仕様書

１．目的

災害（地震、津波等）時において、被災地域の「サービスステーション（以下「ＳＳ」という。）」の営業状況、被害状況等を早期に収集した上で、住民が必要とするＳＳの営業状況等を効果的かつ効率的に発信することにより、住民によるパニックバイや特定のＳＳへの殺到による道路渋滞等を抑制することは、被災地域における石油製品の安定供給を確保するために極めて重要である。

災害時情報収集システム（以下「システム」という。）は、災害時においてＳＳの営業状況等を迅速かつ効率的に収集するとともに、インターネット上の外部公開ウェブサイト（以下「ウェブサイト」という。）でアクセス可能な地図サービスと連携することで、収集したＳＳの営業状況等を効果的かつ効率的に発信するためのものであり、本仕様書は、その利用等に係るサービス（以下「本サービス」という。）を調達するものである。

２．システム利用者数等

（１）報告対象ＳＳ（ＩＤ数＝約２４，７００）

・中核ＳＳ　　約１，６００拠点
・小口燃料配送拠点　　約５００拠点
・住民拠点ＳＳ　　約１５．０００拠点
・その他ＳＳ　　約７，６００拠点

報告対象者は、１拠点１ＩＤとし、責任者クラスを想定。

（２）管理者（ＩＤ数＝２００）

・資源エネルギー庁燃料流通政策室	３
・各経済産業局担当課	１２（９経済産業局×１＋３）
・都道府県防災担当課	４７（４７都道府県）
・全国石油商業組合連合会	１
・都道府県石油商業組合	４７（４７石油商業組合）
・石油連盟	１
・石油元売会社	１８
・ＮＥＸＣＯ東日本・中日本・西日本	４４
・その他	２７

３．求められる機能及び作業内容

以下の仕様を満たすシステムを提供すること。

（１）災害の設定

① 地震発生時

国内で震度５強以上の地震が発生した場合、受注者は、管理者のメールアドレス宛てに発生状況を通知するとともに、報告事象をシステム上で設定し、報告対象ＳＳがウェブサイト上で報告し、管理者が集計できる機能を提供すること。

② 大津波警報発令時

上記、地震発生時に連動して発生する大津波警報は、上記の運用に含めるが、大津波警報が独立して発令されるケース等（沿岸部や海外で発生した地震による場合を想定）は、資源エネルギー庁（以下「当庁」という。）が報告事象を設定し、報告対象ＳＳの運営者は、当庁の要請に基づきウェブサイト上で報告し、管理者が集計できる機能を提供すること。

③ その他の災害時（噴火、台風、洪水、豪雪、停電等）

当庁が報告事象を設定し、報告対象ＳＳの運営者は、当庁の要請に基づきウェブサイト上で報告し、管理者が集計できる機能を提供すること。

（２）報告対象ＳＳの返答方法

報告対象ＳＳの運営者が以下の方法で報告できる機能を提供すること。また、ウェブサイトを利用して、ＰＣや、スマートフォン、フィーチャーフォン等の端末から報告できること。その際、（３）の状況報告内容（案）のように、回答項目を選択する等簡易な方法で報告できること。

① メール配信による方法

報告対象ＳＳにメールを配信し、メール本文に専用ウェブサイトのＵＲＬを記載し、報告対象ＳＳがそのＵＲＬにアクセスし、状況報告が可能であること。

② 専用ウェブサイトのブックマーク等による方法

万一、①のメールが届かない場合であっても、予め専用ウェブサイトのＵＲＬを報告対象ＳＳの使用する端末のブラウザに登録ができ、災害が発生し状況報告を行う必要があるときは、その登録されたブックマークからアクセスし、状況報告が可能であること。

（３）応答項目

以下に記載の内容の報告・集計が可能であること。また、設問内容は任意に簡易な方法で変更可能であること。また、スマートフォン向けに特化した報告画面、集計画面を提供すること。

【状況報告内容（案)】

1．営業状況を報告してください

営業状況	営業可能（給油・配送可能） 営業停止（給油・配送不可） 通常営業時間外のため状況確認中
営業可能（給油・配送可能）	通常通電（自家発電機稼働なし） 停電中（自家発電機稼働中）
営業時間（災害時）	（○○：○○～○○：○○）
営業停止（給油・配送不可）	現場不在で給油所等の状況を確認できていないため 給油所設備の点検待ちのため 給油所設備が損壊し修理が必要なため 燃料在庫がないため 人員不足のため 避難指示が発動されたため ローリーが被災したため（小口燃料配送拠点のみ) その他（コメントへ記載）
営業再開目安	当日中に再開予定 翌日に再開予定 ２～３日後再開予定 再開不可 不明

2．燃料の在庫状況を報告してください。

ガソリン	有（充分） 無（不足）
軽油	有（充分） 無（不足）
灯油	有（充分） 無（不足）

3．発電機稼働訓練について

発電機稼働訓練（直近）実施月を記載	（○）月に実施

（4）メール送信

システムで利用するＩＤに対して、２つ以上のメールアドレスが登録できること。また、災害発生等により、通信ネットワークが混雑している場合でも、携帯電話会社により制限されることなく、受注者からメールが送信されること。さらに、受注者と携帯電話会社の間で輻輳規制を受けない、特定接続が行われていること。

（５）災害の管理

① 同時期に発生した複数の災害に対して、複数災害事象として同時に管理ができ、事象ごとに状況報告と集計が行えること。

② 大規模地震が発生した場合、気象庁発表情報を元に、自動的に状況報告事象を設定するのではなく、誤報情報か否か等の情報の正確性を判断するための人的判断を行い、報告事象を設定する仕組みであること。

③ 同様に大規模地震の際、余震については、受注者の人的判断の下で、本震と同一の一つの事象として管理が可能であり、余震発生の毎に確認メールが送信されない工夫がされていること。

（６）管理者の機能

① ＰＣ、スマートフォン等からウェブサイト上で状況報告の回答状況の確認・集計が可能であること。また、集計内容は、報告段階、都道府県、報告対象ＳＳの区分などでＣＳＶファイルに出力可能であること。

② 管理者用の操作端末を限定せず、私用のＰＣ、スマートフォン等からの操作も可能であること。

③ 災害時の利用以外に緊急連絡網として、管理者が設問・回答を任意に作成し 、対象者を設定し、メール送信・集計可能であること。

④ メールの送信を実施できる管理者、データのメンテナンスを行う管理者などの管理者の権限種別を設定ができること。

⑤ ウェブサイト上から組織情報、ユーザー情報（報告対象者や管理者）をメンテナンスできること。メンテナンスは、ＣＳＶファイルのアップロードにより一括で登録・変更・削除が可能であること。

⑥ データメンテナンスの際、登録した連絡先、パスワード等を更新しない制御が可能であること。

⑦ 連絡先の未登録ユーザー及び無効アドレスを抽出する機能を有すること。

⑧ メールアドレスについては、実際のメールを送信することなく、無効アドレスの確認が月に１回できる機能を有すること。

⑨ 総合的な管理者となる当庁において、利用者のメールアドレスの登録状況が容易に確認可能なこと。

（７）メンテナンス

月に一度、指定した特定のシステム管理者宛に災害通知メールを送信し、正常にメールが受信されていることを確認すること。

４．地図サービスとの連携機能

インターネット上でアクセス可能な地図サービスと連携することで、収集した

ＳＳの営業情報等を効果的かつ効率的に発信できること。ただし、地図サービスの提供内容（デザイン、検索方法等)、地図サービス上に表示する内容（給油所名、住所等)、自動連携の仕組み（更新方法、解除要件等)、自動連携できない場合の表示内容などの詳細については、当庁と協議の上、変更可能なものとする。また、災害が発生した場合を考慮した上での１日あたりの想定閲覧回数は２万回程度とする。

（１）地図サービスとの連携

① 公開用の地図サービスとの連携

平時において、ＰＣ、スマートフォン等の端末からウェブサイト上でアクセス可能な地図サービスに、２.（１）のうち当庁が必要と判断するＳＳの情報を表示できること。また、災害時において、平時における情報の表示に加えて、システムで収集した報告対象ＳＳの営業状況等の内容を、報告状況や営業状況等に応じた地図サービス上のアイコンの色分けなどにより、効果的に表示できること。

② 関係者閲覧用の地図サービスとの連携

平時及び災害時において、上記①と同様の機能を有する地図サービスとして、上記①とは別に、２.（１）のうち当庁が必要と判断するＳＳの情報について、当庁が必要と判断する関係者のみが閲覧可能な地図サービスを提供すること。その際、当該地図サービスにアクセス可能な利用者を制限する方法も提供すること。

③ 地図サービスとの自動連携

システムで収集した報告対象ＳＳの営業状況等の情報のうち、上記①及び②の地図サービスに表示する情報は、システムでの自動連携がされていること。また、災害時において、当庁の判断に基づき、自動連携が開始できる仕組みを備えていること。

（２）地図サービス上の表示方法

２.（１）のうち当庁が必要と判断するＳＳの情報が、アイコンなどでＳＳの住所情報等に基づきプロットされ、そのアイコンをクリックすることで、当該ＳＳの情報等が閲覧できること。また、地図上での拡大縮小が簡易な方法で可能であること。

５．システムインフラ

（１）システムは、耐震対策、セキュリティ対策が図られたデータセンターに設置していること。また、データセンターは、２か所以上に配置されていること。

（２）相互のデータセンター間は、概ね３００ｋｍ以上離れていること。

（３）システムは、冗長構成を図り、故障によるシステム停止を回避していること。
（４）システムを構成する設備、回線等は受注者の資産であること。なお、電話、ウェブサイト等を用いた各ユーザー側からの送信に要する通信費用、システム側から送信されるメールの受信料及びシステム接続のためのインターネット通信料は、本サービスの費用に含まない。
（５）システムの提供形態は、あらかじめ当該仕様を満たしている機能を、サービスとして提供しているもの（クラウドサービス）を利用する形式とする。
（６）システムは２４時間３６５日運用可能な体制であること。
（７）管理者からの故障申告、問い合わせ等を電話及びメールにて、２４時間３６５日受付可能な体制で運用していること。
（８）大量の一斉メールを配信する際における輻輳対策を講じること。
（９）システムと連携する地図サービスは、災害時に利用が想定される十分なキャパシティを有しているサービスを選定すること。ただし、何らかの要因により地図サービスが停止した場合、当該地図サービスの提供事業者が可及的速やかに改善を図り、復旧ができ次第、関係者にその旨を伝達することができ、また復旧後に停止要因等の調査を行うことができる事業者のサービスを選定すること。
（１０）本サービスの内容について、契約締結後にサービスレベル合意書を提案すること。

６．情報管理体制
（１）請負人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、注文者に対し「情報取扱者名簿」（氏名、住所、生年月日、所属部署、役職等が記載されたもの）及び「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)」（別紙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、契約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（以下「当庁」という。）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。

（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、同意を得なければならない。

７．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、当庁の担当職員（以下「担当職員」という。）の指示に従うこと。

８．セキュリティ要件

以下の事項について遵守すること。

(1)　受注者は、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「当庁」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（「情報セキュリティに関する事項の遵守の方法の実施状況報告書」（別紙２））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、担当職員と受注者が協議し不十分であると認めた場合、受注者は、速やかに担当職員と協議し対策を講ずること。

(2)　受注者は、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)　受注者は、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、当庁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)　受注者は、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庁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)　受注者は、本業務を終了又は契約解除する場合には、受注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)　受注者は、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庁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、当庁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)　受注者は、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)　受注者は、「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５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)　受注者は、当庁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)　受注者は、本業務に従事する者を限定すること。また、受注者の資本関係・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)　受注者は、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)　受注者は、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、受注者自身（再受注先を含む。）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)　受注者は、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)　受注者は、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)　受注者は、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等の当庁外向け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。　ただし、経済産業省外の者にとって、使用するメールアドレス等が既知の場合には、この限りでない。

(16)　受注者は、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、当庁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、当庁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システム等の当庁外向け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。

⑦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)　受注者は、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。また、外部サービスを利用する場合は、その利用状況を管理すること。

　　なお、受注者は、受注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)　受注者は、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、当庁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当庁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、当庁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。

９．操作マニュアル作成等

システムの操作方法について、容易に操作ができるよう、ＰＣ、スマートフォン等から利用する方法等について、マニュアルを作成し、作成後は報告対象ＳＳや管理者がいつでも閲覧できる状態にすること。

１０．マスタデータ作成支援

新規報告対象ＳＳに係るマスタデータ作成を支援する。

１１．導入期間

令和６年４月１日（月）～令和７年３月３１日（月）

本サービスを実現可能とすること。

１２．納入物

（１）操作説明書（報告対象ＳＳ用、管理者用）

（２）操作説明書（データメンテナンス用）

（３）環境設定書等

以上を、各１部電子媒体（Microsoft Word等の加工可能な形式及びＰＤＦ）で納入すること

１３．納入先

〒１００―８９０１　　東京都千代田区霞が関一丁目３番１号

資源エネルギー庁 資源・燃料部 燃料流通政策室（経済産業省別館４階４０９）

１４．その他

（１）事業責任者、連絡窓口担当者を明確にし、随時、担当者との連絡がとれる体制を整備すること。

（２）当庁が改善の余地があると判断した事項については、当庁と協議等の上で改善に必要な措置を速やかに講ずること。なお、協議等を行った場合は、協議後３営業日以内に議事録を提出し、担当職員の了承を得ること。

（３）本作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について提案がある場合には、担当職員に提案、協議の上、当該提案に基づき実施してもよい。

（別紙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						
下請負先	F						

（※１）受注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。

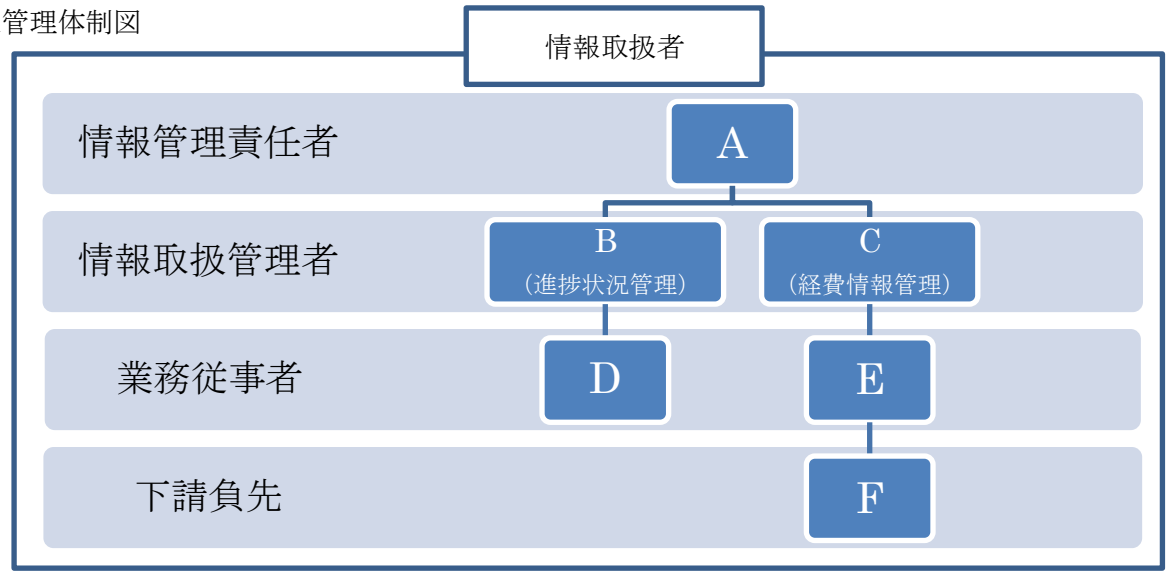
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※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。（下請負先も含む。）

・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。

（別紙２）

令和　　年　　月　　日

資源エネルギー庁燃料流通政策室　殿

住　　所
名　　称
代表者氏名

情報セキュリティに関する事項の遵守の方法の実施状況報告書

情報セキュリティに関する事項（１）の規定に基づき、下記のとおり報告します。

記

１．契約件名等

契約締結日	
契約件名	

２．報告事項

項目	確認事項	実施状況
情報セキュリティに関する事項 2）	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。	
情報セキュリティに関する事項 3）	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、経済産業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、事前に経済産業省の担当職員（以下「担当職員」という。）の許可を得る。 なお、この場合であっても、担当職員の許可なく複製しない。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。	
情報セキュリティに関する事項 4）	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経済産業省外で複製しない。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。	
情報セキュリティに関する事項 5）	本業務を終了又は契約解除する場合には、受注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。その際、担当職員の確認を必ず受ける。	
情報セキュリティに関する事項 6）	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経済産業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、経済産業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。	
情報セキュリティに関する事項 7）	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。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。	

情報セキュリティに関する事項 8）	本業務全体における情報セキュリティの確保のため、「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」（令和5年度版）、「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）及び「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）（以下「規程等」と総称する。）に基づく情報セキュリティ対策を講じる。	
情報セキュリティに関する事項 9）	経済産業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。	
情報セキュリティに関する事項 10）	本業務に従事する者を限定する。また、受注者の資本関係・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。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。	
情報セキュリティに関する事項 11）	本業務の一部を再委託する場合には、再委託することにより生ずる脅威に対して情報セキュリティに関する事項1）から10）まで及び12）から18）までの規定に基づく情報セキュリティ対策が十分に確保される措置を講じる。	
情報セキュリティに関する事項 12）	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、受注者が管理責任を有するサーバ等を利用する場合には、当該ウェブサイト又は当該サーバ等で利用する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。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。	
情報セキュリティに関する事項 13）	本業務の実施に当たって、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。 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。	
情報セキュリティに関する事項 14）	ウェブサイト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。）に従う。また、ウェブサイトの構築又は改修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。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。 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には、その指示に従う。	
情報セキュリティに関する事項 15）	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等の当庁外向け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。	
情報セキュリティに関する事項 16）	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。 1）各工程において、当庁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、当庁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システム等の当庁外向け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。 7）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。	
情報セキュリティに関する事項 17）	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、「情報セキュリティに関する事項8）」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。また、外部サービスを利用する場合は、その利用状況を管理すること。なお、受注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。	
情報セキュリティに関する事項 18）	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。 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。 ①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。 ②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。 ③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、当庁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）当庁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、当庁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。	

記載要領

1．「実施状況」は、情報セキュリティに関する事項２）から１８）までに規定した事項について、情報セキュリティに関する事項１）に基づき提出した確認書類で示された遵守の方法の実施状況をチェックするものであり、「実施」、「未実施」又は「該当なし」のいずれか一つを記載すること。「未実施」又は「該当なし」と記載した項目については、別葉にて理由も報告すること。

2．上記に記載のない項目を追加することは妨げないが、事前に経済産業省と相談すること。

（この報告書の提出時期：定期的（契約期間における半期を目処（複数年の契約においては年１回以上））。）