令和７年度「青少年ネット安全・安心のための環境整備事業実施業務」仕様書

１　趣旨

青少年が安全に安心してインターネットを利用する環境を整備するため、ネットパトロール及びネットトラブル相談窓口による有害情報対策を実施するとともに、同業務その他の調査で把握した県内青少年のインターネット利用実態を的確に反映したネットリテラシー促進のための情報モラル教育を推進する。

２　業務実施期間

令和７年４月１日～令和８年３月31日

３　業務実施拠点

⑴ ネットパトロール及びネットトラブル相談窓口
受託者が用意する場所

⑵ ネットリテラシー促進のための情報モラル講座
和歌山県内において県が指定する場所

４　業務内容

⑴ ネットパトロールの実施

ア　インターネット上の各種サイトを探索し、和歌山県内の１８歳未満の青少年（以下「県内青少年」という。）に関する問題行動記事や誹謗中傷記事、個人情報記事等を抽出すること。

イ　対象者は、児童生徒、有職又は無職を問わず、県内青少年とすること。

ウ　発見した書き込み及びトラブル事象（以下「事象」という。）並びにその後の経過等については、飲酒や喫煙などの分類（以下「分類」という。）により分析と整理を行い、１週間毎に報告すること。

エ　ウの報告とは別に月１回、当該月の事象の発見件数、分類及びその後の経過等を前月までの累計とともに作成し、報告すること。

オ　ウの報告にかかわらず、緊急を要する事象については、速やかに報告するとともに、必要に応じてサイト運営会社やインターネットホットラインセンター等の機関に削除依頼すること。

カ　契約期間中、原則として週に５日間のネットパトロールを実施すること。
ただし、受託者における休業日（祝日、年末年始等）を含む週については、県と協議の上実施すること。

⑵ ネットリテラシー促進のための情報モラル講座業務

ア　原則として県内全ての小、中、高等学校及び特別支援学校の児童生徒を対象とし、情報モラル講座を開催すること。
その他の者を対象とする申込又は相談があった場合は、県による実施可否の判断に基づき開催すること。
なお、対象者の取りまとめは県が行い、原則として１校あたり１回までとし、１回あたり１～２時間の開催とする。

イ　講座は、和歌山県が指定する県内各地域で年間８０回程度、開催すること。

ウ　講座の内容は、和歌山県が指定する題材とし、必要に応じて児童生徒との対話形式を取り入れること。

エ　講座を開催した後は、遅延なく講座内容等を記録した報告書を作成し、提出すること。

⑶ ネットトラブル相談窓口の運営

ア　県内青少年に関する誹謗中傷、個人情報の掲載、不適切な画像の掲載、自撮り画像（児童ポルノ相当）の要求等のネットトラブルに関する相談を受け付け、削除方法や対処方法

について、回答を行う和歌山県ネットトラブル相談窓口を運営する。

イ　相談の受付及び回答は、受託者が運営するチャットシステムで(1)カに基づきネットパトロールを実施する日の午後３時から午後７時までの時間帯に行う。

ウ　和歌山県ネットトラブル相談窓口の広報資料を作成の上、各種機会を通じて青少年等に広報を行うこと。

エ　チャットシステムについては、県が監査を行えるものであること。

また、チャットのデータ保存場所は国内に限定することとし、更に海外からはアクセスできないようにすること。なお、不要となったデータは速やかに削除すること。

オ　相談の内容及び回答結果については、原則、取扱日の翌業務日に報告すること。

カ　オの報告にかかわらず、緊急を要する事案については、速やかに報告するとともに、必要に応じてサイト運営会社やインターネットホットラインセンター等の機関に削除依頼すること。

⑷ 県民向け啓発資料の作成

ア　情報モラルに関する県民の意識を啓発するため、月１回、県民向けの啓発資料を作成し提出すること。

イ　啓発資料には、各月ごとのネットパトロールの集計分析結果や、委託事業全般を通じて収集した情報を基に、インターネット上でどのような問題が生じているのか、どのようなことに注意すればネットトラブル被害を防止できるか等の内容を盛り込むこと。

ウ　また、特筆すべき事象については、適宜、事例等としてまとめ、同様に啓発資料として作成し提出すること。

エ　上記資料の内容については、和歌山県と協議した上で、和歌山県ホームページに掲載する。

５　実施体制

⑴　人員体制

ア　ネットパトロール要員　１名以上

イ　情報モラル講座、広報啓発及び調査分析のための要員　１名以上

ウ　ネットトラブル相談窓口要員　１名以上

エ　サポート体制

受託者は、職員の急な欠員等緊急事態が発生しても業務が滞らないような体制を常時整備すること。また、本事業を実施するにあたって個人情報を取り扱う場合においては、個人情報の保護に関する法律（平成１５年法律第５７号）に基づき、その取扱いに十分留意し、漏洩、滅失及び毀損の防止その他個人情報の保護に努めるものとする。

６　対象経費等

本事業に係る経費については、概ね次のとおりとする。

- 人件費、社会保険料等
- 上記職員の活動に要する旅費等の経費
- 講座に要する資料等の経費
- 印刷物等広報に要する経費
- 業務に要する消耗品費、通信運搬費
- 施設に係る光熱水費、維持管理費

７　成果品等

成果品等の提出部数及び納入場所等は、次のとおりとする。

⑴　成果品等及び提出部数

ア　ネットパトロール結果報告書　一式（及び電子データ）

イ　情報モラル講座報告書　一式（及び電子データ）

ウ　ネットトラブル相談窓口報告書　一式（及び電子データ）

エ　啓発資料　　一式（及び電子データ）

⑵ 提出場所

ア　名称　　和歌山県共生社会推進部こども家庭局こども支援課

イ　所在地　郵便番号　６４０－８５８５　和歌山市小松原通一丁目１番地

⑶ 著作権

委託業務を通じて作成した講座、統計、啓発資料等成果品の著作権は、すべて和歌山県に帰属する。

８　その他留意事項

⑴ 本業務は原則として再委託できない。

ただし、一部の業務は協議により再委託することを認める場合がある。

⑵ 業務遂行にあたっては、和歌山県と十分に協議しながら進めること。

⑶ 本事業は新年度事業のため、予算の執行については和歌山県議会の議決を経た令和７年度予算の成立が条件となる。

⑷ 和歌山県の情報セキュリティポリシーを遵守すること。

⑸ 別添【「安全確保の措置」に係る遵守事項】及び【記憶装置のデータ消去及び破壊仕様書】に定める各事項を満たすこと。

またネットトラブル相談窓口の運営にあたり外部サービスを利用する場合には別添【外部サービス要件確認表（機密性２以上）】に定める各事項を満たすこと。

⑹ 本事業で使用するコンピュータ等は、十分なセキュリティ対策を講じること。

また、サイバーテロ、ウイルス感染及び情報漏洩等のセキュリティインシデント発生時には、和歌山県に報告の上、速やかに対応すること。

⑺ 業務に問題が生じた際は、速やかに和歌山県に報告するとともに業務に支障がでないように対応すること。

「安全確保の措置」に係る遵守事項

（基本的事項）
第１　乙は、この契約による事務の実施に当たっては、甲の情報を閲覧する者の個人情報を侵害することのないよう、甲から委託を受けて情報を公開するために利用する機器等の管理を適正に行わなければならない。
２　乙は、この契約による事務の実施に当たり、ホスティングサービス、レンタルサーバー、ハウジングサービス又はこれらに類するサービスを利用する場合は、第１項に沿って本遵守事項に定める各事項を満たすよう、この契約による事務を処理するに当たり、事前にサービス提供者との間で取り決め又は確認をすること。

（ウイルス対策の実践）
第２　乙は、この契約による事務の実施に当たっては、利用するサーバ等の機器について、ウイルス検知用データは常に最新のものに更新すること。
２　Ｗｅｂサーバの管理用又は更新用等にパソコン等の機器を利用する場合は、乙はこれら機器に対しても第１項で規定する措置を講じること。

（ソフトウェアの更新）
第３　乙は、本遵守事項の第２の対象となる機器で利用するソフトウェアに対しては、定期的に修正プログラムを適用し、できる限りソフトウェアを最新の状態にしておくこと。

（ファイアウォールの導入）
第４　乙は、この契約による事務の実施に当たっては、ファイアウォールを設定し通過させるパケットや遮断するパケットに対するルールを設定しておくこと。
２　乙は、侵入防止システム（IPS）を導入すること。ただし、甲の承諾があるときは、この限りでない。

（セキュリティ診断）
第５　乙は、外部の者によるセキュリティ診断を受けること。ただし、甲の承諾があるときは、この限りでない。

（ログのチェック）
第６　乙は、この契約による委託期間中、定期的にログ（Web サーバー、OS、ルータ、DB 等）をチェックすること。

（コンテンツ内容の確認等）
第７　乙は、著作権を侵害するような写真やイラスト、ファイル等は使用しないこと。
２　乙は、この契約による事務を処理するに当たっては、コンテンツの取込持出時の検疫方法と取扱手順を事前に定めておくこと。

（パスワードの管理）
第８　乙は、この契約による事務を処理するに当たっては、本遵守事項の第２の対象となる機器等には安全なパスワードを設定することとし、定期的に変更すること。また、不要なアカウントを登録しないこと。

（コンテンツ等の管理）
第９　乙は、Web サーバやデータベースサーバ等、コンテンツや情報等を格納するディレクトリやファイルに対しては適正なアクセス権限を設定すること。
２　乙は、この契約による事務を処理するに当たり、下記の対策を講じること
① SQL インジェクション、クロスサイト・スクリプティング等の脆弱性への対策を講じること。
② 不要なページやウェブサイトを公開しないこと。

③ 不要なエラーメッセージを返さないこと。
④ 不要なサービスやアプリケーションを起動させないこと。

（セキュリティポリシー）
第１０　乙は、この契約による事務を処理するに当たり、セキュリティポリシーを策定すること。ただし、既にセキュリティポリシーを定めている場合はこの限りではない。
２　乙は、この契約による事務を処理するに当たり、不正侵入やウイルス感染が発生した場合の対応方法を策定しておくこと。ただし、既にこれらの対応方法を定めている場合はこの限りでない。

（調査）
第１１　甲は、乙がこの契約による事務を処理するに当たり、本遵守事項に定める各事項の状況について、随時調査することができるものとする。

(別記第３号様式)

記憶装置のデータ消去及び破壊仕様書

(趣旨)

第１　記憶装置のデータ消去及び破壊仕様書（以下「本仕様書」という。）は、知事部局が管理するシステム及び端末（以下「情報システム」という。）のデータ消去及び破壊について必要な事項を定めるものとする。

ただし、次の各号の何れかに該当する場合は処理に代えることが出来るものとする。

（１）県が利用を認めた外部サービスであって、サービス内で適切な処理を実施する場合

（２）処理が実施されたことを政府機関等又は第三者機関によって認証等されることが明らかと県が認めた場合

(用語の定義)

第２　本仕様書において用いる用語の定義は、次の各号に掲げるところによる。

（１）記憶装置とは、情報システムが停止した後もデータの保存を継続する装置のことをいう。

（２）処理とは、情報システムの記憶装置上の対象データへのアクセスを不可能な状態にする行為をいう。

(処理場所)

第３　処理場所は、県組織の敷地内とする。

なお、情報システムの記憶装置の設置場所が県組織の敷地外にある場合は、当該設置場所にて処理を行うこと。

(処理者)

第４　県から委託を受けた者（以下「受託者」という。）又は受託者から処理を請け負った者（以下「請負者」という。）とする。

なお、第６の１のただし書きに該当する場合を除き、処理は立ち会いも含め２名以上で実施すること。

(記憶装置の処理手順)

第５　処理者は、障害等による交換を含め機器を撤去する前に、処理場所において、記憶装置上の情報を本細則で規定する方法で全て処理すること。

ただし、マイナンバー利用事務系システムの記憶装置については、すべて物理的な方法により破壊すること。

(立ち会い)

第６　受託者又は請負者が処理を行う場合は、原則として、県職員が立ち会うものとする。

ただし、予期し得えず開庁時間以外で処理を行わなければならない場合（以下「緊急処理」という。）、受託者又は請負者が第６の２で定める手続き（以下「代行手続き」という。）を実施することにより、県職員の立ち会いを要しないこととする。

２　代行手続きは、次のとおりとする。

（１）緊急処理の内容を記した報告書（別記第１号様式。以下「緊急処理報告書」という。）及び処理をしたと判る資料（写真、データ消去証明書等）を県に提出すること。

（２）緊急処理報告書は、処理した日の翌開庁日までに提出すること。

(処理の方法)

第７　処理にあたっては、米国国立標準技術研究所規格（NIST SP800-88 rev.1)の消去、除去又は破壊の方式によるものとし、当該規格の付録 A に記載されている方法にて、記憶装置の媒体ごとに適した方法で処理すること。ただし、本方式と同等以上のレベルでデータ消去をおこなえる場合は、この限りでない。

(処理同等措置)

第８　受託者又は請負者は、処理と同等の措置（以下「処理同等措置」という。）を行うことが出来ると考える場合は、次の各号に掲げる事項を全て満たすことが出来ると分かる内容を記した申請書（別記第２号様式。以下「処理同等措置利用申請書」という。）を予め県に対し提出することができるものとする。

この場合、処理同等措置利用申請書の内容を県が認めた場合に限り、受託者又は請負者は処理同等措置を行うことが出来るものとする。

ただし、処理同等措置は処理場所において行わなければならない。

（１）処理場所にて、記憶装置に対し暗号化や専用ツール等によるセキュリティロックをかける等の技術的安全対策（以下「技術的安全対策措置」という。）が可能であること。

（２）技術的安全対策措置を実施した場合、データ復元ソフト等を利用しても記憶装置に記憶された情報を読み出すことは一切不可能であること。

（３）技術的安全対策措置を実施した後は解除することが不可能であること。

（別記第１号様式）

年　　月　　日

和歌山県知事　様

（団体名）
（処理者）
　部署名
　職　名
　署　名

緊　急　処　理　報　告　書

　下記のとおり緊急処理を実施したので報告します。
　なお、報告に反して緊急処理を実施していなかった場合、本報告書で署名した者は連帯して一切の責任を負います。

記

１　契約件名

２　緊急処理を行った理由

３　緊急処理の実施日時
　　年　　月　　日、　　時　　分

４　緊急処理の実施場所

５　緊急処理の内容

６　報告者以外の処理者（複数で処理を行った場合のみ記述）

（団体名） （処理者） 　部署名 　職　名 　署　名 ＿＿＿＿＿＿＿＿ （団体名） （処理者） 　部署名 　職　名 　署　名 ＿＿＿＿＿＿＿＿	（団体名） （処理者） 　部署名 　職　名 　署　名 ＿＿＿＿＿＿＿＿ （団体名） （処理者） 　部署名 　職　名 　署　名 ＿＿＿＿＿＿＿＿

（注）処理をしたと判る資料（写真、データ消去証明書等）を添付すること

（別記第２号様式）

年　　月　　日

和歌山県知事　様

（団体名）
（代表者）
職名
氏名

処 理 同 等 措 置 利 用 申 請 書

下記の契約で利用する記憶装置の交換又は廃棄にあたり、「記憶装置のデータ消去及び破壊仕様書」に規定する処理同等措置の利用を認めて頂くようお願いします。

なお、下記に反した処理を行った場合又は下記の処理同等措置を行った場合でも記憶装置に記憶された情報を読み出すことが出来た場合は一切の責任を負います。

記

１　契約件名

２　処理同等措置の内容

（１）処理場所にて、記憶装置に対し専用ツール等によるセキュリティロックをかける等の技術的安全対策（以下「技術的安全対策措置」という。）が可能です。

（具体的な措置内容）

（２）技術的安全対策措置を実施した後は、データ復元ソフト等を利用しても記憶装置に記憶された情報を読み出すことは一切不可能です。

（具体的な措置内容）

（３）技術的安全対策措置を実施した後は、解除することが一切不可能です。

（具体的な措置内容）

外部サービス要件確認表（機密性２以上）

外部サービス名称			記入日			
外部サービス提供者名称			記入者			
区分		要件	取扱情報が機密性2以上の場合			
			要否	適用状況	備考	
1.外部サービス要件（機密性2以上）						
1.1.	セキュリティ評価制度	利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））への登録が行われていること。	任意			
1.2.		1.1でISMAPへの登録が行われていない場合 利用しようとする外部サービス（アプリケーション）が政府情報システムのためのセキュリティ評価制度「ISMAP-LIU」（ISMAP for Low-Impact Use）への登録が行われていること。	任意			
1.3.	SLA	サービスレベルの保証が定められていること。 SLAには以下の内容が定められていること。 ・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順及び情報セキュリティインシデントの対応等の取り決め ・外部サービス利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得、保持し、定期的にレビューできること。 ・利用する外部サービス又はシステムの技術的脆弱性に関する情報は、公表された後に速やかにクラウドサービス利用者が入手できるようになっていること。	任意			
1.4.	生成AIを利用したサービスにおける入力情報の取扱	外部サービスが生成AIを利用したサービスに該当する場合においては、同サービスへの入力情報が、県の許可なく生成AIの学習に用いられたり、サービスを提供する事業者による監査の対象にならないことが確認できること。	必須			
1.1.でISMAPへの登録が行われている場合、1.2.でISMAP-LIUへの登録が行われている場合、以下の要件は不要						
1.5.	資格・認証 ※アプリケーション 提供事業者のみ	サービス提供を行う組織が、ISO/IEC 27001認証を取得していること。	任意			
1.6.	資格・認証 ※クラウドサービス プロバイダー （外部サービスを構成する基盤部分について記入すること）	サービス提供を行う組織が、ISO/IEC 27001認証を取得していること。	必須			
1.7.		サービス提供を行う組織が、ISO/IEC 27017認証もしくはPCI DSSを取得していること。	必須			
1.8.		サービス提供を行う組織が、ISO/IEC 27018認証を取得していること。	任意			
1.9.	データの所在・適用法と裁判管轄	サービス上のユーザ所有データ（バックアップデータを含む。）の所在地が日本国内に限定できること。	必須			
1.10.		サービス提供事業の実施場所（事務所、運用場所）（地域（リージョン）が特定できるようにすること）を情報提供すること。提供にあたっては文書にて内容を確約すること。	必須			
1.11.		準拠法、裁判管轄を国内に指定できること。	必須			
1.12.		県が登録したデータは、県に確実に提供でき、提供後のデータの所有権・管理権は、県が保有すること。また、県が登録したデータは、本契約に明示的に定められているところを除き、県の承諾なく、利用できないものとすること。	必須			
1.13.	データセンター要件	データセンターは、日本データセンター協会が制定するデータセンターファシリティスタンダードのティア3相当の基準を満たした設備とすること。	必須			
1.5 及び 1.7の認証を取得している場合、以下の要件は不要　※以上の要件を満たせない場合は、以下の各要件について根拠資料等を提出させる等、入念な審査を行う。						
1.14.	セキュリティ対策・体制	サービス提供業務の遂行のために提供する情報（契約等の手続に付随して外部サービス事業者が知りうる利用者情報等）を、サービス提供業務の遂行目的外で利用しないこと。情報の目的外利用の禁止に対する遵守（義務）の表明をすること。	必須			
1.15.		サービス提供を行う組織若しくはその従業員、再委託先又はその他の者によって、県の意図しない変更が加えられないための管理体制について提示すること。	必須			
1.16.		情報セキュリティインシデントが発生した場合に、被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について提示すること。	必須			
1.17.		障害や情報セキュリティインシデントの発生、監査結果等によって、情報セキュリティ対策の履行が不十分であると認められた場合の対処（改善の実施等）方法について提示すること。	必須			
1.18.	データ暗号化	機密性の高いデータ等については、暗号化等によって蓄積・伝送データを保護できること。	必須			
1.19.	ログ取得	外部サービス上におけるアクセスログ等の証跡に係る保存期間について、1年間以上の保存が可能であること。その手法について提示すること。	必須			
1.20.	脆弱性対策	外部サービス上の脆弱性を発見する方法があり、実施可能であること。その手法について提示すること。	必須			
1.21.	不正アクセス対策	通信内容を監視する等により、不正アクセスや不正侵入を検知及び通知できること。	必須			
1.22.	機器停止	機器に異常があった場合、検知できること。 また、機器を死活監視し、停止した場合、検知できること。	必須			
1.23.	データ取扱い時の権限管理	データの取り扱いについて、権限管理及びアクセス制御ができること。	必須			
1.24.	保守端末	保守端末は、認証管理、持出管理、施錠管理、ログ管理等によりセキュリティを確保していること。	必須			
1.25.	データ消去	データを消去する際は、ISO27001に準拠してデータを復元できないように電子的に完全に消去又は廃棄すること。また、データを消去又は廃棄した証明書を提示すること。 なお、ISO27001にデータ消去が未規定の場合、サービス終了までに規定し、認証を受けること。	必須			
1.26.	セキュリティ監査	情報セキュリティ監査の受入れが行われていること。	任意			
1.27.	セキュリティ教育	情報セキュリティ意識の向上を図るための教育を実施する計画が策定され、その実施体制が整備されていること。	必須			