（別添１）

スキームＤウェブサイト管理に係る要件

1　https://scheemd.mext.go.jp/　を外部へ情報提供するためのサーバーを用意すること。
2　上記サブドメインに対応すること。
3　ユーザー領域として、契約日より３GB 以上のディスク容量を提供すること。
4　暗号化技術を利用した FTPS 等で発注者においてコンテンツのアップロードが随時可能なこと。
5　意図しないデータ消失に備えてバックアップを行い、最低でも１日前のデータに復旧できること。
6　発注者がウェブサイトを管理できるようにインターネット経由で利用できる管理機能を提供すること。なお、利便性及びセキュリティ上の理由から、操作はウェブブラウザで行えるものとし、TLS1.2 で通信経路を暗号化すること。
7　情報セキュリティに関する要件は、以下のとおりとする。
(1)機密情報と情報セキュリティ
ア　機密情報
　本契約において、機密情報とは本契約締結日以降、本件業務を実施するために文部科学省が受注者に開示する一切の情報をさすものとし、かつ、公には入手できないものとする。なお、前項にかかわらず機密情報が、受注者により以下に該当する情報である旨を証明する通知がなされ、文部科学省が当該通知の内容が適正であるものと判断した場合には、当該機密情報は機密保持義務を負わないものとする。
・既に、公知、公用の情報
・開示後、受注者の責めによらず、公知、公用となった情報
・開示を受けたときに既に受注者が取得していた情報
・開示を受けた後、正当な権限を有する第三者により守秘義務を負うことなしに受注者が入手した情報
・受注者が開示された情報と無関係に開発、創作した情報
・法令により開示することが義務付けられた情報
イ　情報セキュリティ
　受注者は、機密保持につとめ、以下を遵守すること。
(ｱ)契約締結後、速やかに実施すべき遵守事項
・情報セキュリティ対策方針を作成し、以下の内容を明記又は添付の上で主管課に対して説明を行うこと。また、情報セキュリティ対策方針を変更する場合には、速やかに主管課に提出し、承認を得ること。
①情報セキュリティ対策の全般的な実施内容及び管理体制
②機密情報管理者の選任と、機密情報にアクセスする作業員の名簿及び機密情報保持誓約書の提出
③情報セキュリティに関する専門性（資格・研修実績等）・実績に関する情報提供
④情報セキュリティインシデントへの対処方法

⑤情報セキュリティ対策その他の契約の履行状況の確認方法

⑥情報セキュリティ対策の履行が不十分な場合の対処方法

（ｲ） 契約期間中の遵守事項

・文部科学省から開示された機密事項を機密として保持し、また文部科学省の書面による事前の承諾を得ることなく、作業名簿に記載されていない第三者に機密情報を開示、漏洩、公表してはならない。

・機密情報を機密にしておくために合理的な安全保障の予防処置をとらなければならない。

・機密情報の引渡し及び受領については、日時、種類、受取人等記録をつけること。

・機密情報の保管については、施錠管理的適切な対策を施すこと。

・機密情報を電子メールで送信する際は、事前に決めたパスワードを設定の上、送信すること。

・全ての機密情報は文部科学省の所有物であり、かつ文部科学省の所有物のまま残ることを確認する。受注者は機密清報についていかなる権利も有さない。

・機密情報は本業務実施のためのみに利用するものとし、目的外利用については全て禁止する。

・機密情報の複写については、原則禁止とする。ただし事前に書面にて文部科学省の許可を得た場合についてはこの限りではない。

・本件業務に関わる情報セキュリティ事故やその予兆が確認された場合は，必ず当省担当者に報告すること。

・受注者において情報セキュリティ事故が発生した場合は，必ず当省担当者に報告すること。

・当省担当者からの要求に応じて，本件業務の情報セキュリティが確保されていることを確認できる資料を提供すること。

・当省担当者が本件業務の情報セキュリティが確保されていないことを理由に受注者に対する改善を要求された場合は対応すること。

・当省担当者の求めに応じて本件業務に関わる情報セキュリティ監査を受け入れること。

⑵サプライチェーン・リスク対応及び必要提出書類について

ア 本システムの開発・構築等の各工程において、下記（ア）から（オ）の情報セキュリティに係るサプライチェーン・リスクを低減する対策が行われていること。

⑺各工程において信頼できる品質保証体制が確立されていること。

⑴脆弱性検査等のテストの実施が確認できること。

⑼各工程における不正行為の有無について、定期的な監査が行われていること。

⑵製造者が不正な変更を加えないよう、サプライチェーン全体が適切に管理されていること。

⑶不正な変更が発見された場合に、文部科学省と受注者が連携して原因を調査・排除できる体制を整備していること。

イ 本システムに文部科学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ための具体的な管理手順や品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。また、本システムに文部科学省の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や受注者事業

所等への立入検査等、当省と連携して原因を調査し、当省の求めに応じ操作ログや作業履歴等を提出すること。
ウ 責任者及び業務担当者の所属・専門性（情報セキュリティに係る資格・研修実績等）や職務実績、国籍がわかる資料、及び資本関係・役員の情報がわかる資料を提出すること。
エ 調達機器等の選定にあたってはサプライチェーン・リスクに配慮し、候補となる機器等についてはあらかじめ文部科学省に機器等リストを提出し、文部科学省がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、文部科学省と迅速かつ密接に連携し提案の見直しを図ること。

(3)法令等の遵守
ア 受注者は、「政府機関の情報セキュリティ対策のための統一基準群」及び「文部科学省情報セキュリティポリシー」を遵守すること。なお、「文部科学省情報セキュリティポリシー」は非公表の資料であるが、契約締結後に受注者が文部科学省に守秘義務の誓約書を提出した後に開示する。また、各文書については最新版を参照すること。
イ 受注者は、受注業務の実施において、民法、刑法、著作権法、不正アクセス行為の禁止等に関する法律、行政機関の保有する個人情報の保護に関する法律等の関連する法令、行政手続における特定の個人を識別するための番号の利用等に関する法律等を遵守すること。

(4)その他の文書、標準への遵守
ア 本業務の遂行に当たっては、標準ガイドラインに基づき、作業を行うこと。具体的な作業内容及び手順等については、「デジタル・ガバメント推進標準ガイドライン」（デジタル社会推進会議幹事会決定 令和 4 年 4 月 20 日最終改定）を参考とすること。

(5) 情報システムに係る基本的な対策
①違反への対処
当該情報システムにおいて文部科学省情報セキュリティポリシーへの重大な違反の報告を受けた場合及び自ら重大な違反を知った場合には、文部科学省に報告すること。
②障害・事故等の対処
ア 障害・事故等の発生に備えた事前準備
(ｱ) 当該情報システムの情報セキュリティに関する障害・事故等（インシデント及び故障を含む。以下「障害・事故等」という。）が発生した場合、被害の拡大を防ぐとともに、障害・事故等から復旧するための体制を整備すること。
(ｲ) 障害・事故等が発生した際の対処手順を整備すること。
イ 障害・事故等の発生時における報告と応急措置
障害・事故等が発生した場合には、対処手順等に基づいて措置を講ずるとともに、必要に応じて、利用者へ対処の支援を行うこと。
③文部科学省外の情報セキュリティ水準の低下を招く行為の防止
当該情報システムに係る文部科学省外の情報セキュリティ水準の低下を招く行為を防止するために、当該情報システムに関わる以下の行為を禁止する。
・ 文部科学省外の利用者がインターネット等を介して当該情報システムを利用する際に、脆弱

性が指摘されているソフトウェアや、脆弱性が指摘されているバージョンのソフトウェアを利用するように要求すること

・ 文部科学省外の利用者がインターネット等を介して当該情報システムを利用する際に、ソフトウェアの設定を脆弱に設定変更させること

・ 文部科学省外の利用者がインターネット等を介して当該情報システムを利用する際に、ソフトウェアの削除や、ハードウェアの機能の停止を求める行為

④セキュリティホール対策

ア 本件業務で提供される電子計算機及び通信回線装置上で利用しているソフトウェアに係る公開されたセキュリティホールの情報を原則として週に一回程度の頻度で入手すること。

イ 本件業務で提供される電子計算機及び通信回線装置上で利用しているソフトウェアに係るセキュリティホールの情報を入手した場合には、当該セキュリティホールが情報システムにもたらすリスクを分析した上で、以下の事項について判断し、セキュリティホール対策計画を策定すること。

・ 対策の必要性

・ 対策方法

・ 対策方法が存在しない場合の一時的な回避方法

・ 対策方法又は回避方法が情報システムに与える影響

・ 対策の実施予定

・ 対策試験の必要性

・ 対策試験の方法

・ 対策試験の実施予定

ウ セキュリティホール対策計画に基づきセキュリティホール対策を講ずること。

エ 信頼できる方法でパッチ又はバージョンアップソフトウェア等のセキュリティホールを解決するために利用されるファイル（以下「対策用ファイル」という。）を入手すること。また、当該対策用ファイルの完全性検証方法が用意されている場合は、検証を行うこと。

⑤不正プログラム対策

ア 不正プログラムに関する情報の収集に努めること。ウイルス等の感染が認められた場合は、以下のとおり対処すること。

・ 感染した機器を切り離す（物理的に端末を切り離す、若しくは、システム的に切り離してもよい）。

・ 文部科学省に連絡する。

・ 感染の疑いのある他のシステムの検査をする

・ 不正プログラムを駆除する

・ 改ざん等の発生を確認し、必要に応じ、プログラムの再インストールを実施する

・ 当該機器の不正プログラムの再確認を行う

・ 情報システム責任者の承認を経て、当該機器の再接続を行う

イ 不正プログラム対策を検知するために、不正プログラム対策の状況を適宜把握し、その見直しを行うこと。

⑹情報システムの構成要素についての対策

情報システムの構成要素についての対策では、主に以下の観点にて運用・保守をすること。

①サーバ装置に係る要件

情報システムにおいて基準となる時刻に、サーバ装置の時刻を同期すること。

②ウェブに係る要件

ウェブの導入については、次のア及びイの要件を満たすこと。要件を満たすための機能の実装に当たっては、独立行政法人 情報処理推進機構の「安全なウェブサイトの作り方」を参照すること。（http://www.ipa.go.jp/security/vuln/websecurity.html）

ア　ウェブサーバの導入時

情報セキュリティが確保されるよう適切にウェブサーバのセキュリティを維持するための措置として以下の機能を実装すること。

⑺ウェブサーバの機能を必要な機能に制限すること。

⑴ウェブサーバに保存された情報へのアクセス制限を適切に設定すること。

⑼識別コードを適切に管理すること。

⑽個人情報等重要な情報の通信は、暗号化と電子証明書による認証の機能を設けること。

⑾ウェブサーバからウェブクライアントに攻撃の糸口になり得る情報を送信しないように設定すること。

⑿ウェブサーバに保存された情報に機密情報を含む場合は、利用が想定される情報のみをウェブサーバ上に置き、それ以外の利用を想定していない機密情報が含まれないことを確認すること。

イ　ウェブアプリケーションの開発時

情報セキュリティが適切に確保されるようにウェブアプリケーションの開発においてセキュリティを維持するための措置として以下の機能を実装すること。

⑺利用者による URL の確認を妨げないこと。

⑴ウェブアプリケーションが使用するファイルのパス名を限定すること。

⑼不正な入力データを排除すること。

⑽不正な出力データを排除すること。

⑾安全なセッション管理を行うこと。

③文部科学省の管理外の安全区域における対策

情報システムを省外の施設に設置する場合は、以下の措置を講ずること。

ア　立入り及び退出の管理

⑺安全区域（電子計算機及び通信回線装置を設置した事務室又はサーバルーム等の内部であって、アクセスを許可されたもの以外の侵入や自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策が講じられている区域）への不審者等の許可を得ていない者の立入りを防止するために、以下の措置を講ずること。

・ 身分証明書の提示の義務化

・ 安全区域の表示の制限

⑴当該情報システムを設置した安全区域を物理的に隔離し入退出を管理するために、以下の措置を実行すること。

・ 当該安全区域を施錠可能にし、区域を隔離する

・ 当該安全区域が無人になる場合は、扉を施錠する
・ 当該鍵の貸出しを管理する

(ｳ)安全区域に入退室する者が入室を許可された者であることの確認を行うための措置として、以下の対策を実施すること。

・ 当該安全区域に立ち入る資格者の一覧の作成
・ 許可を受けた者の身分証の確認
・ 訪問者の氏名、電話番号、要件、訪問先、入退館時刻の記録

(ｴ)許可を受けた者であっても、夜間、土日など、予定されていない時刻の入退館については、入退館をあらかじめ届け出させ、記録すること

イ　入室後の管理

安全区域に立ち入った者の作業管理を以下のように行うこと。

・ 監督者の配置
・ 許可されない区画への立入り・利用制限
・ カメラ、ビデオ等の記録用機器の利用制限

ウ　電子計算機及び通信回線装置のセキュリティ確保

当該情報システムについては、設置及び利用場所が確定している電子計算機(サーバ、デスクトップ端末等)の盗難及び当該場所からの不正な持ち出しを防止するための措置を講ずるために以下の事項を実施すること。

・ サーバ等はサーバラックに固定し、容易に持ち出せないようにする
・ サーバラックは施錠可能なものにし、操作を実施しないときには施錠する
・ サーバルーム等の安全区域に立ち入った者が施設を立ち去る際に持ち物を確認する
・ デスクトップ端末等は、セキュリティワイヤーで固定する

8　契約終了時のサーバ内のデータ消去については物理破壊又は暗号化消去によることとし、データ適正消去実行証明協議会（ADEC）によるデータ適正消去実行証明を提出すること。