仕様書（案）

１．件名

令和７年度グリーントランスフォーメーションリーグ運営事業費（排出量取引制度の本格稼働に向けた環境整備事業）

２．事業目的

政府は、排出削減と経済成長の同時実現に向けて、「脱炭素成長型経済構造移行推進戦略（GX 推進戦略）」において、2026 年度より排出量取引制度を本格稼働することとしている。具体的には、2023 年度から試行的に開始したＧＸリーグにおける排出量取引制度での取組状況を基礎として、企業の GX のための取組を加速させていくため、2026 年度からは制度に係る公平性・実効性を高める形で、改正 GX 推進法の下で排出量取引制度を導入することとしている。2026 年度から導入する排出量取引制度において、国は一定の排出規模以上の企業（300～400 社程度を想定。以下「対象企業」という。）に対して、政府指針に基づいて排出枠を無償で割当て、企業は毎年度自らの直接排出量を算定・報告し、当該直接排出量と同量の排出枠を償却する義務が毎年度課される。なお、対象企業の実際の排出量があらかじめ国から無償で割り当てられた排出枠の量を超過する際、当該対象企業は、排出枠の不足分について、排出削減を先行的に行ったことで排出枠の余剰が生じている企業等から取引を通じて調達することとなる。このうち、国による排出枠の割当て、企業による排出量の報告、償却義務の履行並びに企業が保有する排出枠の管理及び企業間の排出枠の取引等による移転の記録等は電子システム上で行うことを想定している。

本事業においては、2026 年度からの排出量取引制度を執行する上で必要な上記電子システムの構築を行う。

３．事業内容

受託者は、２．の事業目的を達成するため、経済産業省と連携し、排出量取引制度システム（図１参照）の構築にかかる以下の内容を実施する。なお、本事業を実施する上で関係する者は下表（表 1）の通りである。

事業実施にあたっては、2026 年度以降の排出量取引制度の骨格について検討された会議体（「GX 実現に向けたカーボンプライシング専門ワーキンググループ[1]」）における検討状況及び今後政府において設置される当該制度の詳細設計を検討する会議体における検討状況を踏まえること。加えて、2023 年度から試行的に実施している排出量取引制度の運営にかかる委託事業[2]における調査結果や開発したシステムの仕様を参照すること。また、必要に応じて、海外における排出量取引制度のシステムの仕様や国内外の類似の機能または本システム構築において参考となる機能を持つシステムの仕様等について調査しながら進めること。調査対象や調査の詳細に

---

[1] 内閣官房「GX 実現に向けたカーボンプライシング専門ワーキンググループ」
https://www.cas.go.jp/jp/seisaku/gx_jikkou_kaigi/carbon_pricing_wg/kaisai.html

[2] ①令和３年度補正カーボンニュートラル・トップリーグ整備事業委託費（グリーントランスフォーメーションリーグ設立準備及び排出量取引のシステム実証等事業）
②令和５年度グリーン・トランスフォーメーションリーグ運営事業委託費(GX リーグ事務局運営及び GX リーグ参画企業による自主的な排出量取引のための環境整備事業)
③令和６年度グリーン・トランスフォーメーションリーグ運営事業費(GX リーグ事務局運営及び GX リーグ参画企業による自主的な排出量取引のための環境整備事業)

ついては経済産業省担当者と相談した上で進める。

図１　排出量取引制度システムの概要

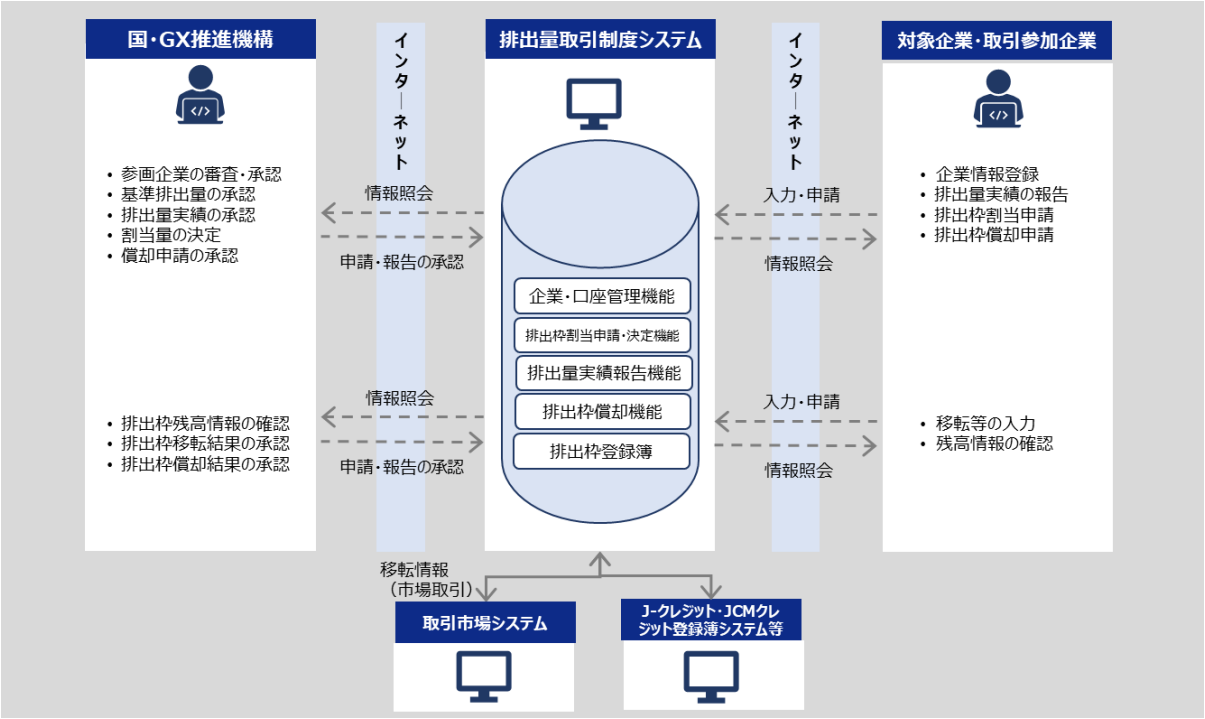


表１　事業における関係者一覧

関係者	役割/関係性
国・脱炭素成長型経済構造移行推進機構（GX 推進機構）	対象企業・取引参加企業からの申請を受け付け、承認・決定を行う。
対象企業・取引参加企業	自社の排出量及び排出枠にかかる申請・報告を国・GX 推進機構に行う。また、排出枠の残高情報をシステム上で確認する。
取引市場システム	取引市場における取引に基づく排出枠の移転情報を排出量取引制度システムに連携する。
J-クレジット・JCM クレジット登録簿システム	各登録簿システム上におけるクレジットの無効化情報等を排出量取引制度システムに連携する。

（１）2026 年度以降の排出量取引に係るシステム構築

2026 年度以降より執行する排出量取引制度を実施するにあたって必要な以下①から④のシステム構築を実施すること。

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、経済産業省担当者に提案、協議の上、当該提案に基づき実施してもよい。

① 2026 年度以降の排出量取引制度システム構築に向けた要件定義業務

次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。

a. 企業・口座管理機能

対象企業及び取引参加企業[3]に対して、アカウントを発行し、制度執行の事務の一部を担う脱炭素成長型経済構造移行推進機構（以下、「GX 推進機構」という。）及び企業が排出枠管理機能、排出枠の保有・移転等を記録する登録簿機能を利用するために必要な ID、パスワード、口座番号等を管理する。セキュリティ強化対策として、ログインあるいは重要操作を行う際には多要素認証及び二段階認証を行う等の機能を検討・実装する。

b. 排出枠の割当申請・決定機能

対象企業が、法令において規定された算定方法及び各企業が提出する基礎情報に基づき、排出枠の割当量を計算し、国に対して申請する機能及び当該申請に対して国が割当量を決定する機能。割当量の計算方法については、関係法令の規定内容を参照の上、システム上で計算できる機能を実装すること。また、割当量の決定後は、各対象企業の登録簿上で保有残高へ割当処理により反映を行う。

c. 排出量の実績報告機能

対象企業が、法令において規定された算定方法に基づき算定された自社の排出量を国に対して報告する機能。

d. 排出枠の償却機能

対象企業が、国に対して、当該年度における自社の排出量と同量の排出枠を償却し、償却した排出枠について移転等をできない状態にする機能。償却の実行時には、各対象企業の登録簿上で保有残高へ残高反映（減算）を行う。

e. 排出枠登録簿

対象企業等の排出枠の保有状況の管理及び移転の記録等を行う登録簿を整備する。登録簿内に企業毎の排出枠の保有状況を管理する口座を整備し、口座保有企業が残高情報の閲覧等を行える環境整備・維持を行う。また、対象企業等が排出枠を企業間で相対取引又は取引所取引等の取引形態に応じて、排出枠の移転を記録し、口座の残高に反映する。

f. ワークフロー・権限管理機能

上記 a. ～e. の機能を適切に管理可能なワークフロー・権限管理について検討すること

・統合的な業務管理フロー・ステータスの管理機能

・対象企業等からの申請、GX 推進機構側の承認管理機能

[3] 排出枠の取引市場には、対象企業の他に一定の要件を満たした企業に取引参加を認める方針としている。なお、取引参加を認める要件については 2026 年度以降に検討する。

・ワークフローに従ったアクセス・操作権限管理機能
・上記に伴うタスク管理、履歴管理、メール通知管理機能　　等

g. 外部接続機能

GX 推進機構が運営・管理する排出枠の取引市場システム、制度上で活用が認められているカーボン・クレジット（J-クレジット・JCM クレジット）の登録簿システム及びこれらのクレジットの取引市場システム[4]とのデータ連携を行うための外部接続機能を検討すること。また、必要に応じて、その他の、国による企業の排出量等の報告にかかる制度のシステムとの連携可能性についても検討すること。

また、取引市場システム及び外部の登録簿システム担当者への要件説明、並びに適切なインフラ・アプリケーション接続仕様の検討を行うこと。

h. セキュリティについて

政府ガイドラインである『情報システムに係る政府調達におけるセキュリティ要件策定マニュアル』に則り、セキュリティ対策要件を定めて対策を実施すること。

セキュリティに関する専門的なスキルを有する人材・会社における脆弱性確認テストを実施し、セキュリティ品質の担保を行うこと。

i. 運用・性能について

- 他システムとの接続や相互運用能力については、接続対象システムと電子的な手段によって情報を伝達する機能を有すること。
- 一定頻度でデータのバックアップを取り、適切に保管すること。バックアップを取る頻度は経済産業省担当者と相談の上で決定すること。
- 本システムの想定運用時間（平日 8:00～18:00（ただし、本システムのメンテナンスによる計画停止時間等は除く））を遵守して稼働できるシステムを検討すること。
- 障害発生時には速やかに復旧できるような機能および運用を検討すること。
- 障害発生時における電磁的記録は障害発生時点の状態に 12 時間以内に復旧できること。
- 使用想定ユーザのユースケースを鑑み、適切な機能および画面デザインを検討すること。
- システムの処理能力についてはピーク時に妥当な時間内で処理できる十分な性能を有するように検討すること。

② 2026 年度以降の排出量取引システムの構築業務

①で定義された要件に関して、以下の点に留意しながら、経済産業省担当者と開発スケジュールを協議し、当該開発スケジュールに従って開発・テストを行うこと。

・システム構築にあたって、外部サービスを利用する場合には、下記の a.～c. の選定基準に適合するサービスを選定すること。

---

[4] 一例として、日本取引所グループにおいて J-クレジットの取引市場として運営しているカーボン・クレジット市場がある。

a. 外部サービス提供者が対策基準を遵守し得る者であること。
b. 外部サービス提供者が対策基準と同等の情報セキュリティ管理体制を整備していること。
c. クラウドサービス選定における外部サービス提供者については、「政府情報システムのためのセキュリティ評価制度（ＩＳＭＡＰ、ISMAP-LIU)」の管理基準を満たすクラウドサービス事業者であること。

・受託者は、担当課室（経済産業省ＧＸグループ環境経済室）が受入テストを実施するにあたり、環境整備、運用等の支援を行うこと。
・具体的な制度設計と並行してシステム構築業務を実施する必要があるため、それに耐えうる柔軟な体制構築、プロジェクトマネジメント力、推進力を有していること。
・開発中の不具合やスケジュールに遅れが生じた場合には、速やかに経済産業省担当者に報告し、対応すること。なお、2025 年度のシステム構築範囲については要件定義で定めた結果を以って判断することとする。

③ システム利用にかかる手順書等の作成

②で構築したシステムについて、制度執行者（経済産業省担当者及び GX 推進機構）が利用するにあたっての手順書・ガイドライン等を作成すること。また、対象企業等が利用するにあたってのガイドライン及びＱ＆Ａ等を整備すること。

④ システムの運用・保守

②で構築したシステムについて、システム稼働後から本事業の終了までの期間、システムの運用・保守を行う。システム稼働後は、安定的なシステム運営を行い、不具合が生じた場合は速やかな対応・報告を実施すること。

（２）事業進行状況報告等

本事業の実施に当たっては、経済産業省担当者と調整の上、適切に進めることとし、定期的（少なくとも月２回以上）に経済産業省担当者に対して進捗状況を報告すること。また、経済産業省担当者が進捗状況の報告や情報の共有を求める場合には、速やかに応じること。

４．業務実施場所

受託事業者の責任において「経済産業省情報セキュリティ対策基準」を遵守の上で業務実施場所を整備すること。

５．調整

上記に掲げる事項の他、各事業内容を実施する上での詳細な事項については、適宜経済産業省担当者と協議し、決定することとする。

６．事業実施期間

委託契約締結日～令和８年３月３１日

７．成果物の作成及び納入

事業実施期間内において、以下の成果物を納入すること。なお、納入物の詳細については、経済産業省担当者と受託者が別途協議の上決定するものとする。また、以下に含まれていない場合であっても、経済産業省担当者及び受託者が必要と認める場合はこの限りでない。

（１）システム構築における成果物一式

a. 要件定義成果物
- -要件定義書
- -業務フロー
- -業務要件一覧
- -機能・非機能要件一覧
- -画面イメージ（ドキュメントではなく画面操作デモが可能な成果物）

b. アプリケーション設計書
- -概要設計書一式
- -基本設計書一式

c. 基盤設計書
- -基盤設計書一式
- -方式設計書一式

d. 製造
- -ソースコード一式
- -テスト仕様書・報告書

e. セキュリティ対策成果物
- -脆弱性分析・テスト結果
- -上記に対する対策結果

f. システム運用
- -運用保守プロセス
- -プロジェクトセキュリティルール
- -各種運用手順書

g. クラウド事業者のアカウント、環境一式

h. Web 参照可能なマニュアル一式

（２）契約金額内訳及び情報資産管理標準シート

・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が記載されたエクセルの電子データを契約締結後速やかに提出すること。
・経済産業省が定める時期に情報資産管理標準シートを提出すること。
・経済産業省が指定する様式について、当省が定める時期に提出すること。

（３）その他

・インターネット公開するシステムは原則として go.jp ドメインを用いること。
・受託者は、本システムの整備・管理に当たり、担当課室（経済産業省 GX グループ環境経済室）が必要と認める関係者（自府省内の関係部局等を想定）からの説明要請や質問等が

あった場合には、担当課室（経済産業省 GX グループ環境経済室）が実施する資料作成、回答案作成等の支援を行うこと。

８．納入場所

経済産業省ＧＸグループ環境経済室

９．事業実施体制

（１）事業実施体制

事業実施体制については下図及び下表の通り想定している。なお、詳細の体制については受託者決定後に協議の上、決定する。また、受託者の情報セキュリティ対策の管理体制については、別途、１３．（２）の通り作成すること。

図２　本事業実施体制

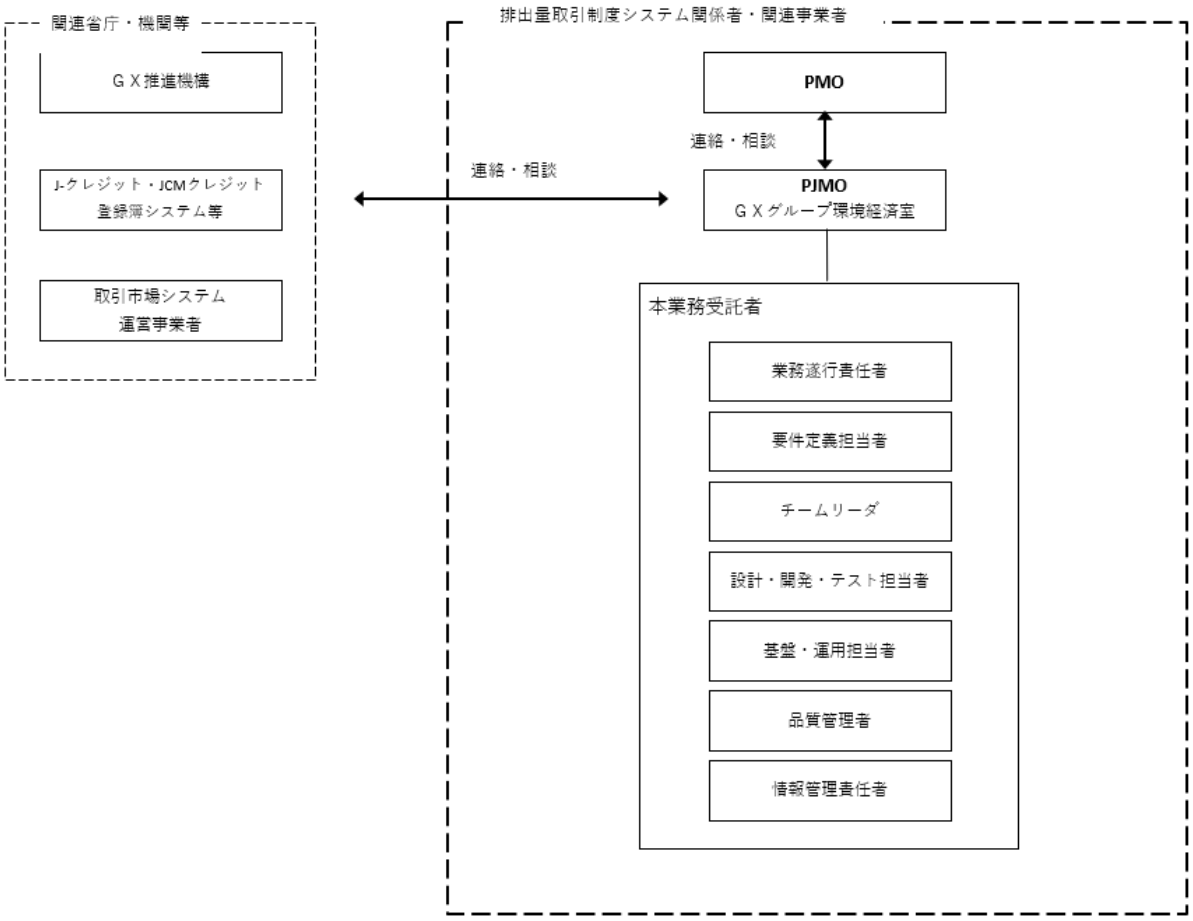


表２　本事業における組織等の役割

組織等	本業務における役割
担当部署（PJMO）	排出量取引制度システムの管理組織として、本業務の進捗等を管理する。
本業務受託者	本業務を実施する。
PMO	担当部署からの排出量取引制度システムに係る相談対応を行う。

表３　本業務受託者に求める作業実施体制の役割

組織等	本業務における役割
業務遂行責任者	本業務全体を統括し、必要な意思決定を行う。また、各関連する組織・部門とのコミュニケーション窓口を担う。
要件定義担当者	排出量取引制度システムに関する要求事項の整理、システム要件の定義を担う。
チームリーダ	排出量取引制度システムに関する設計・開発において作業状況の監視・監督を担うとともに、チーム間の調整を図る。
設計・開発・テスト担当者	排出量取引制度システムに関するアプリケーションの設計・開発・テストを担う。
基盤・運用担当者	排出量取引制度システムに関する基盤、運用の設計・開発・テストを担う。
品質管理者	本業務全体において所定の品質を確保するため、監視・管理を担う。
情報管理責任者	本業務の情報取扱い全てに関する監督を担う。

（２）作業要員に求める資格等の要件

a.　業務遂行責任者

受託者における業務遂行責任者には、本システムと同等規模のシステム開発、短期間での大規模システム開発、及びクラウドサービスを活用したシステムの設計・開発の遂行責任者としての経験を２年以上有し、次のいずれかに該当すること。

・情報処理の促進に関する法律（昭和 45 年法律第 90 号）に基づき実施される情報処理技術者試験のうちプロジェクトマネージャ試験の合格者
・プロジェクトマネジメント協会（PMI）が認定するプロジェクトマネジメントプロフェッショナル（PMP）の資格保有者又は技術士（情報工学部門又は総合技術監理部門（情報工学を選択科目とする者））の資格を有すること
・上記のいずれかの試験合格者・資格保有者等と同等の能力を有することが、経歴等において、明らかな者

b.　チームリーダ

チームリーダは、設計・開発の経験年数を５年以上有すること。また、その中でリーダクラスとしての経験を２年以上有し、次のいずれかに該当すること。複数の資格を持つ者がいる場合、当該者で複数の役割を兼ねることができるものとする。

・システムアーキテクト試験の合格者
・データベーススペシャリスト試験の合格者
・ネットワークスペシャリスト試験の合格者
・上記のいずれかの試験合格者・資格保有者等と同等の能力を有することが、経歴等において、明らかな者

c.　基盤運用担当者

クラウドサービスの基盤運用担当者は、次のいずれかに該当すること。

・主として利用するクラウドサービスについて、当該クラウドサービスプロバイダが認定している資格の中で、上級資格を保有していること。

・上記の試験合格者・資格保有者等と同等の能力を有することが、経歴等において、明らかな者。

d. 情報管理責任者

情報管理責任者は、次のいずれかに該当すること。

・情報処理安全確保支援士試験の合格者または資格登録者
・特定非営利活動法人日本システム監査人協会（SAAJ）が認定する公認情報システム監査人（CAS）の資格保有者
・情報システムコントロール協会（ISACA）が認定する公認情報システム監査人（CISA）の資格保有者
・情報システムコントロール協会（ISACA）が認定する公認情報セキュリティマネージャ（CISM）の資格保有者
・International Information Systems Security Certification Consortium が認定するセキュリティプロフェッショナル認証資格（CISSP）の資格保有者
・上記のいずれかの試験合格者・資格保有者等と同等の能力を有することが、経歴等において、明らかな者。

１０．事業スケジュール

本事業の実施スケジュールの想定は以下の通り。

なお、各機能にかかる要件定義・設計開発について、どの順序で実施するかは受託者と経済産業省担当者と協議の上で確定すること。

１１．入札参加に関する事項

（１） 応札者は、品質マネジメントシステムに係る以下のいずれかの条件を満たすこと。

・品質マネジメントシステムの規格である「JIS Q 9001」又は「ISO9001」（登録活動範囲が情報処理に関するものであること。）の認定を、業務を遂行する組織が有していること。
・上記と同等の品質管理手順及び体制が明確化された品質マネジメントシステムを有している事業者であること（管理体制、品質マネジメントシステム運営規程、品質管理手順規定等を提示すること。）

（２）応札者は、情報セキュリティ実施基準である「JIS Q 27001」、「ISO/IEC27001」又は「ISMS」の認証を有していること。

１２．その他

（１）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。

（２）情報管理体制

①受託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（経済産業省 GX グループ環境経済室）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。

（３）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、経済産業省担当者の指示に従うこと。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】

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。

【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○○○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））。）

（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。

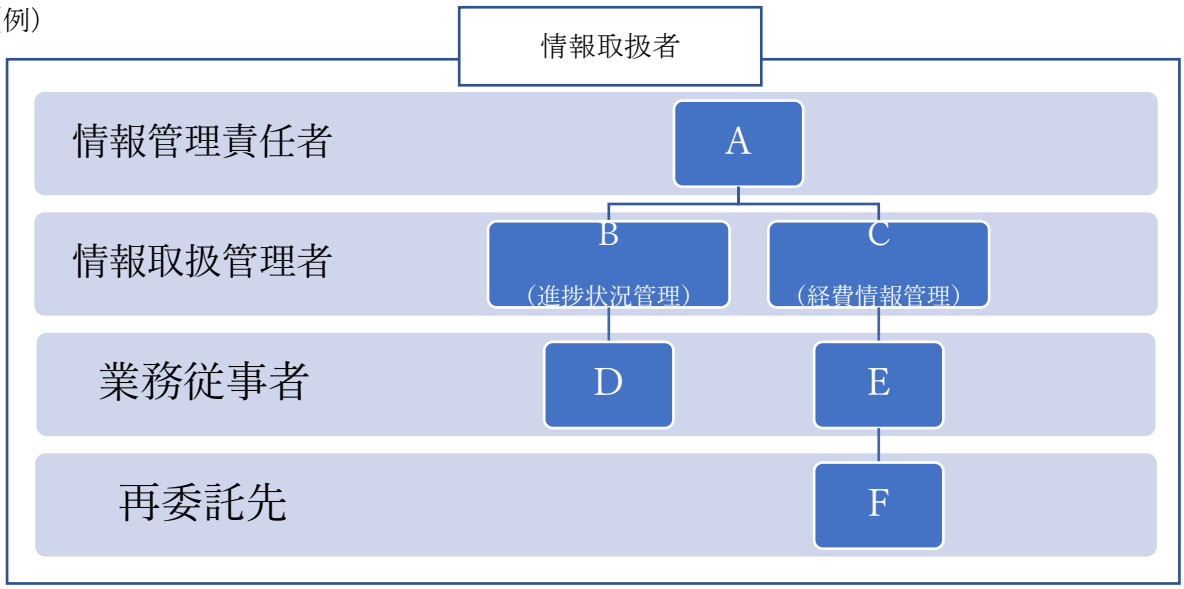
（※３）本事業の遂行にあたって保護すべき情報を取り扱う可能性のある者。

（※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。