令和7年度「環境問題の情報発信・解析及び市民参加型環境イベント実施業務」委託に関する仕様書

１．業務名

令和7年度「環境問題の情報発信・解析及び市民参加型環境イベント実施業務」

２．業務目的

本業務では、WEBサイトやSNSアカウントを使った情報発信や市民参加型環境イベントの実施を通じて、ごみの減量・リサイクルや海洋ごみ問題などの環境問題への市民の意識啓発を図ることを目的とする。

３．契約方法

委託契約・総価契約

４．契約期間

令和7年4月1日～令和8年3月31日まで

５．業務内容

（１）WEBサイト「GO GREEN KOBE」を使った情報発信

① 本市のWEBサイト「GO GREEN KOBE」の管理・運用を行うこと。

【URL】

「GO GREEN KOBE」：https://gogreenkobe.jp/

「こうべキエーロ」による生ごみの減量や海洋ごみ問題など、広く環境問題を啓発するサイト。

② 本業務の趣旨・目的が市民に広く理解され、波及効果が期待できるような記事の企画・作成を行い、WEBサイトに掲載すること。

③ 記事の作成に必要な情報収集や調査、取材を行うこと（月1回以上）。

④ 取材先への調整や、写真・動画撮影を行うこと（月1回以上）。

⑤　本市からの提供記事や独自に作成した記事を編集し、記事等のアップロードを行うこと（年間15回以上）。

⑥　WEBサイトを通して問い合わせを受けた際には、内容を確認し回答を行うこと。なお、回答内容は必要に応じて本市と協議を行うこと。

⑦　別紙1「ホームページサーバ等確認チェックリスト（第2版）」および別紙2「ウェブアプリケーションのセキュリティ実装チェックリスト」のチェック項目に基づき、WEBサイトおよびサーバの運用を行うこと。また、契約締結後各チェックリストを記入し提出すること。

※　③～⑤の具体的な実施スケジュールについては、本市と協議の上決定すること。

（２）WEBサイト「KOBE PLASTIC NEXT」を使った情報発信

①　本市のWEBサイト「KOBE PLASTIC NEXT」の管理・運用を行うこと。

【URL】

「KOBE PLASTIC NEXT」：https://kobeplasticnext.jp/

エコノバ（資源回収ステーション）、つめかえパックリサイクル、ボトルtoボトルリサイクルを中心に、プラスチック問題を啓発するサイト。

②　本業務の趣旨・目的が市民に広く理解され、波及効果が期待できるような記事の企画・作成を行い、WEBサイトに掲載すること。

③　記事の作成に必要な情報収集や調査、取材を行うこと（月1回以上）。

④　取材先への調整や、写真・動画撮影を行うこと（月1回以上）。

⑤　本市からの提供記事や独自に作成した記事を編集し、記事等のアップロードを行うこと（年間15回以上）。

⑥　WEBサイトを通して問い合わせを受けた際には、内容を確認し回答を行うこと。なお、回答内容は必要に応じて本市と協議を行うこと。

⑦　別紙1「ホームページサーバ等確認チェックリスト（第2版）」および別紙2「ウェブアプリケーションのセキュリティ実装チェックリスト」のチェック項目に基づき、WEBサイトおよびサーバの運用を行うこと。また、契約締結後各チェックリストを記入し提出すること。

※　③～⑤の具体的な実施スケジュールについては、本市と協議の上決定すること。

（３）SNSアカウントを使った情報発信

① 本市の既存の公式Facebook（GO GREEN KOBE）及びInstagram（@gogreenkobe）のアカウント（以下、「SNSアカウント」という。）を引き継ぎ、環境問題に関する記事掲載や、リアルタイムかつSNSの特性に応じた環境情報の情報発信を行うこと。また、別途本市が指定するハッシュタグも使うこと。

【留意事項】

Instagram のフィード投稿・ストーリーズ投稿・リール投稿の使い分けにあたっては、それぞれの投稿の特性や閲覧するユーザーの属性を踏まえて内容を検討し、本市に提案すること。

② 本業務の趣旨・目的が市民に広く理解され、波及効果が期待できるような記事の企画・作成を行い、SNSアカウントに掲載すること（更新は令和8年3月中旬まで週2回以上実施）。また、掲載にあたっては環境省や他の環境団体が作成した記事をシェアするなどして活用することも可とする。（ただし、シェアする際には出典等を明らかにするとともに、記事の信ぴょう性についても十分確認すること）

③ SNSアカウントの認知度向上のため、本業務完了時点でのフォロワー数をFacebook及びInstagramそれぞれで2,500人を目標とし、目標を達成するための取り組みを提案し、本市と協議の上実施すること。

④ 既にSNSなどで一定の発信力を持っているインフルエンサー等と連携し、環境活動に関する情報を魅力的に発信する手法を提案し実施すること。

⑤ 市内で環境活動を行い活躍している若い世代とも連携し、SNSやWEBサイト、プロモーション動画など若い世代に響く手法を活用し、発信すること。

（４）市民参加型環境イベントの提案及び実施

① 企画・提案

ごみの減量・リサイクルなどの環境問題に関する市民参加型イベントを下記のとおり実施すること。

イベント開催規模	回数
目標参加者数：累計1,500人以上	１回以上

なお、企画に際しては以下の点を考慮した企画内容とすること。

・ 本市の事業（食品ロス削減、こうべキエーロ、マイボトル啓発、エコノバ（資源

回収ステーション）、つめかえパックリサイクル等）とも関連し、ごみ減量・リサイクルや海洋プラスチックごみ問題を効果的に啓発できるような実施方法を検討すること。

（参考）

- 神戸市ホームページ「ごみ減量のススメ」
  https://www.city.kobe.lg.jp/a25748/kurashi/recycle/gomi/genryo/3r/index.html
- 神戸市ホームページ「海洋プラスチックごみ問題」
  https://www.city.kobe.lg.jp/a25748/kurashi/recycle/education/kaiyougomi.html

・ 参加者が環境問題を自分事として捉え、自らの生活に取り入れるきっかけになる内容とすること。

② スケジュール

イベント開催までのスケジュール(広報や会場・出演者との調整、制作物の作成等に係る進捗管理)について提案すること。

③ 広報・申込受付対応

・ イベント参加者の募集に必要なチラシやポスター、SNS掲載画像等をデザイン・作成すること。また、WEBサイトやSNSアカウント（広告掲載を含む）を活用して効果的に発信すること。

・ 必要に応じて参加者の申込受付や問い合わせ対応を行うこと。

④ 保険

参加者および会場に対する保険の加入に必要な手続きを行うこと。

⑤ 会場設営・撤去

・ 会場の設営および撤去を行うこと。

・ 資材の調達においては、リース・レンタル用品や再生利用された原材料を使用した物品を調達するなど、可能な限り環境負荷の低減に努めること。

⑥ 当日運営

・ 当日の円滑な運営のために必要な進行表や会場図面等を予め作成し、本市と協議のうえ決定すること。

・ 来場者案内や呼び込み、問合せ対応等を行うこと。

・ 十分な安全対策および安全管理(熱中症予防対策、感染症対策含む)を行うために必要なスタッフを配置し、事故を防止すること。

・ 廃棄物が発生する場合は、廃棄物の発生抑制に努めるとともに適正に処理すること。

・ 上記以外に、当日運営に必要な一切の業務を行うこと。

⑦ 結果報告

イベント参加者数を含む当日の開催状況を記載した報告書を、各イベント終了後に提出すること。また、記録写真も併せて提出すること。

（5）WEBサイト・SNSアカウント運用状況の解析業務

① 1ヶ月毎のWEBサイト・SNSアカウント運用状況の解析結果、及び運用における課題を可視化し報告書にまとめ、PDFデータを電子メールにて提出すること。また、上半期（4月1日～9月30日）時点での解析結果および課題を報告書にまとめ、10月上旬にPDFデータを電子メールにて提出すること。

【留意事項】

解析の際は、下記事項を含め報告書にまとめること。

・ WEBサイト：PV数、（アクセス）ユーザー数、各ページのビュー数、WEBサイトへの主な流入経路

・ SNSアカウント：投稿数、リーチ数、エンゲージメント数（率）、プロフィールからのWEBサイトアクセス数（率）

② 上記の結果に基づき、記事内容やSNSの配信方法について、本市へKPIの観点から改善策を提案し、それを実施すること。

（6）ミーティング

本業務の進め方の協議や進行管理・成果等について、常に本市と連携を図り、情報共有しながら適切な業務が遂行されるよう、対面またはオンラインでのミーティングを適宜開催すること。

6．その他留意事項

（1）本業務に必要な調整全般を行うこと。

（２）本業務で個人情報の取り扱いが生じる場合は、本市の「神戸市情報セキュリティポリシー」及び「情報セキュリティ遵守特記事項」を遵守すること。

なお、「神戸市情報セキュリティポリシー」及び「情報セキュリティ遵守特記事項」については、以下のホームページを参照すること。

https://www.city.kobe.lg.jp/a06814/shise/jore/youkou/0400/policy.html

（３）印刷物を作成する場合は、可能な限り「神戸市グリーン調達等方針に係る判断基準」【21-2 印刷】に定めるAランクの条件を満たすとともに、成果物にはリサイクル適正ランクを表示すること。

７．成果物

（１）動画・作品・写真データ

本業務で作成した動画・作品・写真データ等を、必要に応じて都度納品すること。

・提出形式：電子データ

（２）業務完了報告書

本業務完了後、WEBサイト・SNSアカウントの運用やイベントの実施等について活動実績を記載した報告書を提出すること。

・提出期限：令和8年3月31日

・提出方法：PDFデータを電子メールで提出

（３）納品先

神戸市環境局資源循環課

メールアドレス: 3r@city.kobe.lg.jp

８．その他の事項

（１）実施体制

本業務を円滑かつ確実に遂行することが可能な体制を整備すること。また、業務全体を統率する業務遂行責任者をおくこと。

（２）年間の事業実施スケジュール（事業計画書）及び月次活動計画書の作成

契約締結後、年間の事業実施スケジュール（事業計画書）を作成し、提出すること。

（３）再委託について

原則として、本業務の全部または一部を第三者に再委託してはならない。ただし、事前に書面にて報告し、本市の承諾を得たときは、この限りではない。

（４）著作権の帰属

この契約により作成される成果物の著作権は以下に定めるところによる。

① 成果物の著作権（著作権法第 27 条及び第 28 条に規定する権利を含む。） は、発注者である本市に譲渡するものとし、譲渡に係る費用は見積金額に含めること。また、譲渡が難しい場合においては、本市と協議の上、譲渡を行わないことができる。ただし、その場合においても、本市の使用権及び改変を要求する権利は留保しておくこととする。

② 受託者は、本市に譲渡する前項の著作権法上の権利を、本市以外の第三者に譲渡しないこと。

③ 受託者は、本市の事前の回答を得なければ、著作権法第 18 条及び第 19 条を行使することができないものとする。

（５）秘密の遵守

受託者は、本業務により知り得た情報等を本業務においてのみ使用することとし、これらを他の目的に使用し、又は他のものに漏洩してはならない。本業務の契約が終了し、又は解除された後においても同様とする。

（６）仕様変更

受託者は、本仕様書の変更を必要とする場合には、あらかじめ本市と協議のうえ、承認を得ること。

（７）記載外事項

本仕様書に定めのない事項または本仕様書について疑義の生じた事項については、本市と受託者とが協議して定めるものとする。

（８）帳簿等の保管

受託者は、委託料の対象となる経費の支出状況等が分かる帳簿等を整備するものとし、本業務を完了し、又は中止し、若しくは廃止した日の属する年度の終了後5年間これを保存しておかなければならない。

（９）第三者の権利侵害

受託者は、納品する成果物について、第三者の商標権、肖像権、著作権、その他の諸権利を侵害するものではないことを保証することとし、成果物について第三者の権利を侵害していた場合に生じる問題の一切の責任は、受託者が負うものとする。

（10）業務の引き継ぎ

本業務の契約履行期間の満了、全部もしくは一部の解除、またはその他契約の終了事由の如何を問わず、本業務が終了となる場合には、受託者は本市の指示のもと、本業務終了日までに本市が継続して本業務を遂行できるよう必要な措置を講じるため、業務引き継ぎに伴う本業務の関係者への連絡やシステム移行等に必要となる構成要素（WEBサイトやSNSアカウント等）を円滑に提供できるようにすること。なお、移行用のページやコンテンツ等の提供に係る費用は保守運用契約に含まれるものとし、新たな費用は発生しないものとして取り扱うこと。

別紙1

ホームページサーバ等確認チェックリスト（第2版）

ホームページタイトル	
URL（トップページ）	
所管局・部・課	環境局資源循環課
外部委託先事業者名	
担当者連絡先	

※選択肢は、プルダウンメニューから選択してください

回答結果については取扱注意

※　回答が「いいえ」になっている場合は，危険な状態です。早急に改善をお願いします。
※　調査結果は所管課で確認し，回答内容はセキュリティ情報のため関係者以外には秘密にして下さい。

チェック項目			説　明
A. サーバで使用しているOS・ミドルウェア・ウェブアプリケーションの脆弱性の確認 **（WAFやIPS等により脆弱性への攻撃に対する対応を別途行っている場合は、「はい」と回答しても構いません。）**			
1	**サーバで使用しているOSにセキュリティパッチを速やかに適用しているか（重要）** **（［いいえの場合］は非常に危険です。）**		OSの脆弱性を利用することにより、管理者権限を奪われ、サーバを乗っ取られたり、不正なプログラムを実行されます。セキュリティパッチは必ず実行するようにしてください。
2	**サーバで使用しているミドルウェア（OS上で動作し、アプリケーションソフトに対してOSよりも高度で具体的な機能を提供するソフトウェア。OSとアプリケーションソフトの中間的な性格を持っている。）に速やかにセキュリティパッチを適用したり最新版にアップデートしているか（重要）** **（［いいえの場合］は危険です。）**		ミドルウェアにも脆弱性が存在しており、脆弱性を放置しているとそれを利用したウェブサイトの改ざん等が行われる可能性が高まります。速やかにセキュリティパッチを実行したり、最新版へのアップデートを行ってください。 ※ミドルウェアの例 Struts,JBoss,ColdFusion,Tomcat,WebSphere,WebLogic,Joomla!,Apache HTTP Server,IIS
3	**サーバで使用しているアプリケーションソフトに速やかにセキュリティパッチを適用したり最新版にアップデートしているか（重要）** **（［いいえの場合］は非常に危険です。）**		アプリケーションソフトにも脆弱性が存在しており、脆弱性を放置しているとそれを利用したウェブサイトの改ざん等が行われる可能性が高まります。速やかにセキュリティパッチを実行したり、最新版へのアップデートを行ってください。
4～14については、別紙「ウェブアプリケーションのセキュリティ実装 チェックリスト（IPA作成）」でチェックを実施した上でご回答ください。 **（別紙のチェックリストで未対策の項目にチェックが入っている場合に、いいえと回答してください）** **ウェブアプリケーションを使用していない場合は、該当なしと回答してください。**			
4	SQLインジェクションに対する対策はできているか		「SQLインジェクション」とは、データベースと連携したウェブアプリケーションにおいて、SQL文（データベースへの命令文）の組み立て方法に問題があり、それを利用して不正にデータベースを利用しようとする攻撃のことを指します。 情報漏えいやデータベースの改ざんの他、不正ログイン等が行われる可能性があります。
5	OSコマンドインジェクションに対する対策はできているか		「OSコマンドインジェクション」とは、外部からウェブサイトへOSを操作するコマンドを含んだ要求を送ることにより、OSを不正に操作しようとする攻撃のことを指します。 情報漏えいやデータベースの改ざんの他、不正ログインやそのサーバを踏み台とした他のサーバへの攻撃等が行われる可能性があります。
6	ディレクトリ・トラバーサルに対する対策はできているか		「ディレクトリ・トラバーサル」とは、パラメータにファイル名を指定しているウェブアプリケーションで、ファイル名指定の実装に問題がある場合、それを利用して外部から任意のファイルを指定し、アプリケーションが意図しない操作をさせる攻撃のことを指します。 情報漏えいやデータベースの改ざん等が行われる可能性があります。
7	セッション管理の不備に対する対策はできているか		「セッション管理の不備」とは、セッションID（利用者を識別するための情報）を発行し、セッション管理を行っているウェブアプリケーションで、セッション管理に問題がある場合、それを利用してログイン中の利用者になりすます攻撃のことを指します。 情報漏えいやデータの改ざん等が行われる可能性があります。
8	クロスサイト・スクリプティングに対する対策はできているか		「クロスサイト・スクリプティング」とは、利用者の入力情報等を基にウェブページを作成するウェブアプリケーションで、ウェブページへの出力処理に問題がある場合、それを利用してウェブページへ不正なスクリプト（小さなプログラム）を埋め込む攻撃のことを指します。 ウェブサイト上への偽のページの作成やCookieの窃取等が行われる可能性があります。
9	クロスサイト・リクエスト・フォージェリに対する対策はできているか		「クロスサイト・リクエスト・フォージェリ」とは、ログイン機能の存在するウェブサイトで、ログインした利用者からのリクエストについて、その利用者が意図したリクエストであるかどうかを識別する仕組みを持たない場合、それを利用して利用者が予期しない処理を実行させる攻撃のことを指します。 情報漏えいやデータの改ざん等が行われる可能性があります。
10	HTTPヘッダ・インジェクションに対する対策はできているか		「HTTPヘッダ・インジェクション」とは、HTTP レスポンスヘッダの出力処理に問題があるウェブアプリケーションで、攻撃者が、レスポンス内容に任意のヘッダフィールドを追加したり、任意のボディを作成したり、複数のレスポンスを作り出すような攻撃のことを指します。 ウェブサイト上への偽のページの作成やCookieの窃取等が行われる可能性があります。
11	メールヘッダ・インジェクションに対する対策はできているか		「メールヘッダ・インジェクション」とは、利用者が入力した内容を、特定のメールアドレスに送信する機能を持つウェブアプリケーションに問題がある場合、攻撃者が、任意のメールアドレスを指定してメールを送信させる攻撃のことを指します。 迷惑メール等の送信が行われる可能性があります。
12	クリックジャッキングに対する対策はできているか		「クリックジャッキング」とは、ログインしている利用者のみが使用可能な機能がマウス操作のみで使用可能な場合、細工された外部サイトを閲覧し操作することにより、利用者が誤操作し、意図しない機能を実行させる攻撃のことを指します。 ログイン後の利用者のみが利用可能なサービスの悪用や設定の変更が行われる可能性があります。
13	バッファオーバーフローに対する対策はできているか		「バッファオーバーフロー」とは、プログラムが入力されたデータを適切に扱わない場合、プログラムが確保したメモリの領域を超えて領域外のメモリが上書きされ、意図しないコードを実行してしまう攻撃のことを指します。 プログラムの異常終了や任意のプログラムが実行されウイルス感染等が行われる可能性があります。
14	アクセス制御や認可制御の欠落に対する対策はできているか		「アクセス制御や認可制御の欠落」とは、パスワード等の秘密情報の入力を必要とする認証機能やログイン中の利用者が他人になりすましてアクセスできないようにする機能が必要であるにも関わらず実装されていないことを指します。 情報漏えいやデータの改ざん等が行われる可能性があります。

	チェック項目		説　明
B. 更新のためのアカウント・パスワード等の確認			
15	**更新方法にFTP（File Transfer Protocol）を使用していないか（重要）（ＦＴＰを使用している場合=［いいえの場合］は非常に危険です。）**		FTP（ファイル転送プロトコル）は，ホームページデータをサーバにアップロードする際に，よく使用される仕組みですが，Gumblarなどウイルスに対して脆弱性があります。従来はこの仕組みが主流でしたが，項目16のとおり，できるだけ早く移行するかwebサービスの見直しをしてください。
16	更新方法にFTPを使用している場合，SFTP（Secure Copy Protocol），SCP(SSH File Transfer Protocol) その他暗号化による方法への移行ができるか		FTPは，データを暗号化せずに通信するため，IDやパスワードを盗まれる恐れがあります。SFTPやSCPの仕組みはデータを暗号化して通信するため，これらのリスクを低減できます。暗号化が困難な場合は，回線を通じて画面更新をせず，媒体を使う運用方法も考えられます。
17	FTPやSFTP，SSH等を使用している場合、ID，パスワードを定期的(6ヶ月に1回以上）に変更しているか		ID・パスワードを盗まれるリスクを考慮して，定期的（6ヶ月に1回以上）に変更することが推奨されます。
18	FTPやSFTP，SSH等を使用している場合、パスワードは、8桁以上の複雑なもの（少なくとも英数小文字大文字混合）にしているか		辞書攻撃による不正アクセスを防ぐためにも、複雑なパスワードにすることが推奨されます。
19	FTPやSFTP，SSH等を使用している場合、必要最低限のIDしか利用できないようにしているか		不要なIDが残されていると、それを利用して不正アクセスが行われることが考えられます。定期的に不要なIDをチェックし、削除することを推奨します。
C. その他項目の確認			
20	ウイルス対策ソフトの定義ファイルは最新状態か		ウイルス対策ソフトの定義ファイルの適用日付を確認してください。
21	**サーバに接続（更新作業）できる発信元IPアドレスの制限はかけているか（重要）（制限していない場合=［いいえの場合］は非常に危険です。）**		発信元IPアドレスを制限しないと，FTPのIP・パスワードが漏えいすることで，世界中からホームページを改ざんされる恐れがあります。必ず発信元IPアドレス制限は実施してください。但し，レンタルサーバ等を利用している場合でこの方法が技術的に困難な場合は，他の方法（特に項番14）でセキュリティを確保するようにして下さい。
22	サーバにおいて、必要のないサービスを稼動させていないか、また、必要なサービスであっても、それに対するアクセス権限を必要最低限に設定しているか		ウェブサイト運営に必要のないサービスがウェブサーバ上で稼動している場合、そのサービスに対する管理が十分でなく、脆弱性が存在するバージョンをそのまま利用している可能性があるため、不要なサービスは稼動させず、必要な最低限のサービスのみ稼動させるようにしてください。
23	ホームページの改ざんチェックができる仕組みを導入しているかもしくはサーバに不審なアクセスが行われていないか、また、不正なフォルダやファイル等が作成されていないか定期的に確認（1日1回以上）しているか		ホームページの改ざんチェックサービスを利用するなど、改ざんを検知できる仕組みが整っていることが望ましいですが、少なくとも、改ざんされていないか定期的に確認を行うことは必要です。
24	公開しているウェブサイトのデータを定期的にバックアップしているか		ウェブサイトのデータのバックアップがないと、サイトを復旧させる際に、再度データの作成から始めていかないといけなくなります。定期的に、ウェブサイトのデータのバックアップを取得しておきましょう。
25	ウェブサイト等の復旧手順が策定され、定期的に手順の確認を行っているか		事件・事故が発生した場合に備えて、復旧手順を策定し、手順を確認しておくことが必要です。
26	ウェブサイト等のドメインはLGドメイン（～.lg.jp）を利用しているか。		LGドメイン以外のドメイン（.com、.net、.jpなど）は誰でも取得ができるので、ホームページを閉鎖した後に第三者に取得され賭博やアダルトサイト等に利用される事案が発生しています。他のドメインを利用しなければいけない理由が特にない場合は、LGドメインを取得してください。

別紙2

「安全なウェブサイトの作り方 改訂第7版」（チェックリスト）　　IPA（独立行政法人情報処理推進機構）

■ ウェブアプリケーションのセキュリティ実装 チェックリスト（1/3）

No	脆弱性の種類	対策の性質	チェック	実施項目	解説
1	SQLインジェクション	**根本的解決**	※ □ 対応済 □ 未対策 □ 対応不要	□ **SQL文の組み立ては全てプレースホルダで実装する。**	1-(i)-a
				□ **SQL文の構成を文字列連結により行う場合は、アプリケーションの変数をSQL文のリテラルとして正しく構成する。**	1-(i)-b
		根本的解決	□ 対応済 □ 未対策 □ 対応不要	**ウェブアプリケーションに渡されるパラメータにSQL文を直接指定しない。**	1-(ii)
		保険的対策	□ 対応済 □ 未対策 □ 対応不要	エラーメッセージをそのままブラウザに表示しない。	1-(iii)
		保険的対策	□ 対応済 □ 未対策 □ 対応不要	データベースアカウントに適切な権限を与える。	1-(iv)
2	OSコマンド・インジェクション	**根本的解決**	□ 対応済 □ 未対策 □ 対応不要	□ **シェルを起動できる言語機能の利用を避ける。**	2-(i)
		保険的対策	□ 対応済 □ 未対策 □ 対応不要	□ シェルを起動できる言語機能を利用する場合は、その引数を構成する全ての変数に対してチェックを行い、あらかじめ許可した処理のみを実行する。	2-(ii)
3	パス名パラメータの未チェック／ディレクトリ・トラバーサル	**根本的解決**	※ □ 対応済 □ 未対策 □ 対応不要	□ **外部からのパラメータでウェブサーバ内のファイル名を直接指定する実装を避ける。**	3-(i)-a
				□ **ファイルを開く際は、固定のディレクトリを指定し、かつファイル名にディレクトリ名が含まれないようにする。**	3-(i)-b
		保険的対策	□ 対応済 □ 未対策 □ 対応不要	ウェブサーバ内のファイルへのアクセス権限の設定を正しく管理する。	3-(ii)
		保険的対策	□ 対応済 □ 未対策 □ 対応不要	ファイル名のチェックを行う。	3-(iii)
4	セッション管理の不備	**根本的解決**	□ 対応済 □ 未対策 □ 対応不要	**セッションIDを推測が困難なものにする。**	4-(i)
		根本的解決	□ 対応済 □ 未対策 □ 対応不要	**セッションIDをURLパラメータに格納しない。**	4-(ii)
		根本的解決	□ 対応済 □ 未対策 □ 対応不要	**HTTPS通信で利用するCookieにはsecure属性を加える。**	4-(iii)
		根本的解決	※ □ 対応済 □ 未対策 □ 対応不要	□ **ログイン成功後に、新しくセッションを開始する。**	4-(iv)-a
				□ **ログイン成功後に、既存のセッションIDとは別に秘密情報を発行し、ページの遷移ごとにその値を確認する。**	4-(iv)-b
		保険的対策	□ 対応済 □ 未対策 □ 対応不要	セッションIDを固定値にしない。	4-(v)
		保険的対策	□ 対応済 □ 未対策 □ 対応不要	セッションIDをCookieにセットする場合、有効期限の設定に注意する。	4-(vi)

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

■ ウェブアプリケーションのセキュリティ実装 チェックリスト（2/3）

No	脆弱性の種類		対策の性質	チェック	実施項目	解説
5	クロスサイト・スクリプティング	HTMLテキストの入力を許可しない場合の対策	**根本的解決**	□ 対応済 □ 未対策 □ 対応不要	**ウェブページに出力する全ての要素に対して、エスケープ処理を施す。**	5-(i)
			根本的解決	□ 対応済 □ 未対策 □ 対応不要	**URLを出力するときは、「http://」や「https://」で始まるURLのみを許可する。**	5-(ii)
			根本的解決	□ 対応済 □ 未対策 □ 対応不要	**<script>…</script> 要素の内容を動的に生成しない。**	5-(iii)
			根本的解決	□ 対応済 □ 未対策 □ 対応不要	**スタイルシートを任意のサイトから取り込めるようにしない。**	5-(iv)
			保険的対策	□ 対応済 □ 未対策 □ 対応不要	入力値の内容チェックを行う。	5-(v)
		HTMLテキストの入力を許可する場合の対策	**根本的解決**	□ 対応済 □ 未対策 □ 対応不要	**入力されたHTMLテキストから構文解析木を作成し、スクリプトを含まない必要な要素のみを抽出する。**	5-(vi)
			保険的対策	□ 対応済 □ 未対策 □ 対応不要	入力されたHTMLテキストから、スクリプトに該当する文字列を排除する。	5-(vii)
		全てのウェブアプリケーションに共通の対策	**根本的解決**	□ 対応済 □ 未対策 □ 対応不要	**HTTPレスポンスヘッダのContent-Typeフィールドに文字コード（charset）の指定を行う。**	5-(viii)
			保険的対策	□ 対応済 □ 未対策 □ 対応不要	Cookie情報の漏えい対策として、発行するCookieにHttpOnly属性を加え、TRACEメソッドを無効化する。	5-(ix)
			保険的対策	□ 対応済 □ 未対策 □ 対応不要	クロスサイト・スクリプティングの潜在的な脆弱性対策として有効なブラウザの機能を有効にするレスポンスヘッダを返す。	5-(x)
6	CSRF （クロスサイト・リクエスト・フォージェリ）		**根本的解決**	※ □ 対応済 □ 未対策 □ 対応不要	□ **処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行する。**	6-(i)-a
					□ **処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。**	6-(i)-b
					□ **Refererが正しいリンク元かを確認し、正しい場合のみ処理を実行する。**	6-(i)-c
			保険的対策	□ 対応済 □ 未対策 □ 対応不要	重要な操作を行った際に、その旨を登録済みのメールアドレスに自動送信する。	6-(ii)
7	HTTPヘッダ・インジェクション		**根本的解決**	※ □ 対応済 □ 未対策 □ 対応不要	□ **ヘッダの出力を直接行わず、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用APIを使用する。**	7-(i)-a
					□ **改行コードを適切に処理するヘッダ出力用APIを利用できない場合は、改行を許可しないよう、開発者自身で適切な処理を実装する。**	7-(i)-b
			保険的対策	□ 対応済 □ 未対策 □ 対応不要	外部からの入力の全てについて、改行コードを削除する。	7-(ii)

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

■ ウェブアプリケーションのセキュリティ実装 チェックリスト（3/3）

No	脆弱性の種類	対策の性質	チェック	実施項目	解説
8	メールヘッダ・インジェクション	**根本的解決**	※ □ 対応済 □ 未対策 □ 対応不要	□ **メールヘッダを固定値にして、外部からの入力はすべてメール本文に出力する。**	8-(i)-a
				□ **ウェブアプリケーションの実行環境や言語に用意されているメール送信用APIを使用する（8-(i) を採用できない場合）。**	8-(i)-b
		根本的解決	□ 対応済 □ 未対策 □ 対応不要	**HTMLで宛先を指定しない。**	8-(ii)
		保険的対策	□ 対応済 □ 未対策 □ 対応不要	外部からの入力の全てについて、改行コードを削除する。	8-(iii)
9	クリックジャッキング	**根本的解決**	※ □ 対応済 □ 未対策 □ 対応不要	□ **HTTPレスポンスヘッダに、X-Frame-Optionsヘッダフィールドを出力し、他ドメインのサイトからのframe要素やiframe要素による読み込みを制限する。**	9-(i)-a
				□ **処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。**	9-(i)-b
		保険的対策	□ 対応済 □ 未対策 □ 対応不要	重要な処理は、一連の操作をマウスのみで実行できないようにする。	9-(ii)
10	バッファオーバーフロー	**根本的解決**	※ □ 対応済 □ 未対策 □ 対応不要	□ **直接メモリにアクセスできない言語で記述する。**	10-(i)-a
				□ **直接メモリにアクセスできる言語で記述する部分を最小限にする。**	10-(i)-b
		根本的解決	□ 対応済 □ 未対策 □ 対応不要	**脆弱性が修正されたバージョンのライブラリを使用する。**	10-(ii)
11	アクセス制御や認可制御の欠落	**根本的解決**	□ 対応済 □ 未対策 □ 対応不要	**アクセス制御機能による防御措置が必要とされるウェブサイトには、パスワード等の秘密情報の入力を必要とする認証機能を設ける。**	11-(i)
		根本的解決	□ 対応済 □ 未対策 □ 対応不要	**認証機能に加えて認可制御の処理を実装し、ログイン中の利用者が他人になりすましてアクセスできないようにする。**	11-(ii)

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。