神戸市水道局キッズページ制作業務
委託仕様書

1．委託業務名

神戸市水道局キッズページ制作業務

2．業務の目的

（1）背景

神戸市水道局では、継続的な経営改善に努めながら、安全で良質な水を安定的に届けることを目的に事業を進めているが、節水型社会の進展や人口減少が進む中、今後は水需要や給水収益の減少がさらに進み事業環境が厳しくなっていくことが予想される。そのような中、市民の財産である神戸の水道を守り続けていくためには、市民の水道事業への関心を高め、課題を共有していくことが不可欠である。一方で、これまで水道水の安定供給に努めてきた結果、断水を経験することがほとんどない現在では、水道は蛇口から出ることが当たり前となっており、市民の関心は決して高くない。

（2）目的

子どもの頃から水道の知識を身につけてもらうとともに、大人にとっても興味深いコンテンツを用意し、広く水道に親しんでもらうことを目的とする。

学校で水道について学習する小学校4年生を主な対象として、水源から蛇口までの神戸の水道の仕組みや、水道水の安全性、大切な水を育む自然の仕組み、災害時の水利用などについて、身近に感じてもらいながら分かりやすく解説する。また、イベント情報や既に実施したイベントの報告等、時期に応じたコンテンツを職員によって更新可能なものとし、一度訪問して終わりではなく、水道局のイベントへの参加や水の科学博物館への来館などのアクションにつなげる。

3．契約金額・及び期間

（1）委託予定金額

上限4,320,000円（消費税及び地方消費税を含む）

（2）委託期間

契約締結の日から、平成30年3月31日まで

4. 業務概要

（1）WEB サイトの企画・設計

① 業務内容

(ア) 企画会議及び編集会議の運営・議事録の作成

(イ) 業務実施内容及び作業工程を示した業務計画書の作成

② 留意事項

(ア) WEB サイトの全体構成・デザイン等を議論するため、神戸市水道局職員等との企画会議を適宜開催すること。会議後は、速やかに議事録を作成し、提出すること。

(イ) WEB サイトへの具体的な掲載内容等を議論するため、編集会議を適宜開催すること。

（2）WEB サイト制作

① 業務内容

(ア) サイトの全体構成及びデザインの制作

(イ) 水道事業学習コンテンツの制作

(ウ) マルチデバイスへの対応（レスポンシブ Web デザインの導入等）

(エ) 一般的に利用が可能なオーサリングツールの導入（CMS の導入等）

(オ) SNS との連動

(カ) ゲーム性のあるコンテンツの作成

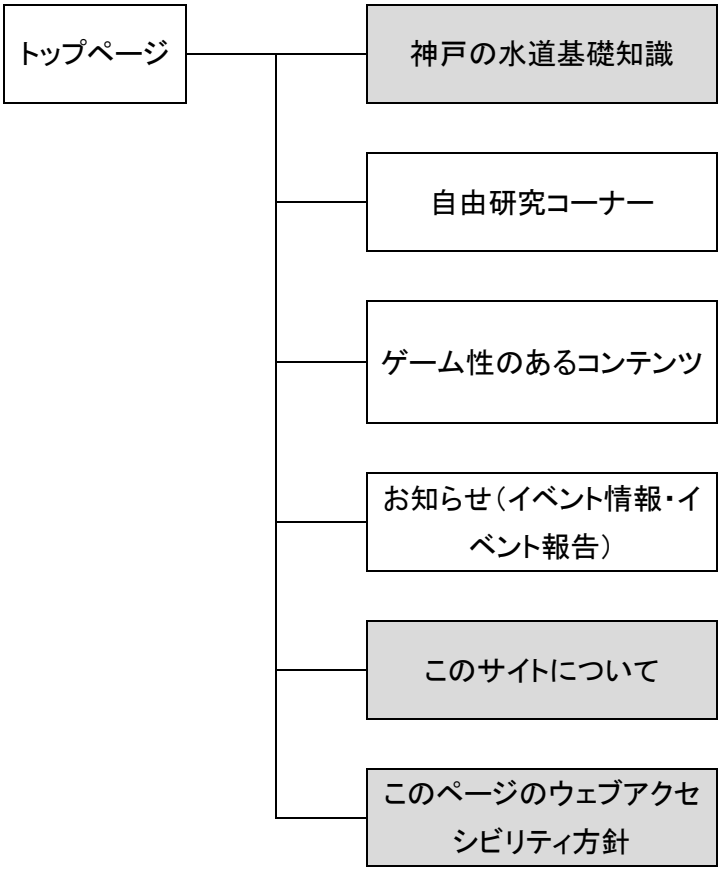
(キ) SEO 対策

(ク) 効果測定方法の確保

② 留意事項

(ア) 本業務の目的に沿ったサイトの全体構成を検討・提案し制作すること。トップページ及びサイト全体のデザインについては、子どもだけでなく大人が見ても興味を持つような独創的かつ魅力的なものとすること。

※本サイトのサイトマップイメージ（案）



（※１）グレー部分についてはホームページ開設後、基本的に更新の予定無し。

（※２）その他はオーサリングツールを使用した、職員による更新を想定。

また、上記以外のより良い独自企画や今後の展開について、良い提案がある場合には、提案可能とする。

(イ) 小学4年生を主な対象とし、好奇心を誘い、確実に水道の仕組みや水道局の仕事内容等について学習できるコンテンツを制作すること。コンテンツ内容については、現在のキッズページ及びパンフレット『神戸の水道』、小学校社会科副読本『わたしたちの神戸 3・4年』等を参考にし、水道局職員との協議により決定していくこと。

(ウ) PC 及びスマートフォンなど、マルチデバイスでの利用を考慮すること。ただし、デバイスごとに別のサイトを制作するのではなく、同ドメイン・同ページを使用し、画面サイズによって最適化される構造とすること。

(エ) 時期に応じて自由研究の題材提供やイベント情報等を掲載することを想定し、専門知識を持たない職員でも容易にコンテンツの作成や修正ができ、最新の情報や映像、及びリンク先を更新・公開できるページを設けること。また、簡単にイベントに参加できるようにするための申し込みフォームを設置するなど、イベント参加につなげる工夫をすること。

(オ) 保護者間等の情報共有を想定し、SNS 共有ボタンを配すなど Facebook や Twitter、LINE といった SNS との連動を図ること。また、OGP を設定すること。なお、専用の Facebook ページ等を新しく作成する必要はない。

(カ) 水道事業にまつわる、ゲーム性のあるコンテンツ、またはゲーミフィケーション（日常の様々な要素をゲームの形にする）を取り入れたコンテンツを水道局職員と協議して作成すること。

(キ) 必要とされる場面を想定して SEO 対策を行う。また、更新可能コンテンツにおいても職員により SEO キーワードを入力できるようにすること。

(ク) アクセス解析（ページビュー、セッション、直帰率、検索ワード等）のデータを職員により取得できるようにすること。その他、提案に応じて効果測定の方法を考案し、委託期間終了後も継続的に測定できるようにすること。

(ケ) コンテンツ制作に係る文章や写真、イラスト等は原則として受託者により用意する。ただし、適宜神戸市水道局より資料や撮影の機会等を提供するものとする。

(コ) ウェブアクセシビリティを遵守すること。JIS X 8341-3:2016適合レベル「AA」の達成及び「神戸市ホームページ作成事業者用ガイドライン」の遵守「神戸市ホームページ作成ガイドライン」に沿って、ユーザビリティを考慮し制作すること。

（http://www.city.kobe.lg.jp/other/arukikata/web_accessibility/guideline.html）

（３）動作環境の構築及び保守

① 業務内容

(ア) レンタルサーバ、ハードウェア、ソフトウェア等の調達

(イ) 新規ドメインの取得

(ウ) SSL 証明書の取得

(エ) セキュリティ対応

(オ) システムトラブル対応

② 留意事項

(ア) 神戸市が所有する情報資産の機密性、完全性、可用性を確保した運用が可能なシステムとすること。

(イ) ドメイン名は､本事業の専用 WEB サイトであることをイメージできるものとすること。また、ｊｐドメインなど信頼性の高いドメインを取得すること。

(ウ) 全ページ常時 SSL 化し通信データを暗号化すること。また SSL/TLS サーバー証明書の認証レベルは OV 認証とすること。

(エ) 安全なプログラミングを行い、公開前に十分なセキュリティテストを実施したうえで、別添のホームページサーバ等確認チェックリストと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が全て「はい」の状態を維持すること。

(オ) システム、ハード、ネットワーク環境全般において、脆弱性が報告されていないかを常に確認し、アップデート等のメンテナンスが必要な場合は、速やかに対応すること。

(カ) 情報処理推進機構（IPA)や JPCERT コーディネーションセンターなどから随時セキュリティ問題にかかる情報を入手するとともに、当該 WEB サイトに関わる場合は直ちに神戸市に報告の上、当該情報に基づく対策を講じることが必要か否かを神戸市と協議すること。

(キ) レンタルサーバにて用意されるすべてのソフトウェアについて最新バージョンが使われていることを確認すること。また CMS に関するプラグインを含めたソフトウェアについても、常に最新バージョンを適用すること。何らかのリスクにより最新化対策を講じることが出来なかったものに関しては、その理由、代替措置及び影響について神戸市に直ちに報告すること。

(ク) 本業務の遂行において、受託者における情報セキュリティ対策の履行が不十分である可能性を神戸市が認める場合には、神戸市の求めに応じ協議を行い、合意した対策をとること。

(ケ) OS、データベースや操作状況等に関するログを取得できるようにすること。

(コ) 1日1回、作成したＷｅｂサイトコンテンツファイル等関連データについてバックアップを取得し、常に１週間分のデータを保持すること。

(サ) 公開を一時的に停止する場合に備え、「只今、メンテナンス中」のアナウンスページを事前に準備すること。

(シ) 改ざん被害等発生時の緊急時対応手順書を作成すること。

(ス) 不具合並びに不正アクセスの症状が見受けられた際には、以下の手順に基づき対応すること。

<改ざんの有無の検査を実施>

① 状況の確認

不具合並びに不正アクセスの症状が見受けられた際、もしくは、関係各署より通報が入った際には、優先的に下記の不正アクセスについての確認、調査をおこない、契約後に策定する「緊急連絡体制」に基づき、速やかに対応についての協議を行うこと。

【確認内容】

・公開されているサイト情報の内容
・サーバ内の不正なスクリプトの有無（HTML ファイル、JavaScript ファイル、PHP ファイル、CSS ファイル、Apache などの.htaccess ファイル、ディレクトリの全て）の確認
・サーバアクセスログ
・サーバへの不正アクセスの有無（サーバ会社への確認）
・担当者コンピュータの確認

② サーバ上のデータ並びにシステムに不具合や改ざんが見受けられない場合

・サーバ上のデータ並びにシステムに不具合や改ざんが見受けられない際には、優先的に調査を行い症状の起因分析等の状況確認をし、書面にて情報共有をおこなうこと。

③ 改ざんが見受けられた場合

・ウェブサイトが明らかに改ざんされたと認識した場合、被害の拡大を防ぐために、ウェブサイトを一旦公開停止した上で、「只今、メンテナンス中」のページに表示を切り替え、原因の究明と対策後に正常なバックアップからの復元作業を実施して再公開すること。

（4）WEB サイトのマニュアル作成

① 業務内容

オーサリングツールを使用した、職員による更新を想定したページ（サイトマップイメージの「※2」部分）の管理・運用マニュアルの作成

② 留意事項

本サイトを継続的に活用することを踏まえ、専門的知識を持たない本市職員が情報更新できるよう、分かりやすい内容のマニュアルを制作し、紙媒体で 1 部と修正可能な電子データで提出すること。

5. 納期及び成果物

（1）納期

サイトの公開 … 平成30年1月下旬予定（別途協議による）

その他保守運営等　… 平成30年3月末日

（2）確認

神戸市は、納期までに納品を受けた成果物について確認を行う。なお、受託者はコンテンツの内容、プログラムの動作等について必要なテストを実施し、成果物の確実性に万全を期すこと。また神戸市からの修正等の指示があった場合は速やかに対応すること。

（3）成果物

① 開発ドキュメント（変更、追加、削除その他の履歴を記録すること。）

(ア) ホームページ設計書 サイト構成図

基本仕様書（データ構造、画面遷移等）

ファイル一覧（ディレクトリマップ）

その他システム設計に関連するドキュメント等

(イ) テスト結果報告書 各種テスト内容一覧（テスト方法、テストデータ、判定基準等）

(ウ) コンテンツ 開発したコンテンツ

(エ) ドメイン 新規取得したドメイン

(オ) SSL/TLS サーバー証明書

(カ) マニュアル WEB サイトの管理・更新マニュアル一式

(キ) 緊急時対応手順書

(ク) 議事録 打合せにかかる議事録一式

② 納品場所

神戸市水道局 経営企画部計画調整課

③ 検収方法

(ア) 神戸市は、上記①に掲げる成果物について、契約書、業務仕様書等に基づき WEB サイトの稼働及びドキュメント等について必要な検査を行う。

(イ) 上記（ア）において指摘があった場合には、受託者は神戸市の指示に従い適正に対応するとともに、再度確認を得なければならない。

6. その他の事項

（1）実施体制

① 本仕様書に記載した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 本 WEB サイトは24時間365日運用であり、緊急を要する業務については、委託者から連絡の有無を問わず、受託者は誠意と責任を持って可能な限り迅速に処置を行うよう努めること。また、緊急を要する場合について、平日以外や営業時間外についても連絡が取れるような体制を持つこと。

（2）開発環境

① 設計・開発等については、受託者において開発環境を用意すること。

② 本業務を実施するうえで必要となる機材については、本件受託者において準備することとし、その所要経費は契約金額に含まれるものとする。

（3）瑕疵担保責任

① 成果物の納品日から起算して1年以内に障害が発生した場合、受託者は速やかに原因究明に協力しなければならない。

② 上記①により対応した受託者は、発生した事態の具体的内容、原因、対処措置を内容とする報告書を作成のうえ、神戸市水道局が指定する期日までに提出すること。

③ 上記②の原因を修正するため、必要なプログラム、データ等を納入済みのコンテンツ、開発ドキュメント等へ適用するとともに、正常な稼働が確認できるまで必要な調整を行うこと。

④ 上記①～③に係る経費については、受託者が負担するものとする。

（4）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。

（5）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。）は発注者である神戸市に無償で譲渡するものとする。

② 受託者は、神戸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。

（6）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。

（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神戸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）業務の引継ぎに関する事項

本業務の契約期間の満了、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、業務引継ぎに伴うシステム移行等に必要となる構成要素（ドメイン、SSL 証明書、ページやコンテンツ等）を円滑に提供できるようにすること。なお、提供に係る費用は保守運営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。

(10) 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。

※「安全なウェブサイトの作り方 改訂第7版」を参照しながらチェックを実施してください。

■ 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。

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。