令和８年度 こうべコンポスト普及促進業務

１．委託業務名

令和８年度 こうべコンポスト普及促進業務

２．目的

本市では、土の中の微生物の力で生ごみを分解する「こうべキエーロ」をはじめとするコンポストの活用によるごみの減量に取り組んでいる。

本業務は、市民の資源循環やごみの減量に対する意識啓発を図り、各家庭での具体的な減量・資源化の取り組みにつなげるため、キエーロ並びに竹を活用した堆肥づくりを通じて、コンポスト活動の輪を広げ、継続的な活動につながる仕組みを構築しようとするものである。

本市がコンポストの先駆的な街となることを目指して、本業務に取り組んでいくものとする。

３．契約期間

2026（令和８）年４月１日（水曜）から 2027（令和９）年３月 31 日まで（水曜）

４．業務内容

以下の業務について、企画立案を行い、スケジュール管理により効率的に業務を遂行すること。なお、企画立案については市の方針に沿ったものとなるよう、事前に市と調整を行うこと。また、業務全体の進捗について、定期的に対面で報告を行うこと。

（１） スケジュール

本事業の遂行にあたっては、下記のスケジュールに従って各業務を実施すること。

（令和８年）

・４月１日～５月末　公式ウェブサイトの構築
　　コンポスト講習会用資料・パンフレットの完成

・６月１日～（随時）コンポスト講習会・コンポストＰＲイベント・堆肥活用イベントの実施

（２）情報発信業務

・市民のコンポスト活動の輪を広げていくための効果的な情報発信について具体的な方策を企画したうえで、情報発信業務を実施すること

・公式ウェブサイトを構築し、ロゴ作成、カテゴリー・ページ構成・タイトルなどをわかりやすく親しみやすいサイトとなるよう工夫すること。

※各種コンポスト（基材と容器）を紹介するページを必ず掲載することとし、基材については土と竹チップを使用したコンポストの方法について詳しく説明すること。

・コンポストに取り組む市民・団体を紹介するページ、わかりやすい（失敗しない）コン

ポストのやり方・工夫を紹介するページ、コンパクトでおしゃれなオリジナルコンポスト容器のつくり方、家の中で簡単にできる野菜・植物の栽培方法など専用サイトで発信するコンテンツを作成すること（年間６コンテンツ以上）。
動画なども活用し、公式ウェブサイト、SNS などで発信すること。

・SNS（インスタグラム、フェイスブック）を活用した効果的な（拡散されやすい）情報発信を行うこと（随時更新）
・公式 LINE の運用業務を行うこと（文案作成・発信（月１回以上）、問い合わせ対応、公式アカウント料の支払い（年額税込 198,000 円）。
・ホームページの制作にあたっては、下記「神戸市ホームページ作成事業者用ガイドライン」に準拠すること。
https://www.city.kobe.lg.jp/a57337/homepage/web_accessibility/guideline.html
・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。
・ウェブサイトおよびサーバの運用については、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」のチェック項目を満たしていることを具体的に示す提案を行うこと。
・当該 WEB サイトを運用するサーバ環境を用意すること。また、当該 WEB サイトで使用するドメインは市が管理するドメイン【smartkobe-portal.com】とするため、DNS 設定を行うために必要な情報を提出すること。
・本市が指定するアクセス解析ツール（Google アナリティクス）を用いて、アクセス解析を実施し、サイト利用者の動向を把握すること。サイトに埋め込むタグは、本市より提供する。
・アクセス解析のために利用する各プラットフォームのプライバシーポリシーを遵守・明記すること。（新たにプライバシーポリシーページを作成しない場合は、下記神戸市ホームページのプライバシーポリシーページを参照させる形でもよい。）
https://www.city.kobe.lg.jp/a57337/homepage/p_policy.html
・Google 社の定める規約に従い、Google アナリティクスを導入したウェブサイトの公開にあたり利用者に対して開示すべき事項（例：Cookie 利用による利用者情報の収集の有無）等を当該ウェブサイト上に明示すること。

（３）コンポスト講習会の開催

・市民のコンポスト活動の輪が広がっていくように、一年間を通して、コンポストを学び・体験できる場を提供すること。
・コンポストに関わる活動をする有機農業従事者（オーガニック推進協議会）、農園運営者、造園事業者、里山整備活動団体、企業・大学等（以下、「コンポスト推進団体」と

いう。）と連携し、コンポストが学べる講習会（年間 100 回）を開催すること。受講者についてはのべ 2,000 名以上を確保するよう努めること。講習会を実施するにあたり、推進団体と連携する場合の費用負担は 1 回あたり 5 万円を上限とすること。

※推進団体に支払う 1 回あたりの費用と 5 万円との差額は精算することとする。

・講習会において、コンポストに関する市民への説明はコンポスト推進団体が行うことができるようにサポートするとともに、講習会で使用する説明資料（紙芝居）、配布用パンフレット（堆肥づくりについてイラストを使ってわかりやすく説明するもの。版下のみ）及び講義用動画（堆肥づくりの動作など動きのあるものをわかりやすく説明するもの）を制作すること。

・講習会においては、キエーロに限らず、竹チップを使ったコンポストの方法など、さまざまなコンポストを紹介し、受講者のライフスタイルに沿った取り組み方法を選択できるようにわかりやすく説明をすること。

・講習会の受講者募集は神戸市公式イベントサイト「おでかけ KOBE」を活用することとし、市が「おでかけ KOBE」への情報入力ができるよう、市に対して講習会開催概要等の情報を提供すること。また、市が提供する受講者名簿を管理すること。

・受講者に対しては、本市が別途指定する各種コンポスト容器の中から希望するコンポスト容器（１人１個）を無償で提供するものとし、「プランター型容器」（プランターに波板等の半透明の蓋を取り付けたキエーロ用のもの。40L 以上。）、「不織布型容器」（蓋つき、持ち運びができる堆肥化容器。25L 以上。）については、受託事業者が手配をして、講習会会場への搬出入を行うものとする。

※「プランター型容器」および「不織布型容器」については、受託事業者が製作もしくは調達するものとし、それぞれの詳細仕様と見積金額（１個あたり税込み 5,000 円を上限とする）を提示し、本市の承認を受けることとする。提供する容器の費用は別途契約とする。

・受講者が上記以外のコンポスト容器の提供を希望する場合については、本市が契約をした店舗等において引き渡しを行うこととし、引き渡しの手続き・方法については、受託事業者が受講者に案内を行うこと。

・神戸市内の放置竹林対策活動と連携しコンポスト基材として竹チップを調達し、講習会会場において 14ℓ 入り袋および持ち帰り用簡易バッグを希望者に配布すること。竹チップおよび持ち帰り用簡易バッグの調達については、別途契約とする。

・受講者に定期的（講習会開催日・3 か月後・6 か月後）にアンケートを配布・回収した上、分析して報告すること。

（４）受講者（サポーター）の活動支援

受講者（サポーター）が継続的に活動を行い、さらに活動の輪を広げていくための仕組みを構築・運用すること。

・受講者の継続的な参加を促す仕組みづくりをすること

・受講者から新規受講者への紹介が促進される仕組みづくりをすること

（５）イベント・交流会の開催

上記コンポスト講習会（100 回）において、堆肥活用イベントおよび、コンポスト PR イベントを併せて実施すること。また、コンポスト推進団体を対象とした交流会を実施すること。

◎堆肥活用イベント

・コンポスト推進団体等と協力し、家庭でのコンポストの取組みが継続的に行われる動機づけができる企画とすること。

・家庭から持ち寄り、コンポスト推進団体が運営する農園等で堆肥化させたものを活用して、畑や花壇などの土と混ぜて使用し、野菜や花を栽培する内容のものとする。

・コンポスト推進団体が運営する農園等にコンポスト容器、栽培区画を設置する必要がある場合は、受託事業者が設置するものとする。（設置に関する費用は別途契約）

◎コンポスト PR イベント

・コンポスト推進団体等が主催する集客性の高い園芸イベントなどにおいて、コンポストについて簡単にわかりやすく説明するＰＲブースを設け、コンポストに関する質問・相談、コンポスト講習会の案内等を行う。

◎交流会の開催

コンポスト推進団体を対象とした交流会を開催すること。

コンポストの専門家などを招いて、講演会、トークセッションなどを企画すること。

※交流会では容器の配布は行わない。

（６）出前トークの実施（20 回予定）

◎出前トーク講師派遣　※市職員により実施するため委託業務外（参考掲載）

◎基材搬入作業

出前トーク受講者のうち、希望者に対しては、上記４（３）に記載のある「不織布型容器」（蓋つき、持ち運びができる堆肥化容器。25L 以上のもの。）および竹チップ 14ℓ 入り袋および持ち帰り用簡易バッグを出前トーク会場にて配布するため、受託事業者が手配をして、講習会会場への搬入を行うものとする。提供する容器および竹チップおよび簡易バックの調達費用は別途契約とする。

※実施回数が 20 回に満たない場合は精算する。

（７）コンポストを活用した環境学習の支援（20 校予定）

小学校において、児童がコンポストによる土づくり、野菜栽培を通じて、ごみの減量や資源循環を学ぶ環境学習の支援を行う。

市が指定する市内小学校 20 校（継続 10 校、新規 10 校）において、オーガニック推進協議会、有機農業従事者と連携し、基材（容器、土、竹チップ）・苗の提供、児童向け説明会の実施及びコンポストによる残渣処理及び野菜栽培の現地指導を実施すること。また必要なマニュアル、テキスト等を制作すること。

（業務内容）

各小学校で履行する事項

◎各学校との打合せ（20 校）※市職員により実施するため委託業務外（参考掲載）

・令和 7 年度に作成する教員向けマニュアルに基づき、取り組み事例等の紹介

・年間スケジュール、サポート体制（出前授業、基材の提供、有機農業従事者の派遣）を説明

・スケジュール、コンポスト容器の設置場所、栽培する野菜の種類、収穫した野菜の利用方法などの調整

◎コンポスト出前授業用テキストの作成

・神戸市のごみの現状、ごみの減量、コンポストの特徴、微生物の働き、有機栽培について、わかりやすいテキスト（パワーポイント）を制作すること。

※テキストの印刷費については別途契約とする。

◎コンポスト出前授業（45 分）※市職員により実施するため委託業務外（参考掲載）

◎基材搬入作業（新規校のみ。10 校予定）

・プランター容器（蓋つき）15 個、土（40ℓ）15 袋（有機培養土 10、グリーンリーフ堆肥 5）の搬入及び容器への土入れ作業

※農村地区の小学校では、土に替えて竹チップを使用する可能性あり。

※基材（容器、土、竹チップ）の調達については別途契約とする。

※学校内に調理施設が設置されていない学校については、調理くずを調達し、学校へ届ける場合がある（週 1 回程度）。別途契約とする。

◎児童へのコンポスト実践レクチャー（45 分）※出前授業と同時に実施する場合は不要

・児童向けテキストを制作し、テキストに基づき学校での生ごみ投入・管理方法を指導。テキストでは「生ごみの入れ方・混ぜ方、土のふたの仕方、適量の水分、微生物の働き等」について分かりやすく説明すること。

※テキストの印刷費については別途契約とする。

◎土の入れ替え作業

・学校が実施するコンポストの土（プランター）と学習園の土（畑）の入れ替え作業をサポートする（学校から依頼がある場合に限る）。

◎児童への野菜栽培指導

・オーガニック推進協議会と連携し、野菜苗の搬入と児童が行う野菜苗植えの指導を行う。

※野菜苗の調達については別途契約とする。

◎野菜生育の確認

・必要に応じて、野菜栽培後の生育状況を確認し、改善が必要な場合は報告を行う。

◎児童への野菜収穫レクチャー

・オーガニック推進協議会と連携し、野菜収穫の指導を行う。

◎学校毎の取り組みリポート（まとめ）作成

・各小学校で履行した取組みの日時、内容、参加人数

・教諭や児童の意見や感想（工夫した点、苦労したことなど）

・その他必要と思われることを記載

※本リポートは、本市が広報等に転用することがあるものとする。

※実施校が 20 校に満たない場合は精算する。

5．個人情報保護および情報セキュリティ遵守について

（1）個人情報保護

この業務を実施するにあたり、個人情報の保護の重要性を認識し、個人情報を取り扱う際には、個人の権利利益を侵害してはならない。

（2）情報セキュリティ遵守について

この業務を実施するにあたり、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

6．作業形態

（1）業務責任者

・本市指示のもとに、担当者に対し指揮命令権を有し、業務全体を総括し責任を負う業務責任者を配置すること。

・業務責任者は業務処理状況について常に把握し、適切に管理を行うこと。

・本市からの要請があれば、業務責任者は業務内容について定量的な数値も含めて報告すること。

（2）担当者

・業務責任者指示のもとに、業務を行う担当者を配置すること。

7．成果物

業務報告書を紙媒体及び電子データで提出すること。電子データの場合のファイル形式は、事前に本市の了解を得ること。

8．その他

（1）費用分担

受託者が業務を遂行するにあたり必要となる経費は、契約金額に含まれるものとし、市は、契約金額以外の費用を負担しない。

（2）保険加入

必要に応じてイベント保険に加入すること。

（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。譲渡費用には成果物に係る印刷データの費用を含むこと。なお、データ等はイラストレーター等で納品すること。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。

④ ・必要性や不代替性その他の理由により第三者の利用許諾の元に使用する著作物がある場合には、見積り及び企画提案時に具体的な使用目的や使用方法等の詳細を明らかにすること。なお、申し出があった場合でも、第三者の著作権の使用を許諾するかどうかは本市の裁量による。

（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。

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	
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。

■ 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。