（別紙）

仕様書

１．事業名

令和５年度エネルギー需給構造高度化対策に関する調査等事業（FIT/FIP 制度におけるバイオマス発電に用いる燃料の持続可能性及び GHG 排出量基準等に関する調査）

２．事業目的

2018 年度の調達価格等算定委員会において、FIT 制度下におけるバイオマス燃料の持続可能性を担保するための手段として、それまで認められていなかった第三者認証制度を活用するニーズが明らかになるとともに、主産物・副産物を含めた様々な燃料の持続可能性の確認方法を確立する必要が生じた。この状況を受け、2019 年度には、専門的・技術的に検討する場として総合資源エネルギー調査会のもとに「バイオマス持続可能性ワーキンググループ」（以下、WG という）を立ち上げ、同年 11 月に中間整理を公表した。

WG の中間整理では、2019 年度の議論時点では認められなかった第三者認証スキームについて、その後改正等が行われ、その追加が求められた場合や、新たな第三者認証スキームが整備され、その追加が求められた場合には、WG において再検討することとしている。

加えて、2019 年度の調達価格等算定委員会において、新規燃料の取扱いに関連して、食料競合の懸念に関する判断基準やライフサイクル GHG 排出量の論点についても WG において専門的・技術的な検討を行うこととされた。

これを受けて 2020 年度から 2022 年度までの WG において検討が行われ、持続可能性の確認に係る第三者認証スキームとして、新たに GGL（Green Gold Label）ISCC（International Sustainability & Carbon Certification）及び MSPO（Malaysian Sustainable Palm Oil）Part4 が追加することとなった。

食料競合の懸念の判断基準については、2020 年度 WG において、非可食かつ副産物のバイオマスが食料競合の懸念がないものとし、可食バイオマス及び主産物については、海外における議論の動向も注視しつつ、必要に応じて扱いを検討することと整理した。2022 年度には、業界団体から要望のあった新規燃料候補のうち食料競合の懸念がないと確認されたバイオマス種について、WG において持続可能性の確認方法が整理され、これを踏まえ、調達価格等算定委員会において、2023 年度からこれらのバイオマス種を FIT/FIP 制度新規燃料として認めることとされた。

また、ライフサイクル GHG 排出量については、2021 年度 WG において、排出量の基準として、比較対象電源に対して、2030 年度以降は▲70％を達成することを要求することを前提に、制度開始から 2030 年までの間は▲50％を要求することとした。2022 年度 WG では、農産物の収穫に伴って生じるバイオマス、輸入木質バイオマス、国内木質バイオマスについて、ライフサイクル GHG の確認方法について概ね整理され、これを踏まえ、2023 年度よりライフサイクル GHG の確認を開始することとなった。また、その他のバイオマス種のライフサイクル GHG の確認方法等の残る論点については検討を継続することとしている。

こうした状況を受け、これらの論点に関する調査・研究会による検討等を行い、WG の議論に必要な情報を収集し整理・分析するとともに、バイオマス発電に係る持続可能性等について検討することを、本調査の目的とする。

３．事業内容

本項目にある以下の各項目は、バイオマスのエネルギー利用政策等の検討に資する調査である。分析内容が WG 等の資料に活用されること等を念頭に置き、WG 等での議論に活用しやすい形に整理する。また、全業務に共通して新型コロナウイルス感染症に最大限対応・配慮した上で web 会議等も活用する。なお、会合を要する場合については「新しい生活様式」を参考にした感染対策を必ず

講ずる。

（１） 第三者認証スキームに関する情報収集・分析等

① 第三者認証スキームに関する分析及び評価基準に対する充足状況の評価、並びに検討資料の整理

持続可能性の確認に関して、2022 年度までの WG の検討において、不採用となった第三者認証スキームについて改正等が行われ、その追加が求められた場合や、新たな第三者認証が整備されその追加が求められた場合には再検討することとしている。この状況を踏まえ、既存の第三者認証スキームが改正を行い、その再評価を求められた場合や、新たな第三者認証スキーム等が整備され、その評価を求められた場合に対応し、それらの第三者認証スキームの制度文書等の分析及びヒアリング等を行い、WG が整備した評価基準を充足しているかどうかの評価を行う。

また、ライフサイクル GHG に関して、活用できる新たな第三者認証スキーム等がある場合は、当該第三者認証スキームの制度文書等の分析及びヒアリング等により調査を行う。

上記に際しては、第三者認証スキーム側との調整等も行うものとする。評価のエビデンスは出典・記載箇所を明記した形で資料としてまとめ、対外的な説明に活用できるよう配慮するとともに、必要に応じ英語仮訳版等も作成する。

② 各第三者認証スキームの基準文書の改訂等に係る調整等

WG での議論において FIT/FIP 制度で活用できることが確認された第三者認証スキームについて、新規燃料の対象への追加や FIT/FIP 制度が求めるライフサイクル GHG の確認に係る要件等が基準文書等に適切に反映されるよう、各第三者認証スキームとの調整等を行う。

③ 各第三者認証スキームの監査等の運用実態の調査

WG における議論の動向も踏まえ、FIT/FIP 制度が求める持続可能性を確認できる第三者認証スキームについての運用に関して実態調査を行う。調査方法としては、文献調査に加えて、認証制度を運営する機関及び認証機関に対してのヒアリングを基本とするが、必要に応じて、当項目の検討に活用できそうな内容について、資源エネルギー庁省エネルギー・新エネルギー部新エネルギー課（以下「新エネルギー課」という。）に提言の上、追加的な調査を行う。

（２） バイオマス燃料のライフサイクル GHG 排出量の基準等に関する調査

ライフサイクル GHG 排出量の基準については、2021 年度 WG において、算定式、排出量の基準（比較対象電源のライフサイクル GHG、削減水準、適用スケジュール）について整理した。また、2022 年度 WG において、農産物の収穫に伴って生じるバイオマス、輸入木質バイオマス、国内木質バイオマスについては、確認方法が概ね整理され、その他のバイオマス種の確認方法等の残る論点については継続検討することとされた。

これを踏まえ、必要に応じて専門的に検討を行う場を設定の上、以下の項目について検討をするとともに、状況に応じ、WG 等への報告を行う。

また、秋頃を目途に WG から調達価格等算定委員会へ報告を行うことを想定し、新エネルギー課と密に連携を取り運営する。

① ライフサイクル GHG の算定について

2022 年度に策定した既存燃料の既定値について、木質バイオマスの区分の条件等を必要に応じて検討する。また、新規燃料について、ライフサイクル GHG の既定値を検討する。

② ライフサイクル GHG の排出量の確認手段等について

ライフサイクル GHG の確認手段等について、2022 年度 WG において継続検討となったメタン発酵ガス、一般廃棄物・産業廃棄物、建設資材廃棄物のライフサイクル GHG の確認方法、

国産木質バイオマスの個別計算の方向性等の事項について検討する。

③ ライフサイクルGHGの排出量の情報開示について

2022年度までのWGでの議論を踏まえ、ライフサイクルGHGの排出に係る望ましい情報開示・報告の在り方について検討する。

（3） 発電用バイオマス燃料を取りまく国際的な動向等の調査

発電用バイオマス燃料に関する国際的な動向やパリ協定を踏まえたカーボンニュートラルに向けた各国の取組等、我が国のバイオマスエネルギー利用における持続可能性確保に貢献し得る内容について、常にその動向をチェックし、適宜整理を行い分析・報告する。

また、(1)、(2) に掲げた事項のほか、新エネルギー課が必要と判断した事項について、随時情報収集を行う。

（4） その他WG等における検討に関し必要な調査

バイオマス燃料に関する飼料を含む食料競合や他用途の燃料需要等に係る国内外の議論の動向等の調査、木質バイオマスの持続可能性や情報開示の在り方に関する調査、その他WG等における検討に関して必要な調査を行う。なお、専門的な検討を行う際は、必要に応じて、勉強会等を開催する等、検討の深化を図ることに留意し進める。勉強会等については、委員4名程度、開催回数3回程度を予定するが、具体的には新エネルギー課と調整の上、委員選定、開催スケジュールを決定する。

調査の内容や進め方については事前に新エネルギー課と協議の上実施し、調査の進捗状況や収集した情報について定期的な報告を行う。WGの検討に当たっては、随時状況が変化し、細やかな情報共有が必要であることから、原則月１回以上の定期的なミーティングを実施する予定である。

報告書については、最終版に加え、新エネルギー課が指定する場合は、中間的な取りまとめを作成する。

４．事業期間

委託契約締結日から令和５年３月３１日まで

５．納入物

・調査報告書電子媒体（ＣＤ－Ｒ） １枚

- 調査報告書、調査で得られた元データ、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。
- 調査報告書については、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。
- 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。

・調査報告書電子媒体（ＣＤ－Ｒ） ２枚（公表用）

- 調査報告書及び様式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。
- セキュリティ等の観点から、資源エネルギー庁と協議の上、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。
- 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、資源エネルギー庁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。

- 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。
  ◆各データのファイル名については、調査報告書の図表名と整合をとること。
  ◆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、資源エネルギー庁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。
https://www.meti.go.jp/topic/data/e90622aj.html

６．納入場所
資源エネルギー庁省エネルギー・新エネルギー部新エネルギー課

７．情報セキュリティに関する事項
（１）情報セキュリティ対策
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、別添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。

（２）情報管理体制
① 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、担当課室に対し「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）を契約前に提出し、担当課室の同意を得る。（個人住所、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。）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。
（確保すべき履行体制）
契約を履行する一環として本事業で収集、整理、作成等した一切の情報が、担当課室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しないことを保証する履行体制を有する。

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ない。ただし、担当課室の承認を得た場合は、この限りではない。

③ 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、予め担当課室へ届出を行い、同意を得る。

（３）履行完了後の情報の取扱い
国から提供を受け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。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。

（別添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、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。

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。

（別紙）

情報取扱者名簿及び情報管理体制図

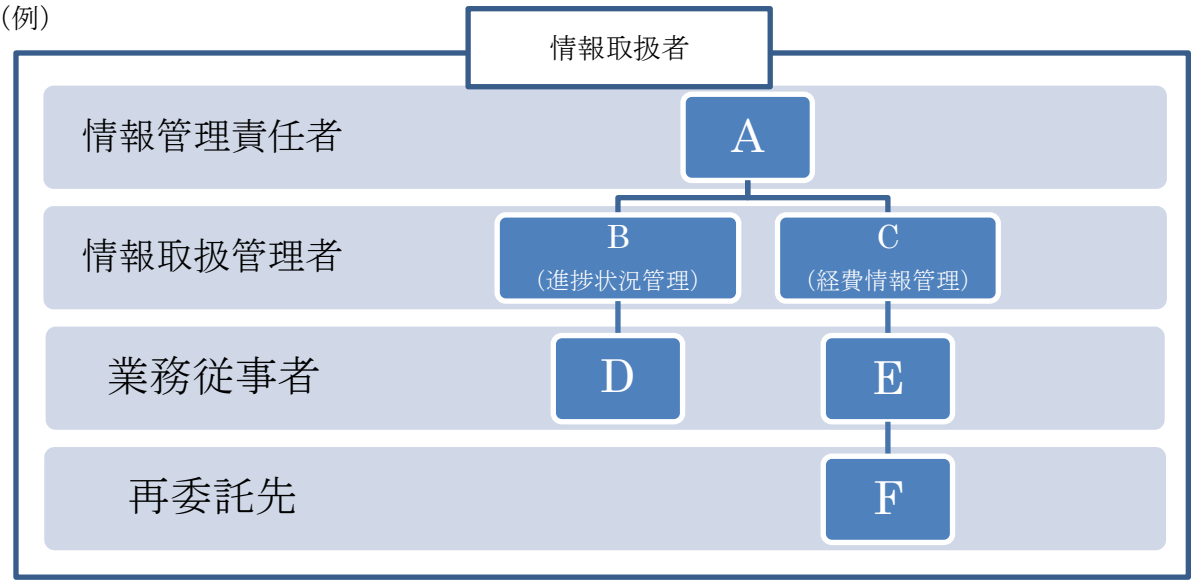
①情報取扱者名簿

		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。