別紙１

仕様書（案）

１．事業名

令和８年度石油・ガス等供給に係る保安対策調査等事業（石油精製プラント等の事故調査）

２．事業目的

本事業は、石油精製プラント等における高圧ガスに係る事故等（以下、「事故」という。）について調査を行い、情報整理するとともに、保安対策上広く展開することが有用と認められるものについて、原因及び類型化の調査を行い、再発防止のための効果的な対策を講じ、教訓を加えてその内容を周知すること等により、高圧ガスに係る公共の安全の確保を図ることを目的とする。

また、認定（完成・保安）検査実施者及び認定高度保安実施者等の高圧ガス認定事業者に対しては、認定基準告示等の認定基準に則した保安管理システムの確立及び継続的改善の状況、パフォーマンス向上状況等の観点から調査を行い、指摘や助言等の情報提供を行うことにより事業者の保安管理システムの改善及び自主保安活動の向上を促し、事故災害の未然防止に資することを目的とする。

３．事業内容

事業内容の詳細については、経済産業省大臣官房産業保安・安全グループ高圧ガス保安室（以下「国」という。）に相談し了解を得た上で、決定することとする。

１）高圧ガス事故の情報整理及び内容分析

（１）高圧ガス保安法第７４条第４項の規定に基づき都道府県知事等から経済産業大臣に報告された事故情報（別添１：高圧ガス事故等調査報告書）又は国からの指示に基づくもののうち、令和８年（１月から１２月）に発生した事故情報の提供を国から受け、各月分の事故情報ごとに高圧ガス保安法事故に分類し、情報整理を行い、月報として、次の各表に取りまとめの上、毎月、国に報告する。月報については、次のアドレスを参照のこと。なお、事故情報を受ける都度、その情報に不備等があれば国へ連絡すること。

（参考）

https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/hipregas/files/2024_kouatsujiko.pdf

表１　高圧ガス事故集計表

表１－１　高圧ガス事故集計表（災害）

表１－２ 高圧ガス事故集計表（喪失・盗難）
表２ 高圧ガス保安法関係事故件数の推移（直近２０年間及び最近６年間、以下同様）
表２－１ 高圧ガス保安法関係事故件数の推移（災害）
表２－２ 高圧ガス保安法関係事故件数の推移（喪失・盗難）
表３ 高圧ガス事故の原因別による分析
表３－１ 高圧ガス事故の原因別による分析（災害）
表３－２ 高圧ガス事故の原因別による分析（喪失・盗難）
表４ 製造事業所の業種別事故件数
表４―１ 製造事業所の業種別事故件数（災害）
表４－２ 製造事業所の業種別事故件数（喪失・盗難）
表５ 製造事業所事故の原因別による分析
表５―１ 製造事業所事故の原因別による分析（災害）
表５－２ 製造事業所事故の原因別による分析（喪失・盗難）
表６ 移動中事故の物質名による分析
表６―１ 移動中事故の物質名による分析（災害）
表６―２ 移動中事故の物質名による分析（喪失・盗難）
表７ 移動中事故の原因別による分析
表７－１ 移動中事故の原因別による分析（災害）
表７－２ 移動中事故の原因別による分析（喪失・盗難）
表８ 消費先事故の物質名による分析
表８―１ 消費先事故の物質名による分析（災害）
表８―２ 消費先事故の物質名による分析（喪失・盗難）
表９ 消費先事故の原因別による分析
表９―１ 消費先事故の原因別による分析（災害）
表９―２ 消費先事故の原因別による分析（喪失・盗難）
表１０ 製造事業所、移動中、消費に係る事故以外の事故の取扱状態による分析
表１０―１ 製造事業所、移動中、消費に係る事故以外の事故の取扱状態による分析（災害）
表１０―２ 製造事業所、移動中、消費に係る事故以外の事故の取扱状態による分析（喪失・盗難）
表１１ 現象別区分による分析
表１１―１ 現象別区分による分析（災害）
表１１―２ 現象別区分による分析（喪失・盗難）表１２ 人的被害の推移
表１３ 事故等級別事故発生件数
表１３―１ 事故等級別事故発生件数（災害）

表１３―２ 事故等級別事故発生件数（喪失・盗難）
※上記表中、「災害」には「危険な状態」を含む。

（２）高圧ガス保安法第７４条第４項の規定に基づき都道府県知事等から経済産業大臣に報告された事故情報及び石油コンビナート等災害防止法の特定事業所で発生した異常現象に係る事故として連絡のあった事故情報のうち、令和８年度（令和８年４月１日から令和９年３月３１日）に発生した事故情報（別添２：事故報告フォーマット）の提供を国から受け、週分ごとに情報整理を行い、週報（別添３：週報フォーマット）として毎週国に報告する。なお、事故情報を受ける都度、その情報に不備等があれば国へ連絡すること。

（３）（１）で得られた情報から、４パターン（①同一事業所で過去に類似の事故が発生、②複数事業所で類似の事故が発生、③反応暴走に起因する事故が発生、④同一事業所における複数事故等の多発）に該当するものを抽出する。

（４）（１）で報告する内容について、取りまとめの都度、高圧ガス事業に従事する関係者等宛てに情報発信を行う（情報発信は１０００者程度を想定。）。情報発信する内容は（１）の表２以下については直近６年間分とする（令和７年以前の情報は国が提供する。）。

なお、情報発信を行う宛先の選定及び管理、並びに使用する機器等の用意は本事業を実施する者が自ら行うこととする。また、宛先の選定は国に相談し了解を得ることとする。

（５）（１）で報告する内容について取りまとめた高圧ガス関係事故年報（ただし、（１）の表２以下については最近２０年間分とする（令和７年以前の情報は国が提供する。）。）を作成する。作成の際は、本年の事故情報に係る分析結果を理解しやすい形で記述すること。様式については、過去の本事業と同じ物とすること。

なお、令和８年１月１日より、高圧ガス・石油コンビナート事故対応要領を改正し、冷凍事業所における人的被害を伴わないフロン（不活性ガス）の漏えいは、事故情報の報告・収集の対象外としたことから、最近２０年間分の年報を作成する際に、今般の対象外にした事故を除外した年報についても作成すること。

（６）国から提供を受ける（１）のデータを毎年蓄積したデータベース（以下、「事故事例データベース」という。）について、以下の作業を実施する。
①（１）及び（３）で得られた情報を事故事例データベースに入力すること。

②事故事例データベースのデータを四半期ごとに取りまとめ、電子媒体で国に提出すること。

③平成９年以降のデータについて、特定認定完成検査実施事業者、特定認定保安検査実施事業者、認定完成検査実施者、認定保安検査実施者、特定認定高度保安実施者、認定高度保安実施者又は自主保安高度化事業者の認定を受けた事業所（以下「認定事業所」という。）で発生した事故を抽出し、その事故を識別できる項目を設け、入力すること。

（参考）

・事故事例データベース
https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/hipregas/jikoboushi/database.html

・高圧ガス・石油コンビナート事故対応要領
https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/hipregas/files/20251225kouatsu_konbi_jikoyoryo1.pdf

（７）国からの指示に基づき事故の関連資料の作成を行う。資料作成に当たっては、（１）～（３）で報告する内容及び国から提供を受ける事故事例データベース（Microsoft Excel 2016及び2019にも対応するもの）をもとに作成すること。

特に、令和８年１～１２月の事故の動向については、年度末の高圧ガス小委員会で報告することを想定して、①令和８年１２月１８日までに、その時点のデータから推測される令和８年の通年の傾向を整理して、高圧ガス保安室に報告するとともに、②令和９年２月５日までに、最終的なデータを集計して、資料を作成し、高圧ガス保安室に報告すること。

（８）（１）から（７）までの内容を本事業の終了期限までに取りまとめ、事業報告書を作成する。

２）石油精製業等の最近の事故調査

（１）国が提供する高圧ガス事故報告情報の中から、令和６年以降に発生した石油精製業等に対し教訓としての価値が高いと思われる事故（１０件程度）を抽出して、事故原因の調査（現地調査を含む。）を行う。この内、複数箇所で発生するなど、特に教訓としての価値が高いと思われる重要な１つのテーマを定め、そのテーマに係る事故を３件程度抽出すること。また、現地調査について、事故を起こした事業者に対して実施することが困難な場合においては、必要に応じて国による立入検査等の実施について、国に相談すること。

具体的には、抽出した事故報告情報に関する「事故区分」、「事故名称」、「事故

発生日時」、「事故発生場所」、「高圧ガス名」、「法令違反の有無」、「被害状況（周囲への影響等）」、「事故概要」、「事故原因」、「再発防止対策」、「教訓及び当該事故に関する注目すべき点」、「その他」の事項について、１事故ごとに５～６ページ程度で図表、写真等を用いて簡潔にまとめた報告書を作成すること。また、年間に複数箇所で発生するなど、特に教訓として価値が高いと思われるテーマとして抽出した３件程度の事故については、これらの共通点、相違点なども含め要因分析を行い、再発防止対策の検討を行うこと。

なお、事故の選択にあたっては、国が選択した事故は必ず対象とするとともに、それ以外の事故についても、国に相談し了解を得ること。また、報告書については、一般国民に理解しやすいように、難しい専門用語等には説明を入れるなど工夫を図り、成果の普及に適した資料（令和６年度石油・ガス供給等に係る保安対策調査等事業（石油精製プラント等の事故情報調査）報告書）（https://www.meti.go.jp/meti_lib/report/2023FY/000379.pdf）を参考に作成すること。また、図表、写真の提供者及び報告書に記載された事故を起こした事業者に対し、国又は受託者が不特定多数に公開することについて了解を得ること。さらに、報告書の内容については国に相談し了解を得ること。

（２）（１）において作成した報告書については、６）（１）で設置する委員会にて審議し、その内容の技術的妥当性等について検討すること。

（３）（２）で審議が終了した調査報告書は、順次、ホームページ等へ公表、又は、プライバシーの保護を考慮した上で高圧ガスの事業者、学識経験者及び行政機関等へ速やかに情報発信を行うこと（情報発信は１０００者程度を想定。）。

なお、情報発信を行う宛先の選定及び管理、並びに使用する機器等の用意は入札する者が自ら行うこととする。また、宛先の選定は国に協議することとする。

（４）（３）でメール配信を行った報告書を本事業の終了期限までに取りまとめ、事業報告書を作成する。

（５）調査・審議を行ったが、何らかの理由により実施期間中にメール配信等ができなかった報告書については、事前に国に相談の上、調査経緯を記載した資料とともに事業報告書に入れること。

３）事故の定義等に関する調査

（１）高圧ガス・石油コンビナート事故対応要領に定められた事故の定義に基づき、

高圧ガス事故の対応を実施してきたところであり、これまでに豊富な高圧ガス事故の情報が蓄積されたところである。今後のより合理的かつ適切な高圧ガス保安行政の執行に向け、これまでに蓄積された高圧ガス事故の情報を精査し、高圧ガス保安の確保を図るに際し現状の実態に即していない運用となっていないかを確認する。その上で、国、自治体及び事業者が保安を担保した上でより合理的に高圧ガス事故に対応できる運用とするため、次の各事項に関する事故の定義等のあり方について調査・分析・検証を行う。その際、事故の種類・場所・原因等と被害状況等の相関関係を分析するなど、統計学的手法も用いた詳細な分析も行う。

①高圧ガス保安法第３６条（危険時の措置及び届出）と同法第６３条（事故届）の現状の整理及び事故報告の差別化の検討。

（２）（１）について６）（１）で設置する委員会にて審議し、その内容の妥当性等について審議すること。

（３）（２）で検証した結果を踏まえ、高圧ガス・石油コンビナート事故対応要領２．事故の定義等のあり方について案をとりまとめ、国へ報告書を提出する。

４）重大事故等の調査

（１）国内で重大事故等が発生した際、国の指示があったとき（１年に５回程度を想定）は、次の①～③により調査を行う。

①指示を受けた日又は数日中に現地調査を実施し、国へ報告書を提出する。報告に当たっては、原則、現地調査当日中に調査結果の概要を報告するとともに、下記事項を含めた調査結果の詳細を、原則、現地調査後２週間以内に報告すること。また、現地調査は、原則、委員会の有識者及び受託者事務局が行うものとするが、委員会の有識者以外の有識者から選定すべき場合は、委嘱等の所要の手続を行うこと。

（調査結果の詳細報告事項）

・趣旨
・概要（調査先、調査対応者、事故発生日時、場所、事故の概要、被害の状況）
・事故原因、再発防止対策
・今後の状況（事業者の取組、自治体の取組等を含む）
・社会的影響の状況
・「高圧ガスに係る事故等」としての取扱いの考察（法令違反の有無等を含む）
・過去の同種の事故の発生状況（事故事例データベース等を活用）
・上記状況を踏まえた、高圧ガス保安法令等における今後の取扱いに係る助言

②①の現地調査実施後に開催する６）（１）の委員会にて、①の現地調査に関して調査を行った者から報告書の説明を受けた後、有識者の意見を聴取し、国へ報告書を提出する。ただし、令和９年２月または３月に発生した事故に関する①の現地調査については、６）（１）の委員会での有識者の意見聴取は不要とする。

③令和８年２月または３月に発生した事故に関する現地調査報告書を国から提供を受け、６）（１）の委員会にて有識者の意見を聴取し、国へ報告書を提出する。

（２）国外で発生した重大事故または国外の規制、事故の発生状況について、国から指示があったとき（１年に１回程度を想定）は、事業者、規制当局、その他関係者に連絡し、情報収集を行い、可能であれば現地調査を実施し、国へ報告書を提出する。現地調査は、原則委員会の有識者及び受託者事務局が行うものとするが、委員会の有識者以外の有識者から選定すべき場合は、委嘱等の所要の手続を行うこと。事業者、規制当局、その他関係者は、国から情報を提供するが、入札する者が自らの有する情報により連絡することを妨げるものではない。

（３）（１）から（２）までの報告書を本事業の終了期限までに取りまとめ、事業報告書を作成する。ただし、国に提出した報告書のうち、必要と判断した個所に限る。詳細は、国に相談し了解を得ること。

５）高圧ガス事故を題材とした視聴覚資料の整備

（１）高圧ガス事故防止のためには、事故、トラブルを題材とした視聴覚資料を作成、広く周知することが有効と考えられるため、過去に国内で発生した事故、トラブルのうち、石油精製業等に対し教訓としての価値が高いと思われる事故、トラブルを２件抽出して、現に事故、トラブルを体験した事業者等の協力を得て、実際の映像（新たに撮影する映像の他、事故、トラブルが発生した当時のニュース映像等を含む。）、ＣＧ映像、シミュレーション結果等により事故、トラブルを再現した視聴覚資料を作成する（それぞれ１０分程度）。

（２）（１）で作成する視聴覚資料の理解を補助するため、必要に応じ、事故、トラブルの概要や専門用語などを解説した１から２ページ程度の資料を作成すること。

（３）視聴覚資料の対象とする事故、トラブルの抽出、作成する視聴覚資料等については、６）（２）で設置する委員会にて審議し、その内容の技術的妥当性等について検討すること。

（４）作成した視聴覚教材の内容及び公開方法は、国と協議すること。

６）委員会の設置・運営

（１）３．２）から４）までの事業を実施するに当たって、有識者からなる委員会（委員：１０名程度、委員会開催回数４回程度、原則対面及びオンライン）を設置し、意見の聴取等を含め、事業の円滑な進行を図ること。また、有識者の選定に当たっては、学識経験者（大学教授等)、研究者、保安管理実施者（県庁等職員)、事業者（労働者）等の中から、それぞれ候補者を選定し、国に相談し了解を得た上で決定すること。

（２）（１）とは別に、３．５）の事業を実施するに当たって、有識者からなる委員会（委員：１３名程度、委員会開催数４回程度）を設置し、意見の聴取等を含め、事業の円滑な進行を図ること。また、有識者の選定に当たっては、学識経験者（大学教授等）、業界団体、保安団体、保安管理実施者（県庁等職員）、事業者（労働者）等の中から、それぞれ候補者を選定し、その後、国に相談し了解を得た上で決定すること。

（３）各委員会開催に当たっては、事前に十分な時間的余裕をもって国に相談するとともに、国の意見を十分踏まえた内容とすること。さらに、委員への資料送付も、国に相談し了解を得た後とすること。

７）高圧ガス保安の実施状況調査

（１）認定事業所への保安管理システム等の調査

認定事業所のうち、１０事業所程度を対象に保安管理システムの実施、継続的改善等の観点から調査を行い、調査結果をもとに改善を要する事項及び評価できる事項について取りまとめて報告書を作成する。

以下に主な調査内容を示す。

①本社の保安にかかる基本姿勢、保安管理の実施状況及び評価

②本社の事業所及び検査管理組織に対する監査の実施状況及び有効性

③保安管理方針の理解、特定要求事項等の遵守状況及び評価

④リスクアセスメント及びリスク低減策の実施状況及び評価

⑤保安管理目標等の達成状況及び評価

⑥保安管理システムの実施に不可欠な資源の用意配分の実施状況及び評価
⑦非定常作業にかかる実施状況及び評価
⑧変更管理（製造施設等の新増設等を含む）の実施状況及び評価
⑨社内外の保安関連情報の積極的な収集及び規程類への有効な活用状況及び評価
⑩機器の寿命管理及び開放検査体制に関する実施状況及び評価
⑪教育訓練に関する実施状況及び評価
⑫保安管理システムの実施状況の調査及び評価の状況、並びに監査の実施状況及びその有効性の評価
⑬検査組織の体制、保安検査の実施状況及び評価並びに検査管理組織の体制、検査管理の実施状況及び評価
⑭上記の他、高圧ガス保安に係る取組みの実施状況
なお、調査を実施する対象の事業者は、国が指示する。

（２）報告書の作成

（１）で実施した調査結果について、本事業の終了期限までに取りまとめ、事業報告書を作成する。ただし、国に提出した報告書のうち、必要と判断した個所に限る。詳細は、国に相談し了解を得ること。

４．実施期間

委託契約締結日から令和９年３月３１日まで

５．納入物

（１）調査報告書等一式

- 調査報告書、報告書骨子（様式１）、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２）、二次利用未承諾リスト（様式３）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[1]な形式のファイルも納入すること。なお、報告書のデータ量が１２８ＭＢ、ページ数が１，０００ページ又は文字数が４００万文字を超過する場合には、いずれの制限も超えないようファイルを分割して提出すること。
- 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「図表等データ」とい

[1] コンピュータプログラムがデータ構造を識別し、データを処理（加工、編集等）できること。例えば HTML, txt, csv, xhtml, epub, gml, kml 等のほか、Word, Excel, PowerPoint 等のデータが該当する（スキャンデータのようなものは該当しない）。

う。）については、構造化されたＥｘｃｅｌやＣＳＶ形式等により納入すること。

（２）調査報告書等一式（公表用）

- 調査報告書及び様式３（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[2]な図表等データを、プロパティを含む状態で納入すること。
- 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、特に以下の点に注意し、削除するなどの適切な処置を講ずること。
  - 報告書・Ｅｘｃｅｌデータ等に個人情報や不適切な企業情報が存在しないか。
  - 報告書（ＰＤＦ）に目視では確認できない埋め込みデータ等が存在しないか。
  - Ｅｘｃｅｌデータ等に目視では確認できない非表示情報が存在しないか。
  - Ｅｘｃｅｌデータ等に非表示の行・列が存在しないか。
- 公開可能かつ二次利用可能な図表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。
  - 図表等データは、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。

（３）様式１～様式３について

- （様式１）委託調査報告書骨子[3]
  - レイアウト（余白、フォント等）に従い、３枚以内にまとめた上でＷｏｒｄ形式にて納入すること。
  - 図表は挿入せずテキスト形式で作成すること。
  - 見出しについては記載された項目のとおりとすること。
- （様式２）委託調査報告書公表用書誌情報[4]
  - ファイル形式はＥｘｃｅｌ形式で納入すること。
  - 報告書の英語版や概要版等、公表用の報告書と同一のＰＤＦファイルと

[2]営利目的を含む、自由な利用（転載・コピー共有等）を行うこと。
[3]委託調査報告書のデータ利活用を促進するため、報告書の概要を骨子としてまとめるもの。
[4]本事業の報告書のオープンデータとしての公表に際し、データとしての検索性を高めるため、当該データの属性情報に関するデータを作成するもの。

することが適当でない公表用の納入物がある場合には１つのＰＤＦファイルごとに作成すること。

- （様式３）二次利用未承諾リスト
  - 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が前提だが、二次利用の了承を得ることが困難な場合又は了承を得ることが報告書の内容に大きな悪影響を与える場合は、報告書の当該箇所に出典等を明示し、知的財産権の所在を明らかにした上で、当該データを様式３に記載すること（知的財産権の所在が不明なものも含む）。
  - ファイル形式はＥｘｃｅｌ形式で納入すること。
- 様式１～３ダウンロード先
  - 委託調査報告書　（METI/経済産業省）

６．納入方法

- メール提出やファイル交換サイト等の手段を用いること。なお、具体的な納入方法は担当課室と協議の上、決定すること。
- 公表用資料一式と非公表資料一式が紛れないように整理して納入すること。

７．納入場所

経済産業省大臣官房産業保安・安全グループ高圧ガス保安室

８．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４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。

９．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。

１０．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「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。

（様式４）

情報取扱者名簿及び情報管理体制図

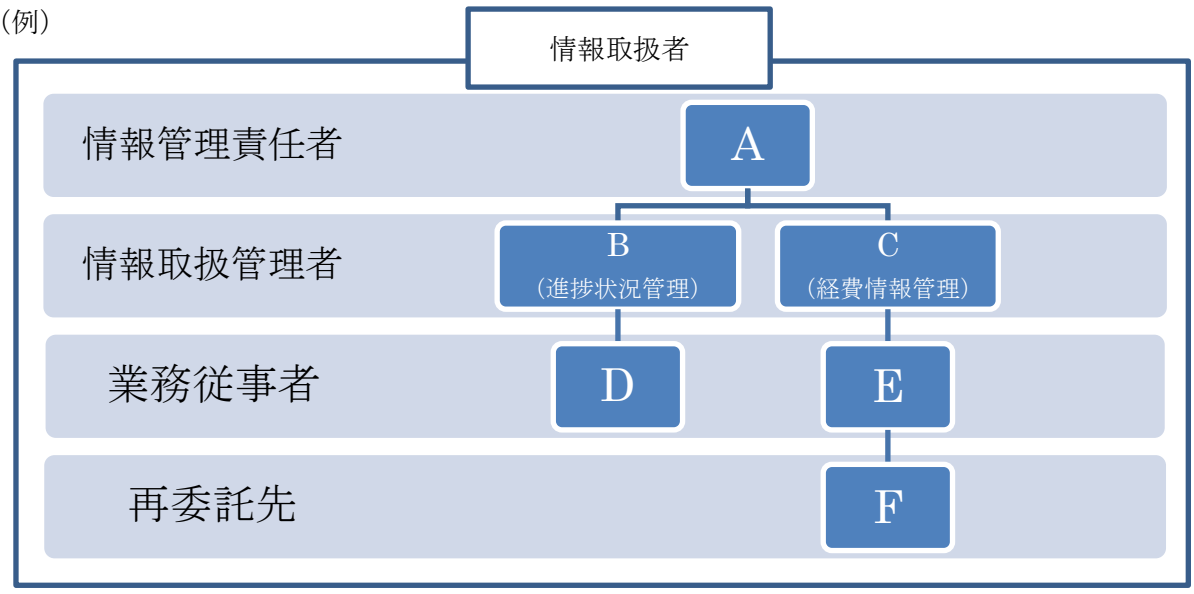
①情報取扱者名簿

		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。

（別記）

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。

【情報セキュリティ関連事項の確保体制および遵守状況の報告】

1）受注者（委託契約の場合には、受託者。以下同じ。）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)～17)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（「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））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。

【情報セキュリティ関連規程等の遵守】

2）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。

3）受注者は、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。

【情報セキュリティを確保するための体制】

4）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。

5) 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、1)から 17)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。

【情報の取扱い】

6) 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。

7) 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。

8) 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。

9) 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。

【情報セキュリティに係る対策、教育、侵害時の対処】

10) 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。

11）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。

【クラウドサービス】

12）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、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスを利用する場合には、これらのサービスで要機密情報を取り扱ってはならず、2)に掲げる規程等で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。

13）受注者は、本業務を実施するに当たり、利用において要機密情報を取り扱うものとして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)」の ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリストから調達することを原則とすること。

14）受注者は、前 2 項におけるクラウドサービスの利用の際は、提供条件等から、利用に当たってのリスクの評価を行い、リスクが許容できることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。

【セキュアな情報システム（外部公開ウェブサイトを含む）の構築・運用・閉鎖】

15）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。 また、以下を含む対策を行うこと。

(a) 不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。

(b) 不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成すること。

(c) 不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。

(d) 不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。

(e) EDR ソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討すること。

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受注者自身（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。

⑦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省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。

⑧外部に公開するウェブサイトを構築又は運用する場合には、以下の対策を実施すること。

・サービス開始前および、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。

・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。

⑨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。

⑩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省外向けシステムを構築又は運用する場合は、当省が指定する期日にドメインの抹消、DNSやCDN情報の削除、運用環境の削除を行える事業者を選定すること。

また、運用を閉鎖する場合は、終了告知を一定期間行うこと。一定期間の終了告知を終えた後は、ドメインの抹消、DNSやCDN情報の削除、ドメインへのリンクの削除、SNSを利用していた場合はアカウント削除等、なりすましの防止策を漏れなく講ずること。

なお、本事項は、「実施」の場合はその実施内容、「未実施」又は「該当なし」の場合はその理由等を必ず報告すること。

【アプリケーション・コンテンツの情報セキュリティ対策】

16）受注者は、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) 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提供するアプリケーション・コンテンツ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、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アプリケーション・コンテンツに掲載すること。

17）受注者は、外部に公開する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。

別紙

令和　　年　　月　　日

経済産業省〇〇〇課長　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３）	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４）	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５）	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１７）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６）	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７）	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８）	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９）	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１０）	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１１）	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１２）	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、定型約款や利用規約等への同意のみで利用可能となるクラウドサービスを利用する場合には、これらのサービスで要機密情報を取り扱ってはならず、「情報セキュリティに関する事項２）」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。	
情報セキュリティに関する事項１３）	本業務を実施するに当たり、利用において要機密情報を取り扱うものとして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）」の ISMAP クラウドサービスリスト又は ISMAP-LIU クラウドサービスリスト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１４）	情報セキュリティに関する事項１２）及び１３）におけるクラウドサービスの利用の際は、提供条件等から、利用に当たってのリスクの評価を行い、リスクが許容できることを確認して担当職員の利用承認を得るとともに、取扱上の注意点を示して提供し、その利用状況を管理すること。	
情報セキュリティに関する事項１５）	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。また、以下を含む対策を行うこと。 ①不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。 ②不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成すること。 ③不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。 ④不正プログラム対策ソフトウェア等を定期的に全てのファイルを対象としたスキャンを実施するように構成すること。 ⑤EDR ソフトウェア等を利用し、端末やサーバ装置（エンドポイント）の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能の導入を検討すること。 （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）受注者自身（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。 （7）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省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。 （8）外部に公開するウェブサイトを構築又は運用する場合には、以下の対策を実施すること。 ・サービス開始前および、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。 ・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。 （9）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１６）	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）提供するアプリケーション・コンテンツ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、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アプリケーション・コンテンツに掲載すること。	
情報セキュリティに関する事項１７）	外部公開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。）に従う。また、ウェブアプリケーション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。	

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１７）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））。）