仕様書案

１．件　名：令和３年度事業環境変化対応型支援事業（デジタル化診断事業）

２．事業の目的（概要）

新型コロナウイルス感染症対応等の必要性が高まる中、中小企業がオンライン会議、テレワーク等のデジタル化・IT 活用を行うに当たって、専門家が支援する制度として実施していた。今後は、ウィズコロナ・ポストコロナ時代として中小企業を取り巻く環境が大きく変化する中で、中小企業がデジタル化の必要性について気付き、デジタル化に当たって必要な対応に取り組むことが重要。

これを踏まえ、令和３年度補正予算においては、自身のデジタル化の課題を明確化できるよう「デジタル化診断ツール」を開発し提供する事業を実施する。

また、中小企業が抱える様々な経営課題や支援ニーズに対応するための専門家派遣事業等の支援策を組み合わせ、商工会議所や金融機関等をはじめとした地域の支援機関とも相互に連携しながら、中小企業のデジタル化を積極的に促進する。

具体的には、デジタル化にまだ取り組めていない中小企業等の事業者を見据えて、デジタル化診断を実施する。有識者の意見等も踏まえながら、事業者に気付きの促しが可能な診断の設問を検討し、より多くの事業者が診断を受けられるような仕組みを設計する。また、診断を通して、中小企業が取り組むべき基礎的な取組の実施状況を確認した上で、実施できていない取組については、診断結果として、取り組むことによる効果や実際の取り組み方等を記載して取組を促していく。また、事業者が受けた診断結果の分析調査を行い、その調査結果を踏まえて今後の対応方針として、5 年後 10 年後に向けての中小企業のデジタル化促進の在り方の検討も行い、気付きを促す診断の自走ができるような設計検討も行う。

３．事業内容

（１）デジタル化診断ツール提供に向けた整備

① デジタル化診断シートの検討

自身のデジタル化の課題を明確化できるよう、デジタル化診断シートを作成し、後述の検討会に出席する有識者や支援機関等の関係者に内容を議論する場を設ける。実際にターゲットとなり得る中小企業等に対してサンプルで診断を受けてもらい、意見等をヒアリングして必要に応じて反映することとする。また、診断結果の内容や、中小企業の診断受診結果の分析の他、今後の中小企業のデジタル化の方向性等についても議論を行う。

② ホームページの作成

Web 版の「デジタル化診断シート」を掲載し、中小企業等が自ら診断を受けられるよう、ホームページを作成する。また、診断結果を踏まえて中小企業等が実際にデジタル化に取り組んだ内容（ベストプラクティス）の掲載や、関連のあるホームページ（支援策、支援機関等のページ）のリンクの掲載等を行うことにより、中小企業等の自己解決力を高め、このホームページを見れば中小企業等がデジタル化に取り組むことができるユーザーフレンドリーな情報提供を行うこととする。

③ 事業者への周知及び支援機関等との連携

特に、デジタル化の取組が進んでいない中小企業等に受診してもらうべく、本事業について周知を行う。事業規模については、PR 資料（※１）を参考とする。例えば、経営相談で地域の支援機関に訪問した中小企業等に対して、その場で診断を受けてもらえるような工夫を入れた上で、上述のホームページ上のデジタル化診断シートがスマホですぐに確認できるよ

うな QR コード付きのパンフレットの作成や、ネット広告等を行う。必要に応じて過去の委託事業成果（※２）を参考とする。また、支援機関等において受診がしやすいよう、支援機関等向けの説明資料の作成等を行う。支援機関等については、商工会議所、よろず支援拠点、認定経営革新等支援機関、IT コーディネータ協会、スマート SME サポーターの他、中小企業診断士、士業従事者、地域未来牽引企業等を想定しており、中小企業庁と相談・連携の上、調整を行う。なお、支援機関等向けの説明資料の作成に当たっては、支援機関等が担っている関連施策（例えば、事業環境変化対応型支援事業における研修プログラムの開発と伴奏支援の実施や各種相談窓口の体制強化）との連携も考慮することとする。

（※１）PR 資料「事業環境変化対応型支援事業」（３）デジタル化支援のための基盤整備（以下 URL の７枚目）
https://www.chusho.meti.go.jp/koukai/yosan/2021/1224/004_r3_pr.pdf

（※２）令和元年度中小企業実態調査事業（中小企業の IT ツール等導入プロセスにおけるナッジ活用の可能性に関する調査）
https://www.meti.go.jp/meti_lib/report/2019FY/000094.pdf

④ データベースの構築

中小企業等が受けたデジタル化診断シートの記入内容を集計して診断結果をアウトプットするためのデータベースを構築する。また、ウェブ上でのデジタル化診断の受診だけではなく、紙媒体での受診も考えられるため、AI-OCR を活用する等、それらもデータ化して同じくデータベースにインプットできるようにする。（デジタル化診断を受けた中小企業等に対しては ID 及びパスワードを発行してマイページを作成し、過去の診断結果を振り返られるように設計し、繰り返し受けてもらえるような仕掛けにする。G-biz ID を活用する等の工夫を行うことも想定されるため、提案内容に盛り込むこと。）なお、データベース構築に当たっては、政府の標準ガイドライン群（※３）に沿って対応するものとする。その他、後述の診断結果に対する相談に当たっての予約システム等、本事業の実施に当たって必要なシステム開発も行う。

（※３）標準ガイドライン群
データ連携モデル
行政サービス・データ連携モデル（β版）
https://cio.go.jp/guides

（２）デジタル化診断を受けた事業者に対する相談対応

① コールセンター等の設置

コールセンター及びメールフォームを設置し、本事業に関する問い合わせ等を受け付けられる体制を構築する。（コールセンターの稼働日については、平日に加えて土日のいずれかとすることが望ましい。）事業規模については、PR 資料（※１）を参考とする。また、診断結果に対する具体的な相談の対応については、IT 関連の資格を保有しているか、デジタル化に関するこれまでの支援実績を保有しているオペレーターが相談対応を行う。その際、診断結果に記載されている内容の解説の他、中小企業等の経営課題等をヒアリングした上で、具体的な取組及び支援策の紹介を行う。なお、オンラインでの対応（ウェブ会議ツールの活用または架電）を想定しているが、必要に応じてオフライン拠点を複数箇所設置することを中小企業庁と相談の上、決定する。相談対応を円滑に進められるよう、予約対応等の工夫も行う。その他、紙媒体で寄せられたデジタル化診断シートの処理等も行う。

（※１）PR 資料「事業環境変化対応型支援事業」（３）デジタル化支援のための基盤整備（以下 URL の７枚目）＜再掲＞
https://www.chusho.meti.go.jp/koukai/yosan/2021/1224/004_r3_pr.pdf

② 診断結果を踏まえたフォローアップ

診断を受けた中小企業等に対して、診断結果を踏まえてデジタル化に取り組んでいるかのフォローアップを行う。具体的には、上述のコールセンターまたは専門家から中小企業等に取組状況をヒアリングし、課題があれば専門家につなげる。ヒアリングした課題を踏まえて、専門家の相談対応やコールセンター対応に反映する。

③ 関連施策及び関係者との連携

②の相談対応において、他の支援策の紹介及び支援機関の紹介を行うに当たって、各施策等の特徴等をまとめたものを作成した上で案内する。既存の各支援策及び支援機関の取組の方向性や内容を把握した上で、本事業の実施に当たって必要な連携を広げられるよう、中小企業庁と相談・連携の上、調整を行う。また、中小企業 119 の地域プラットフォームに登録する等、各支援策につなぐために必要な対応をとる。

（3） 検討会の開催及び報告書作成

本事業を執行しながら検討会を開催し、診断結果を踏まえて中小企業のデジタル化の方向性について議論し、報告書をまとめる。検討会には、中小企業のデジタル化について精通している有識者や中小企業診断士、IT コーディネータ等の経営相談対応を行っている支援者の他、中小団体や関係省庁に参画してもらうことを想定しており、中小企業庁と相談・連携の上、調整を行う。

報告書目次（案）
１．中小企業のデジタル化の必要性・喫緊性

２．中小企業のデジタル化状況
①診断結果の分析（業種別・事業規模別）
②診断後の取組状況の分析（業種別・事業規模別）

３．中小企業のデジタル化の課題
フォローアップで見えてきた課題とその解決策
＜具体例＞
・目標がわからない
・自社の意思決定だけでは進まない
・IT リテラシーが高い人材がいない
・活用可能なツールがわからない（投資余力がない）

４．中小企業のデジタル化の方向性（中長期的方針）

４．事業実施期間

契約締結日～令和５年３月３１日

５．納入物

（1） 調査報告書電子媒体（ＣＤ－Ｒ等） １式

（ア）成果物（後述（３））、調査で得られた元データ、関連資料一式、委託調査報告書公表用書誌情報（様式１）、二次利用未承諾リスト（様式２）を納入すること。

（イ）成果物のうち（ア）～（ウ）については、ＰＤＦ形式に加え、機械判読可能な形式のファイルも納入すること。

（ウ）調査で得られた元データについては、機械判読可能な形式のファイルで納入することとし、特に図表・グラフに係るデータ（以下「Excel 等データ」という。）については、Excel 形式等により納入すること。なお、様式１及び様式２は Excel 形式とする。

（２） 調査報告書電子媒体（ＣＤ－Ｒ等） ２式（公表用）

（ア） 成果物（後述（３））及び様式２（該当がある場合のみ）を一つのＰＤＦファイル（透明テキスト付）に統合したもの、並びに公開可能かつ二次利用可能な Excel 等データを納入すること。

（イ） セキュリティ等の観点から、経済産業省と協議の上、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。

（ウ）調査報告書は、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、経済産業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、下記の様式２に当該箇所を記述し、提出すること。

（ウ） 公開可能かつ二次利用可能な Excel 等データが複数ファイルにわたる場合、１つのフォルダに格納した上で納入すること。

（３） 成果物の構成

３．（１）②のデータベース及び③の広報物、３．（４）の報告書

（４） 各データのファイル名については、成果物の図表名と整合をとること。

（５） Excel 等データは、オープンデータとして公開されることを前提とし、経済産業省以外の第三者の知的財産権が関与する内容を含まないものとすること。

※調査報告書電子媒体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、下記ＵＲＬから行うこと。

http://www.meti.go.jp/topic/data/e90622aj.html

６．納入場所

中小企業庁経営支援部経営支援課

７．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。

８．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。

９．情報セキュリティに関する事項

業務情報を取り扱う場合又は業務情報を取り扱う情報システムやウェブサイトの構築・運用等を行う場合、別記１「情報セキュリティに関する事項」を遵守し、情報セキュリティ対策を実施すること。

（別記１）

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を定めたものを含み、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又は廃棄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「政府機関等の情報セキュリティ対策

のための統一基準群（平成３０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。そ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、約款による外部サービスやソーシャルメディアサービスを利用する場合には、それらサービスで要機密情報を扱わないことや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。

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や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や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。

（様式１）

情報取扱者名簿及び情報管理体制図

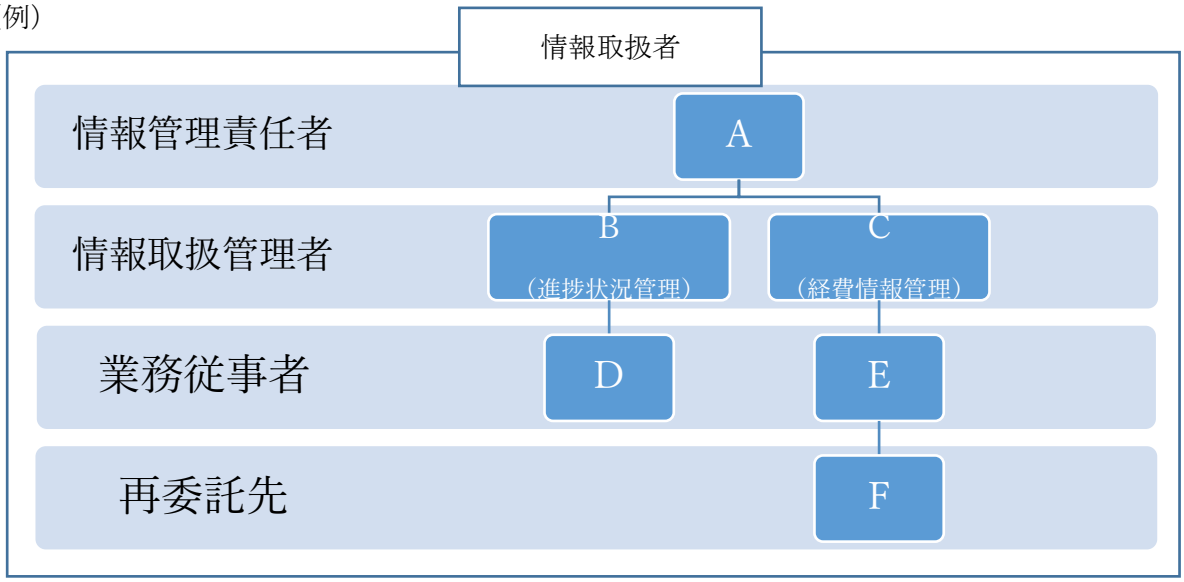
①情報取扱者名簿

		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。