

(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 3 GB 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进行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) 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

- (7) 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。

- (4) 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

(別添1)

開されたセキュリティホール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、システムの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。

(2) 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

(別添 1)

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。

- (ア) ウェブサーバの機能を必要な機能に制限すること。
- (イ) 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。
- (ロ) 識別コードを適切に管理すること。
- (ハ) 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。
- (ニ) 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。
- (ホ) 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。

- (ア) 利用者による URL の確認を妨げないこと。
- (イ) 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。
- (ロ) 不正な入力データを排除すること。
- (ハ) 不正な出力データを排除すること。
- (ニ) 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

- (ア) 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ー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

- (イ) 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

- (ロ) 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

- (ハ) 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

(別添 1)

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
- ・ サーバル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

(3) 情報セキュリティ確保のために参照すべき関連文書

本件業務の遂行に当たっては、情報セキュリティの確保のために、以下の文書の最新版を参照し、準拠、遵守すること。

- ・ 文部科学省情報セキュリティポリシー

※文部科学省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。

- ・ 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3年度版)
- ・ 政府機関等の対策基準策定のためのガイドライン(令和3年度版)

※詳細については内閣官房セキュリティセンターホームページ(<https://www.nisc.go.jp/active/general/ki junr3.html>)を参照すること。

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。