元の Web サイトをリンクさせる場合には、リンク先の情報がエラーとならないよう、最新化を行うこと。
- マップ画面で利用している地図画像データベースやマップ内の検索機能（Yahoo! Open Local Platform）等、外部サービスを利用して実現している機能について、仕様変更等の情報を収集し、変更が生じる場

合には本システム側で表示や検索の不具合が発生しないよう、あらかじめ対処法を立案して対応すること。

3.2.4 ダウンロード

本システムのダウンロード機能の基本要件を以下に記す。

マニュアルや利活用事例集等、リンク先のファイルが PDF の場合は、ファイル形式、サイズを記入すること。必要なファイルについては日付も記載すること。また、データダウンロード機能で取得可能な CSV ファイル、ZIP についても、容量が 5MB 以上の場合はダウンロードボタン上にファイルサイズ容量の記載があると望ましい。

データダウンロードファイルは再編集可能な形式でファイルを提供すること。また、利用者の利便性を考慮し、文字コードは Shift-JIS とすること。

ダウンロードファイルが複数ファイルある場合には、ファイル圧縮ソフト等を使い複数ファイルをブロック単位でダウンロード可能にすること。

ダウンロードファイルの容量が大きい場合、ネットワークエラーが発生する可能性があるため、ファイル分割やデータの軽量化の検討を行うこと。

3.2.5 https

本システムの暗号化機能の基本要件を以下に記す。

- インターネットを介して通信する情報の盗聴及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするため、TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講じること
- 必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること

3.2.6 クラウドサービス

政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ）において登録されたサービスから調達することを原則とすること。

3.2.7 利用規約

本システムの利用規約等に変更が生じる場合、当省の指示に基づき迅速

に変更を行うこと。

4. 非機能要件

次期 RESAS システムにおける非機能要件について、詳細な内容については、「11.入札に係る資料の閲覧について」に記載のある資料を閲覧すること。

5.体制

- 以下に、次期 RESAS システム構築に向けた役割、要員の要件を記すので、これらを満たす体制を構築すること。また、業務計画書において詳細な体制図を記載すること。
- なお、不具合等に対しては速やかに原因を特定し、解消の対応ができる体制を構築すること。
- 契約締結後に要員に対する変更が生じる場合は、その 10 営業日前までに以下の資格を有することを証明できる書類を提出し、当省の承諾を得ること。また、要員の変更に当たっては十分な引継ぎ期間を設け、事業に支障を来さないようにすること。

役割	主な作業内容	要員の要件
要件定義担当者	・システム構築に向けた要件定義を担当する。	要件定義担当者は、以下要件を満たすこと。また、最低１名を本事業に配置すること。 ・統計・データ分析の実務経験を36ヶ月以上有する者

役割	主な作業内容	要員の要件
プロジェクトマネージャ	・システム更新業務全体の方針立案や策定を行う。 ・システム設計・開発の進捗管理、課題管理等を行う。	プロジェクトマネージャは、以下の①又は②の要件を満たす者であること。また、最低１名を本事業に配置すること。 ①以下のいずれかの資格を有する者。 ・経済産業大臣認定「情報処理技術者（プロジェクトマネージャ)」 ・米国 PMI 認定「プロジェクトマネジメントプロフェッショナル（PMP)」 ②情報システムの設計・開発に係るプロジェクト管理の実務経験を36か月以上有する者。
システム設計担当者	・システムの仕様決定及び設計を担当する。	システム設計担当者のリーダーとなる者は、以下の①又は②の要件を満たすこと。また、リーダーとなる者を含め最低１名を本事業に配置すること。 ①以下の資格を有する者。 ・経済産業大臣認定「情報処理技術者（システムアーキテクト）」 ②情報システムの設計・開発業務の実務経験を36か月以上有する者。

役割	主な作業内容	要員の要件
システム開発担当者	・システムの開発に必要な作業を担当する。	システム開発担当者のリーダーとなる者は、以下の①又は②の要件を満たすこと。また、リーダーとなる者を含め最低３名を本事業に配置すること。 ①以下の資格を有する者。 ・経済産業大臣認定「情報処理技術者（システムアーキテクト）」 ②情報システムの開発業務の実務経験を36か月以上有する者。
システム運用・保守担当者	・システムの運用・保守に必要な作業を担当する。	運用・保守担当者のリーダーとなる者は、以下の①又は②の要件を満たすこと。また、リーダーとなる者を含め最低１名を本事業に配置すること。 ①情報システムの設計・開発業務又は運用・保守業務を実施した経験を36ヶ月以上有する者。 ②以下のいずれかの資格を有するもの、あるいはそれと同等の能力を有することが客観的に証明できる者。 ・情報処理技術者（ITサービスマネージャ）（経済産業省） ・ ITIL Foundation 認定資格（ITIL2011）

役割	主な作業内容	要員の要件
情報セキュリティ担当者	・情報システムに関するセキュリティを担当する。	情報セキュリティ担当者となる者は、以下の①又は②の要件を満たすこと。また、最低１名を本事業に配置すること。 ①以下のいずれかの資格を有する者。 ・経済産業大臣認定「情報処理安全確保支援士」 ・経済産業大臣認定「情報処理技術者（情報セキュリティスペシャリスト）」 ②情報システムのセキュリティ関連業務の実務経験を36か月以上有する者。

6. 情報セキュリティに関する事項

以下の事項について遵守すること。

1) 受託者は、契約締結後速やかに、情報セキュリティを確保するための体制並びに以下 2)～18)に記載する事項の遵守の方法及び提出を求める情報、書類等（以下「情報セキュリティを確保するための体制等」という。）について、経済産業省（以下「当省」という。）の担当職員（以下「担当職員」という。）に提示し了承を得た上で確認書類として提出すること。ただし、別途契約締結前に、情報セキュリティを確保するための体制等について担当職員に提示し了承を得た上で提出したときは、この限りでない。また、定期的に、情報セキュリティを確保するための体制等及び対策に係る実施状況を紙媒体又は電子媒体により報告すること。加えて、これらに変更が生じる場合は、事前に担当職員へ案を提出し、同意を得ること。

なお、報告の内容について、担当職員と受託者が協議し不十分であると認めた場合、受託者は、速やかに担当職員と協議し対策を講ずること。

2) 受託者は、本業務に使用するソフトウェア、電子計算機等に係る脆弱性対策、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策、アクセス制御対策、情報漏えい対策を講じるとともに、契約期間中にこれらの対策

に関する情報セキュリティ教育を本業務にかかわる従事者に対し実施すること。

3) 受託者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）の取扱いには十分注意を払い、当省内に複製が可能な電子計算機等の機器を持ち込んで作業を行う必要がある場合には、事前に担当職員の許可を得ること。なお、この場合であっても、担当職員の許可なく複製してはならない。また、作業終了後には、持ち込んだ機器から情報が消去されていることを担当職員が確認できる方法で証明すること。

4) 受託者は、本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体）について、担当職員の許可なく当省外で複製してはならない。また、作業終了後には、複製した情報が電子計算機等から消去されていることを担当職員が確認できる方法で証明すること。

5) 受託者は、本業務を終了又は契約解除する場合には、受託者において本業務遂行中に得た本業務に関する情報（紙媒体及び電子媒体であってこれらの複製を含む。）を速やかに担当職員に返却し、又は廃棄し、若しくは消去すること。その際、担当職員の確認を必ず受けること。

6) 受託者は、契約期間中及び契約終了後においても、本業務に関して知り得た当省の業務上の内容について、他に漏らし、又は他の目的に利用してはならない。

なお、当省の業務上の内容を外部に提供する必要が生じた場合は、提供先で当該情報が適切に取り扱われないおそれがあることに留意し、提供の可否を十分に検討した上で、担当職員の承認を得るとともに、取扱上の注意点を示して提供すること。

7) 受託者は、本業務の遂行において、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の対処方法について担当職員に提示すること。また、情報セキュリティが侵害され、又はそのおそれがあることを認知した場合には、速やかに担当職員に報告を行い、原因究明及びその対処等について担当職員と協議の上、その指示に従うこと。

8) 受託者は、「経済産業省情報セキュリティ管理規程（平成 18･03･22 シ第 1 号)」、「経済産業省情報セキュリティ対策基準（平成 18･03･24 シ第 1 号)」及

び「政府機関等のサイバーセキュリティ対策のための統一基準群（令和３年度版）」（以下「規程等」と総称する。）を遵守すること。また、契約締結時に規程等が改正されている場合は、改正後の規程等を遵守すること。

9)　受託者は、当省又は内閣官房内閣サイバーセキュリティセンターが必要に応じて実施する情報セキュリティ監査、マネジメント監査又はペネトレーションテストを受け入れるとともに、指摘事項への対応を行うこと。

10)　受託者は、本業務に従事する者を限定すること。また、受託者の資本関係・役員の情報、本業務の実施場所、本業務の全ての従事者の所属、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を担当職員に提示すること。なお、本業務の実施期間中に従事者を変更等する場合には、事前にこれらの情報を担当職員に再提示すること。

11)　受託者は、本業務を再委託（業務の一部を第三者に委託することをいい、外注及び請負を含む。以下同じ。）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、上記 1)から 10)まで及び 12)から 18)までの措置の実施を契約等により再委託先に担保させること。また、1)の確認書類には再委託先に係るものも含むこと。

12)　受託者は、外部公開ウェブサイト（以下「ウェブサイト」という。）を構築又は運用するプラットフォームとして、受託者自身（再委託先を含む。）が管理責任を有するサーバ等を利用する場合には、ＯＳ、ミドルウェア等のソフトウェアの脆弱性情報を収集し、セキュリティ修正プログラムが提供されている場合には業務影響に配慮しつつ、速やかに適用を実施すること。また、ウェブサイト構築時においてはサービス開始前に、運用中においては年１回以上、ポートスキャン、脆弱性検査を含むプラットフォーム診断を実施し、脆弱性を検出した場合には必要な対策を実施すること。

13)　受託者は、ウェブサイトを構築又は運用する場合には、インターネットを介して通信する情報の盗聴及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするため、TLS(SSL)暗号化の実施等によりウェブサイトの暗号化の対策等を講じること。

　なお、必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いること。

14) 受託者は、ウェブサイト上のウェブアプリケーションの構築又は改修を行う場合には、独立行政法人情報処理推進機構が公開する最新の「安全なウェブサイトの作り方」（以下「作り方」という。）に基づくこと。また、ウェブアプリケーションの構築又は更改時においてはサービス開始前に、運用中においてはウェブアプリケーションへ修正を加えた場合や新たな脅威が確認された場合に、「作り方」に記載されている脆弱性の検査等（ウェブアプリケーション診断）を実施し、脆弱性を検出した場合には必要な対策を実施すること。併せて、「作り方」のチェックリストに従い対応状況を確認し、その結果を記入したチェックリストを担当職員に提出すること。なお、チェックリストの結果に基づき、担当職員から指示があった場合は、それに従うこと。

15) 受託者は、ウェブサイト又は電子メール送受信機能を含むシステムを構築又は運用する場合には、政府機関のドメインであることが保証されるドメイン名「.go.jp」を使用すること。

16) 受託者は、情報システム（ウェブサイトを含む。以下同じ。）の設計、構築、運用、保守、廃棄等（電子計算機、電子計算機が組み込まれた機器、通信回線装置、電磁的記録媒体等のハードウェア又はソフトウェア（以下「機器等」という。）の調達を含む場合には、その製造工程を含む。）を行う場合には、以下を実施すること。

①各工程において、当省の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。また、具体的な管理手順や品質保証体制を証明する書類等を提出すること。

②情報システムや機器等に意図しない変更が行われる等の不正が見つかったときに、追跡調査や立入検査等、当省と連携して原因を調査し、排除するための手順及び体制を整備していること。これらが妥当であることを証明するため書類を提出すること。

③不正プログラム対策ソフトウェア等の導入に当たり、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有するソフトウェアを導入すること。

④情報セキュリティ対策による情報システムの変更内容について、担当職員

に速やかに報告すること。また、情報システムが構築段階から運用保守段階へ移行する際等、他の事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容を含めること。

⑤サポート期限が切れた又は本業務の期間中にサポート期限が切れる予定がある等、サポートが受けられないソフトウェアの利用を行わないこと、及びその利用を前提としないこと。また、ソフトウェアの名称・バージョン・導入箇所等を管理台帳で管理することに加え、サポート期限に関するものを含むソフトウェアの脆弱性情報を収集し、担当職員に情報提供するとともに、情報を入手した場合には脆弱性対策計画を作成し、担当職員の確認を得た上で対策を講ずること。

⑥電子メール送受信機能を含む場合には、SPF（Sender Policy Framework）等のなりすましの防止策を講ずるとともに SMTP によるサーバ間通信の TLS（SSL）化や S/MIME 等の電子メールにおける暗号化及び電子署名等により保護すること。

17) 受託者は、本業務を実施するに当たり、民間事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービス（ソーシャルメディアサービスを含む）を利用する場合には、これらのサービスで要機密情報を扱ってはならず、8）に掲げる規程等に定める不正アクセス対策を実施するなど規程等を遵守すること。なお、受託者は、委託業務を実施するに当たり、クラウドサービスを調達する際は、「政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ）」において登録されたサービスから調達することを原則とすること。

18) 受託者は、ウェブサイトの構築又はアプリケーション・コンテンツ（アプリケーションプログラム、ウェブコンテンツ等の総称をいう。以下同じ。）の開発・作成を行う場合には、利用者の情報セキュリティ水準の低下を招かぬよう、以下の内容も含めて行うこと。

①提供するウェブサイト又はアプリケーション・コンテンツが不正プログラムを含まないこと。また、そのために以下を含む対策を行うこと。

(a) ウェブサイト又はアプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。

(b) アプリケーションプログラムを提供する場合には、当該アプリケー

ションの仕様に反するプログラムコードが含まれていないことを確認すること。

（c）提供するウェブサイト又はアプリケーション・コンテンツにおいて、当省外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、ＨＴＭＬソースを表示させるなどして確認すること。

②提供するウェブサイト又はアプリケーションが脆弱性を含まないこと。

③実行プログラムの形式以外にコンテンツを提供する手段がない場合を除き、実行プログラム形式でコンテンツを提供しないこと。

④電子証明書を用いた署名等、提供するウェブサイト又はアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをウェブサイト又はアプリケーション・コンテンツの提供先に与えること。なお、電子証明書を用いた署名を用いるときに、政府認証基盤（ＧＰＫＩ）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。

⑤提供するウェブサイト又はアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳ、ソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更をＯＳ、ソフトウェア等の利用者に要求することがないよう、ウェブサイト又はアプリケーション・コンテンツの提供方式を定めて開発すること。

⑥当省外へのアクセスを自動的に発生させる機能やサービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がウェブサイト又はアプリケーション・コンテンツに組み込まれることがないよう開発すること。ただし、必要があって当該機能をウェブサイト又はアプリケーション・コンテンツに組み込む場合は、当省外へのアクセスが情報セキュリティ上安全なものであることを確認した上で、他のウェブサイト等のサーバへ自動的にアクセスが発生すること、サービス利用者その他の者に関する情報が第三者に提供されること及びこれらを無効にする方法等が、サービス利用者において容易に確認ができるよう、担当職員が示すプライバシーポリシー等を当該ウェブサイト又はアプリケーション・コンテンツに掲載すること。

7. その他の事項

(1) 著作権

① 本事業の納品物の著作権は、検収が完了した時点で当省に移転する。

② 受託者は、納品物の作成に当たり、第三者の著作権、工業所有権、ライセンス又はノウハウ（以下「著作権等」という。）を実施・使用するときは、その実施・使用に対する一切の責任を負う。また、受託者は、当省以外の組織において納品物を活用する場合に調整が必要となる著作権等を一覧にした「ライセンス等に関する報告書」を作成の上、提出する。

(2) 機密保持

① 機密保持

ア 当省が開示した情報、契約履行過程で生じた納品物（印刷した帳票を含む。）及び本事業の履行上知り得た一切の事項について、いかなる場合にもこれを当省が開示することを認めていない第三者に開示又は漏えいしてはならないものとし、そのために必要な措置を講じること。

なお、事業の実施上やむを得ず当省が提供した情報を第三者に開示する必要がある場合には、事前に当省と協議し了承を得ること。また、「機密保持体制表」を作成し、当省の了承を得ること。

上記の開示又は漏えい防止に関して当省の了承を得ることについては、本事業の委託期間終了後も同様とする。

イ 本事業の実施に当たって、受領、作成及び出力した一切の情報について、当省の許可なく事業実施場所から持ち出してはならない。

ウ 当省が提供する本事業に関連する文書等について、当省の了承を得た場所に保管し、原則として契約期間終了時までに返却又は裁断・溶解等の処分を行うこと。

エ 本事業の履行上発生したプログラム、データ及びその他納品物については、当省の許可なしに、事業実施場所から外部に持

ち出しや、外部からアクセスできる状態に置いてはならない。

オ　当省以外の物品等を事業実施場所へ持ち込み、又は当省の物品を事業実施場所から持ち出す場合は、事前に当省の許可を得ること。

カ　電子媒体によって運用するプログラム、データ及び文書等については、ウィルスチェックを実施すること。

② 個人情報の保護

ア　個人情報の取扱いに係る事項については、当省と協議の上決定し、書面で提出すること。また、個人情報の適正な取扱いを図るための責任者を選任し、併せて報告すること。

イ　個人情報を複製する際には、事前に当省の許可を得ること。ただし、複製の範囲は必要最小限とし、複製が不要となり次第、その内容が絶対に復元することができないように破棄・消去を実施すること。

ウ なお、受託者は廃棄作業が適切に行われたことを確認し、その保証をすること。

エ　受託者が、個人情報の取扱いにおいて適正な取扱いをしなかった場合は、本事業の契約解除の措置を受けることがある。

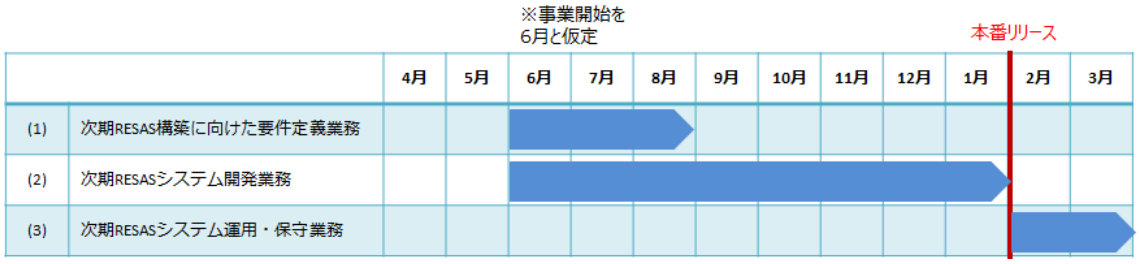
オ　受託者が、本事業を履行する上で個人情報の漏えい等、個人情報の秘密保持に反する行為及び安全確保の上で問題となる事案等を把握した場合には、直ちに当省に報告すること。

(3) その他

本仕様書に関して疑義が生じたとき又は本仕様書に定めがなく、かつ契約書にも記載のない事項については、当省と協議の上、指示に従うものとする。

8. 主なスケジュール

スケジュールについては以下を参照し、各工程の詳細スケジュールを立案し、当省と調整の上決定する。



9. 事業実施期間

・　委託契約締結日から令和６年３月 31 日まで

10. 納品物

10.1 納品物一覧

以下に定める納品物を指定する時期に納品すること。

(1)委託事業報告書

・納品媒体は、CD-R等の電子媒体（公表用２式）とし、PDF及び編集可能な電子ファイルとする。

・本納品物は公表用となるため、セキュリティ等の観点から、当省と協議の上、非公開とするべき部分については、削除するなどの適切な処置を講ずること。また、オープンデータ（二次利用可能な状態）として公開されることを前提とし、当省以外の第三者の知的財産権が関与する内容を報告書に盛り込む場合は、①事前に当該権利保有者の了承を得、②報告書内に出典を明記し、③当該権利保有者に二次利用の了承を得ること。二次利用の了承を得ることが困難な場合等は、二次利用未承諾リスト（様式２）に当該箇所を記述し併せて提出すること。

・令和６年３月31日までに提出すること。

※調査報告書電子ファイルの具体的な作成方法の確認及び様式１・様式２のダウンロードは、次の URL から行うこと。

<https://www.meti.go.jp/topic/data/e90622aj.html>

(2)業務計画書

・　委託契約締結日から 10 営業日以内に編集可能な電子ファイルにて提出すること。

(3)体制図

・ 第一版を委託契約締結日から 10 営業日以内に編集可能な電子ファイルにて提出すること。本事業実施期間中に体制に変更が発生する場合は、体制図を修正し速やかに当省に提出し承諾を得ること。

(4)運用状況週次報告書

・ 運用状況について、週次分を取りまとめたものを毎週第１営業日までに編集可能な電子ファイル又は紙媒体にて提出すること。

(5) Web アクセス月次報告書

・ Web アクセス月次報告書は、PV 数集計月の翌月の２営業日以内に編集可能な電子ファイルをメール添付にて提出すること。ただし、令和６年３月分については、令和６年３月 31 日までに提出すること。

(6)変更管理の取りまとめ報告書

・ 令和６年３月 31 日までに編集可能な電子ファイルにて提出すること。

(7)システム変更・障害対応報告書

・ 障害発生の都度、障害対応の状況について報告すること。

(8)第三者セキュリティ診断結果及び対策結果に関する報告書

・ 令和６年３月 31 日までに編集可能な電子ファイルにて提出すること。

(9)システム開発ドキュメント

令和６年３月 31 日までに編集可能な電子ファイルにて提出すること。また、変更が生じた場合は、提出期限を当省と相談の上、最新版を提出すること。

・ システム方式設計書
  - システム構成図
  - サーバ機能仕様一覧
  - ネットワーク概要図
・ システム運用設計書
  - 監視項目一覧
  - セキュリティ施策一覧
  - バックアップ設計書

・　システム設計書
　－　基本設計書、詳細設計書
　－　開発画面一覧表
　－　画面遷移図
　－　画面項目定義書
　－　テーブル定義書
　－　ソースコード
　－　各テスト実施計画書、項目書及びテスト実施結果
・　ライセンス等に関する報告書

(10)　「2.1(2)定例会議の開催」に定める議事録
・　会議実施の翌日から起算して２営業日以内に、編集可能な電子ファイルにて提出すること。
・　令和６年３月 31 日までに PDF 及び編集可能な電子ファイルにて提出すること。

(11)情報資産管理標準シート
・　令和６年３月 31 日までに PDF 及び編集可能な電子ファイルにて提出すること。

① 受注者は、デジタル・ガバメント推進標準ガイドライン「別紙２　情報システムの経費区分」に基づき区分等した契約金額の内訳を提出すること。

② 受注者は、情報資産管理標準シート改定版を、デジタル庁より作業依頼のある時期（原則毎年度末）に、提出すること。

※納品物については、他の納品物と同一の媒体に格納の上、納入して差し支えない。

10.2 納品場所
・　経済産業省地域経済産業グループ地域経済産業調査室

11.入札に係る資料の閲覧について
・　入札予定者は、当省の立ち合いの下、以下の資料を閲覧し、作業内容、作業ボリューム等について十分に理解した上で入札に参加すること。

・　資料を閲覧する場合、資料に記載のあるすべての事項について秘密を保持する旨の誓約書を提出の上、閲覧すること。

（閲覧可能資料（令和４年度事業における資料又は最新のもの））

・　現行 RESAS に関する資料
- システム構成図
- 開発画面一覧
- ソースコード
- マニュアル
- サーバ環境概要
- 運用状況月次報告書
- データ加工仕様書

・　次期 RESAS システム構築に向けた基盤検証成果物
- システム構成図
- ネットワーク概要図
- システム基盤構築検証結果
- 検証のために作成したソースコード一式

12.不開示情報の取扱いについて

１．情報管理体制

①受注者は本事業で知り得た情報を適切に管理するため、次の履行体制を確保し、発注者に対し「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）」及び「情報取扱者名簿」（氏名、個人住所、生年月日、所属部署、役職等が記載されたもの）様式１を契約前に提出し、担当課室の同意を得ること（住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当課室から求められた場合は速やかに提出すること。）。なお、情報取扱者名簿は、委託業務の遂行のため最低限必要な範囲で情報取扱者を掲載すること。

（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、経済産業省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。

②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又は漏えいしてはならないものとする。ただし、担当課室の承認を得た場合は、この限りではない。

③①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、予め担当課室へ届出を行い、同意を得なければならない。

２．履行完了後の情報の取扱い

国から提供した資料又は国が指定した資料の取扱い（返却・削除等）については、担当職員の指示に従うこと。業務日誌を始めとする経理処理に関する資料については適切に保管すること。

（別添）

情報取扱者名簿及び情報管理体制図

①情報取扱者名簿

		氏名	個人住所	生年月日	所属部署	役職	パスポート番号及び国籍（※４）
情報管理責任者（※１）	A						
情報取扱管理者（※２）	B						
	C						
業務従事者（※３）	D						
	E						
再委託先	F						

（※１）受託事業者としての情報取扱の全ての責任を有する者。必ず明記すること。

（※２）本事業の遂行にあたって主に保護すべき情報を取り扱う者ではないが、本事業の進捗状況などの管理を行うもので、保護すべき情報を取り扱う可能性のある者。

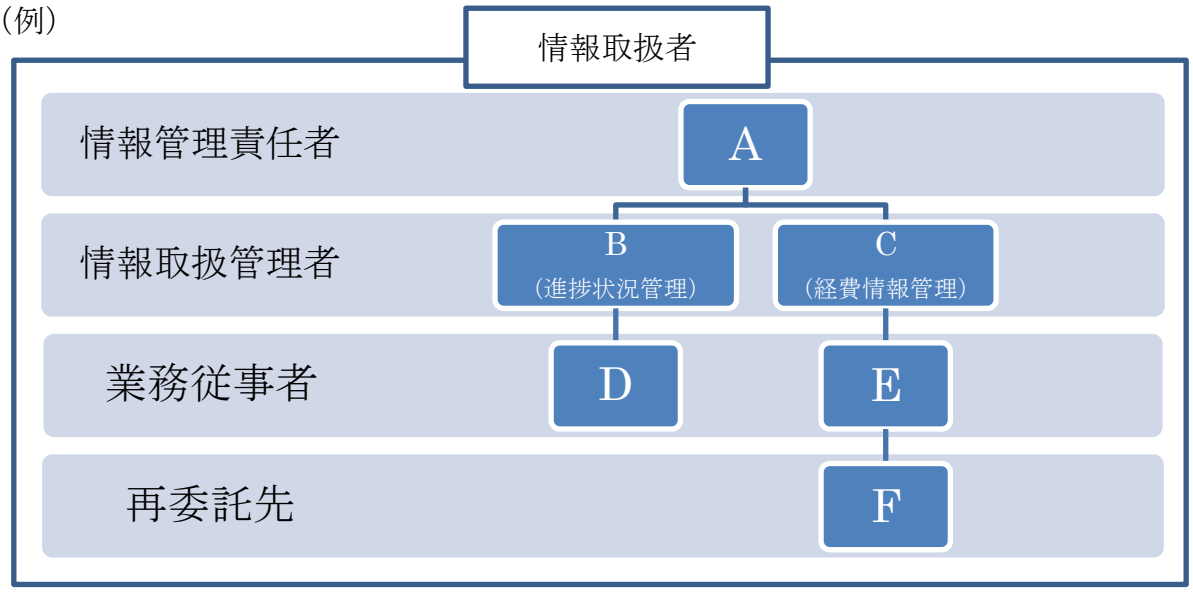
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※４）日本国籍を有する者及び法務大臣から永住の許可を受けた者（入管特例法の「特別永住者」を除く。）以外の者は、パスポート番号等及び国籍を記載。

（※５）住所、生年月日については、必ずしも契約前に提出することを要しないが、その場合であっても担当課室から求められた場合は速やかに提出すること。

②情報管理体制図

（例）



【情報管理体制図に記載すべき事項】

・本事業の遂行にあたって保護すべき情報を取り扱う全ての者。（再委託先も含む。）

・本事業の遂行のため最低限必要な範囲で情報取扱者を設定し記載すること。

以上