「ネットトラブル対策モデル事業業務委託」仕様書

１　目的

インターネット上での誹謗中傷等の発生・深刻化の防止を図り、県民が安全で安心して暮らせる地域社会作りを推進するため、県民に対する悪質な書き込み情報について、AI 等の先進的検索技術と人による精査体制を組み合わせた効率的なネットパトロールを実施する。

２　ネットパトロール業務概要

インターネット上閲覧可能な、第三者の運営・管理する SNS、掲示板、ブログ、画像・動画等共有サービス及びその他一般的な検索サイト等の WEB サービス全般（以下「各種サイト」という。）を網羅先に検索し、県民に係る誹謗中傷等の疑いのある投稿等の情報を収集し、別途定める危険度及び内容に応じて県に報告する。

３　業務実施期間

契約締結日～令和７年３月 31 日

４　業務実施拠点

受託者の定める場所

５　業務内容

ネットパトロールの実施

（１）　調査対象

ア　対象者は、山梨県に在住すると思われる者とし、年齢、国籍、有職又は無職を問わない。

（２）　検索対象

ア　各種サイトにおける県民に関する悪質な書き込み情報（問題行動記事・誹謗中傷記事・個人情報記事等）を検索し判定すること。

イ　検索は、クローラー等の自動検索機能やサイト内検索機能等を活用することで網羅的に行うとともに、判定では、AI による自動判定及びフィルタリングと、目視による人的な確認を組み合わせすことにより、効率化と判定精度の向上を図ること。

ウ　悪質な書き込み情報で被害を受けている者が県民と特定するために、県内の「市町村名」、「学校名」、「団体・企業名」、「イベント名」等を条件として検索すること。また、検索キーワードは本業務に有効と考えるものを提案し、県と協議の上で設定すること。また、キーワードは随時変更できるものとする。

エ　警察庁で実施しているサイバーパトロールにおいて監視対象としている違法・有害情報に関するものは本業務に含まないものとする。詳細は県と協議の上で設定すること。

（３）　調査の結果報告

抽出された書き込み情報を危険度及び内容に応じて下表のとおり分類する。

	危険度	内　容
①	レベル１	・自分自身の個人情報の公開　※
②	レベル２	・自分自身の詳細な個人情報の公開 （※に該当する情報に加えて、県民自身のアカウントのＱＲコード、答案用紙、合格証書の画像等が掲載されたもの）
③		・他人の個人情報の公開（生徒名簿、座席表の画像等）
④		・個人を特定した誹謗中傷
⑤		・情緒不安定等
⑥		・暴力・問題行動（例:児童生徒の飲酒・喫煙、迷惑・危険行為）
⑦		・わいせつ表現（画像等）
⑧	レベル３	・県民を対象とした殺害予告、自殺に係るもの　※

※氏名・市町村名・本人と分かる顔画像等の３つにより、個人を特定出来る書き込み

ア　定期報告

受託者は、危険度の別に分類し、当該月の問題のある書き込みについて、検索・判定結果のリスト及びスクリーンショットをまとめて（レベル１はリストのみ）、毎月１回、原則、調査実施月の翌月５日までに電子メール添付により報告すること。

イ　随時報告

受託者は、危険度別に分類した結果、レベル２・レベル３に分類された書き込みについて、以下に留意の上、電子メール添付により随時報告を行うこと。

- レベル２に分類された書き込みは、発見日から起算して、閉庁日を除き２日以内に、レベル３に分類された書き込みは直ちに報告を行うこと。
- 問題のある書き込みをスクリーンショット等で保存した画像を添付するとともに、問題のある書き込みの問題点を明示すること。
- レベル３に分類された書き込みのうち、生命に関わる書き込み等、緊急性が高いものについては、県が定めた電話連絡先へ緊急連絡を行うこと。

ウ　契約期間中、原則として１日４時間以上、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。

エ　定期報告及び随時報告にあたり、容量制限など、電子メール添付に技術的課題がある場合は、受託者が作成する報告用ウェブサイトへのアップロードによる報告を併用しても差し支えない。

（４）抽出された書き込み情報に対し、必要に応じて削除に向けた対策支援を行う。

６　実施体制

- 受託者は、業務を執行するにあたり、監視員を２名以上配置すること。
- 受託者は、業務を円滑に運営するため、監視員とは別に、監視業務責任者を１名以上配置すること。なお、監視業務責任者は、SNS 等への問題投稿の検索・監視等業務に従事する経験が３年以上の者、又は同等の経験を有する者とする。
- 監視業務責任者は、本仕様書４②ア及びイの定期報告及び随時報告を行うほか、監視員に対する指導を行うこと。また、緊急の対応を要する書き込みを発見した場合等については、県への連絡体制を確保するなど、業務の円滑な執行管理を行うこと。
- 受託者は、本業務開始時までに監視業務責任者及び監視員の名簿を県に提出しなければならない。また、監視業務責任者又は監視員名簿の変更を行う必要が生じた場合には、受託者は、事前にその内容を提出すること。
- 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、個人情報取扱特記事項に基づき、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。

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。

（１）　成果品等及び提出部数

ネットパトロール結果報告書一式（紙媒体及び電子データ）

※ネットパトロール結果報告書には、定期報告、随時報告を集計し、傾向等を記した実績報告書を添付すること。

※紙媒体は、下記提出場所に持参又は郵送にて２部提出し、電子データは、下記メールアドレスへの送付又は CD-R 等の電子記録媒体により提出すること。

（２）提出場所

ア　名称　　山梨県県民生活部県民生活安全課人権・生活安全担当

イ　所在地　郵便番号　４００－８５０１　甲府市丸の内一丁目６番１号

ウ　電話連絡先　０５５－２２３－１３５２

エ　メールアドレス　shokuhin-st@pref.yamanashi.lg.jp

８　その他留意事項

（１）　本業務は原則として再委託できない。ただし、山梨県との協議により再委託することを認める場合がある。

（２）業務遂行にあたっては、山梨県と十分に協議しながら進めること。

（３）山梨県の情報セキュリティポリシーを遵守すること。

（４）別添【「安全確保の措置」に係る遵守事項】に定める各事項を満たすこと。

（５）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、ウィ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、山梨県に報告の上、速やかに対応すること。

（６）業務に問題が生じた際は、速やかに山梨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。