（資料３）

福岡市総合図書館ホームページ
リニューアル業務委託
仕様書

令和7年4月

福岡市教育委員会総合図書館運営課

1　委託件名

福岡市総合図書館ホームページリニューアル業務委託

2　履行期間

契約締結日から令和8年 3 月 31 日まで

3　履行場所

福岡市教育委員会総合図書館運営課　外

4　事業の目的

福岡市総合図書館ホームページ（以下、「本サイト」という。）は、2010 年度に構築され、以降 2013 年度、2016 年度、2019 年度にレイアウト変更や、カレンダーの追加などの改修を行いながら使用しているが、基本的な構成は変わらず、構築後約 15 年が経過している。

現行サイトは閲覧の多数を占めるスマートフォンに対応しておらず、行政機関のホームページに求められるウェブアクセシビリティの規格「JIS X 8341-3:2016 の適合レベル AA」に準拠していない。

福岡市総合図書館ホームページリニューアル業務委託（以下、「本業務」という。）では、こうした課題を解決し、利用者が見やすく使いやすいサイトの実現を目指すとともに、現在別サイトで運用している福岡市総合図書館映像ホール・シネラのホームページコンテンツを本サイトに移行するもの。

5　現状の主な課題

福岡市（以下、「本市」という。）が考える現状の主な課題は以下のとおり。

- スマートフォン用のページの切り替えがなく、パソコンでの閲覧を前提としたデザインになっているため、スマートフォンで閲覧しづらい。
- 情報が多く、デザインに統一性がないことから、見にくく分かりづらいトップページになっている。
- コンテンツ数、ページ数ともに多く、ページ階層も複雑なため、必要な情報にたどり着きにくい。
- 職員が修正できないページがある。
- やさしい日本語に対応していない。
- 英・韓・中（簡体・繁体）に対応すべきと考えているところ、現状対応している外国語が英語のみとなっている。
- 総合図書館本館の3部門（図書・文書・映像）及び 11 の分館の情報の区別がしづらい。

6　委託業務の内容

受注者は、前述の 4 と5に記載の内容を踏まえて、本市と十分に協議しながら、以下の業務を行うこと。

(1) 本業務全体の実施計画及び管理

受注者は、本業務における具体的な体制、スケジュール等を記載した実施計画書を作成すること。

また、本業務の実施にあたっては、本市とミーティング（Web 会議を想定）を必要に応じて適宜開催し、進捗や課題等について管理・共有すること。ミーティングの開催頻度や方法等の詳細については、本市と協議のうえ決定するものとする。

(2) 現状分析及びリニューアルサイト全体の企画・設計

①現状分析

「5　現状の主な課題」を踏まえたうえで、本サイト（https://toshokan.city.fukuoka.lg.jp/）のデザインや各ページの内容、運用方法等についての現状分析を行い、問題点等を洗い出し、移行ページ等について整理すること。

また、外部サイトとして稼働している福岡市総合図書館映像ホール・シネラのサイト（http://www.cinela.com/）については、福岡市総合図書館ホームページと同一ドメインにて稼働させるよう移行することから、併せて現状分析し、移行するページ等について整理すること。

②リニューアルサイト全体の企画・設計

現状分析の結果及び以下のリニューアル方針を踏まえたうえで、リニューアルサイト全体の企画・設計を行うこと。

＜リニューアル方針＞

ア　主にスマートフォンからのアクセスを想定したユーザーインターフェースとすること。

イ　ユーザーが直観的に必要な情報に辿り着けるよう、ユーザー目線かつシンプルな導線を設計すること。

ウ　検索機能の実装により、ユーザーの目的や検索ワードがあいまいな場合でも、必要な情報に辿り着けるようにすること。

エ　デザインや配色、文字のフォント・大きさなどは、「デジタル庁デザインシステム」を参考にしたうえで、誰にとっても見やすいものとすること。

【参考 URL】https://design.digital.go.jp/

オ　不正アクセス、データの改ざん、コンピュータウィルスやワームなどの不正プログラムの侵入を防止するため、情報セキュリティ対策が施された信頼性の高いサイトにすること。

カ　原則、職員がどのページも修正できるようにすること。

キ　HTML や CSS 等の専門知識が無い職員であっても、ページの作成・更新が容易にできるよう、分かりやすくシンプルな運用・管理とすること。

ク　複数の職員がページの作成・更新をすることを踏まえたうえで、サイト全体のトーン＆マ

ナー、品質が長期的に維持できる運用・管理とすること。

ケ　一般的なブラウザ（Edge 最新版、Firefox 最新版、Chrome 最新版、Safari 最新版）で閲覧可能なものとすること。

（3）システム環境の構築

システム環境の構築にあたっては、以下の事項及び別紙1「非機能要件一覧」の内容を満たすこと。

①基本要件

- システム利用時間は、原則として 24 時間 365 日とする。ただし、保守等の予定された停止に関してはこの限りでない。
- サイトの各ページの表示速度は 3 秒以内を目標とすること。
- ブラウザのみで利用できるものとし、専用ソフトウェアのインストールが不要なシステムとすること。
- 本市情報セキュリティポリシー等の規定を遵守し、必要な対策を講じること。

②サーバ及びネットワーク環境

- 本サイトの構築に必要なハードウェア、ソフトウェア、ネットワーク機器、各種サービス（レンタルサーバやクラウドサービス、インターネットプロバイダなどのサービスを含む）を受注者側にて用意すること。
- データセンターについては、国内のサービスを利用すること。

＜データセンター要件＞

データセンターサービスを提供する事業者にて、情報セキュリティマネジメントシステム（ISMS）適合性評価制度に基づく ISMS 認証又はそれと同等の認証を取得された環境を利用すること。

また、データセンター内にて、当該業務を行う場所及び情報を保管する施設その他情報を取り扱う場所において、入退室の規制及び防犯対策その他必要な情報セキュリティ対策を講じること。

③システム（CMS）

- 機能拡張性及び保守性の高いシステムとすること。
- システム稼働後 5 年間はサポートが行われること。
- システムの構築にあたり必要となる開発ソフトウェア等は受注者にて用意すること。

④セキュリティ対策

- 通信の暗号化（常時 SSL 化）を行うこと。暗号化に必要なサーバ証明書に関しても受注者側が準備すること。利用期間は 5 年間とする。
- サーバログ及びアクセスログを常時取得し、障害対応等の必要に応じて解析ができるようにすること。
- ホームページの改ざんを検知する機能や WAF 等のセキュリティ対策を実施すること。
- 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」をもとに、必要なセキュリ

ティ対策を講じること。チェックリストの結果については市に提出するものとし、「未対策／対応不要」とした項目については、その理由を示すこと。

（4）リニューアルサイトの構築

リニューアルサイト全体の企画・設計に基づき、リニューアルサイトを構築すること。構築にあたっては、以下の事項を満たすこと。

①基本要件

- 再構築後も同じ URL を使用すること。
- CMS の運用・管理にあたり、IDごとにアクセス制限（権限管理）を行い、権限外のコンテンツの更新が出来ないように制御すること。また、ID の一括登録・初期設定は受注者が行うこと。

＜ID 数の想定＞

ページ作成者 ID：約 20、 サイト管理者 ID：1

- 管理画面には各職員の端末から ID 及びパスワード認証によりログインできること。合わせて二段階認証等の外部からの不正ログインを防止する対策を実施すること。
- CMS（付随するソフトウェア等含む）は、ID 数や端末台数、ページ数等の増加によって、ライセンス料が変動しないこと。
- 総務省の「みんなの公共サイト運用ガイドライン」に準拠した本サイトのウェブアクセシビリティ方針を作成し、公開すること。ウェブアクセシビリティ方針には、JIS 規格「JIS X 8341-3:2016」の適合レベルを明記すること。

【参考 URL】

https://www.soumu.go.jp/main_sosiki/joho_tsusin/b_free/guideline.html

- 検索エンジンで上位に表示されるよう、SEO 対策を講じること。
- 汎用的なアクセス解析ツールを用いて本サイトのアクセス解析ができること。
- 図書館利用に関する基本的な情報については、やさしい日本語及び以下4言語に対応した市が提供する文または翻訳文をページに掲載すること。（ページ想定は各言語1ページ程度）

【対応言語】 英語、韓国語、中国語（簡体字・繁体字）

②デザイン・動線

- 原則、サイト全体で統一したデザインとすること。
- ユーザーからのアクセスは、主にスマートフォンからを想定しているが、パソコンやタブレット等、今後新しく出現するものも含めて、異なるデバイスからアクセスがあった場合でも、最適な状態で表示・操作ができるように設計すること。
- トップページデザイン及びナビゲーションメニューは、ユーザーの利便性を最優先とすること。なお、臨時休館等の緊急・重要情報については、職員が操作できるものとし、確実にユーザーに届くよう、目立つデザインや配置で表示できるようにすること。
- ページのカテゴリ分類や階層構造は、ユーザーが必要な情報にたどり着きやすいよう設

定すること。また、目的とするページに、原則 1～3 クリックで辿り着くことを目標とすること。

③コンテンツ

移行対象ページ

- （2）①で整理した移行対象ページについて、リニューアル後のカテゴリ分類や階層構造に合うよう必要な修正を加えたうえで、移行作業を行うこと。
- 移行対象ページについては本市と協議の上決定すること。
- HTML ファイルや添付ファイル等のデータについては、受注者が本サイトの公開データから取得作業を行うこと。
- 移行後もページの編集や公開・削除作業が行える状態とすること。
- 移行に伴い、ページデザインが崩れる等の問題が生じた場合は、受注者側で修正を行うこと。

④ページの作成

- HTML や CSS 等の専門知識が無い職員であっても、ページの作成・更新が容易にできるよう、シンプルで分かりやすい管理画面とすること。
- 複数の職員がページの作成・更新をしても、サイト全体のトーン＆マナーが揃うよう、用途に応じたページテンプレートを用意すること。
- アップロードできる画像・ファイルの形式（jpeg、png、pdf、docx 等）及び容量を制限できること。容量を超える場合、画像の自動リサイズができること。難しい場合は警告表示を表示させること。
- ページごとに OGP 画像を設定できること。
- 作成中のページについて、掲載画面がイメージできるようプレビュー機能を設けること。また、できる限り画面表示に近い状態でページを印刷できること。
- ページ公開前に、機械的なアクセシビリティチェック（画像の代替テキスト、機種依存文字、全角英数字の有無等）ができること。

⑤メールマガジン、メールレファレンス

- メールマガジンとメールレファレンスについては、図書館システムの機能を利用するため、不要とする。（これにより、リニューアル後のサイトには個人情報は含まれない）

⑥管理機能

- ログインする ID の権限に応じた管理画面が表示されること。
- サイト管理者を除き、ページ一覧には編集する権限のあるページのみ表示されること。
- トップページやヘッダー・フッター等のサイト共通部分については、サイト管理者のみ編集できる権限とすること。
- 管理画面内で CMS 操作マニュアルを表示できること。

（5）サイトの移行及び公開

- 現行サイトからリニューアルサイトへの移行期間については、本市と協議のうえ決定すること。

なお、データ移行や設定等、移行に伴う作業は、原則受注者が実施すること。

- 移行対象ページが漏れなく移行されているか確認すること。
- 移行対象ページについて、移行期間中に更新されたページの差分反映については、本市と協議のうえ決定すること。
- リニューアルサイトの公開前に、デモサイトを構築し、表示や動作を確認すること。また、本市も確認できる状態とすること。
- 公開にあたっては、サービスの停止期間ができる限り短くなるよう、図書館側と協議の上、対応を決定すること。

（6）運用・保守管理

①リニューアルサイトの運営

- リニューアルサイトの安定稼働のため、（3）②③で用意したハードウェア、ソフトウェア、ネットワーク機器、CMS 等について、定期保守やバージョンアップ反映（大幅な改修や工数が発生するものは除く）等の必要な対応を行うこと。
- アクセス数の集中が見込まれる場合は、本市と協議の上、別途対応方法を提示すること。

＜参考＞

過去 1 年間の平均アクセス数　9,479 件／日

②操作支援

- 操作マニュアルの作成

ページの作成・承認に関する分かりやすい操作マニュアルを作成すること。画面イメージを表示する、分かりやすい表現で記載する等により、専門的知識を持たない職員であっても、ページの作成や更新、公開に関する一連の流れが理解できるようにすること。

- 職員からの操作方法等に関する問い合わせについて、対応できる体制の確保及び窓口を設置すること。

③アクセスログの取得

- リニューアルサイト公開後、各ページのアクセス件数等を取得すること。

④バックアップの実施

- 定期的にデータのバックアップを実施すること。

⑤障害対応

- 障害が発生した場合、本市と密に連携し、早期にシステムを復旧すること。
- 同一事象及び類似事象の発生を防止するため、原因究明や再発防止策の検討・実施等を行うこと。

⑥サービスの中断に関する項目

- 構築したシステムの他社への引継ぎについては、最大限の努力を行うこととする。

7　サイトの公開時期

令和8年3月上旬の公開を予定

8　納品物

下記の項目について、各 1 部納品すること。

項目	提出方法	補足
①本件 Web サイト一式	データ	本要件に準じた Web サイトの公開をもって納品とする。
②実施計画書	データ	体制図、全体スケジュール等を記載
③リニューアルサイト設計書	データ	
④システム・ネットワーク構成図	データ	
⑤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	データ	チェック結果を記載
⑥ウェブアクセシビリティ方針	データ	ページを作成して公開することをもって納品とする
⑦移行対象ページ一覧	データ	
⑧操作マニュアル	紙、データ	

9　納品物の帰属等

（1）　納品物の著作権その他関係情報の一切の権利は発注者に帰属するものとする。

（2）　受注者は、納品物に係る著作者人格権を行使しないものとする。また、受注者は、本委託における納品物の制作に関与した者について、著作権を主張させず、著作者人格権についても行使させないことを約するものとする。

（3）　発注者は納品物の一部について差替え、削除及び追加の必要が生じた場合には、受注者以外の事業者に委託、または発注者自身でその改変を行うことができるものとする。

（4）　発注者は、納品物を他の広報物に使用できるものとする。また、発注者が認める場合に、受注者は第三者による映像等の使用を了承するものとし、使用料がかからないこととする。

（5）　上記（4）の場合において、受注者以外の著作者の許諾が必要な場合には、受注者がその手続きを行うものとする。

（6）　受注者は、納品物について、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、納品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注者が負うものとする。

（7）　著作権・肖像権処理等、権利関係に関する紛争が生じた場合は、受注者の責任において対応し、発注者は責任を負わないものとする。

10 その他留意事項

（1） 委託内容等については、提案競技時点におけるものであり、契約締結の際、受注者と協議のうえ変更を加えることがある。

（2） 本仕様書に定めのない事項及び疑義が生じた場合は、発注者と協議し、指示を受けること。

（3） 業務の再委託に際しては発注者と協議を行うこと。

（4） 別紙3「個人情報・情報資産取扱い特記事項」を遵守すること。

別紙１

非機能要件一覧

要件	対象	内容
可用性	稼働率	・年間のシステム稼働率は99%を目標とすること。
	冗長化	・サーバ障害等によるデータ消去・破壊のリスクを低減させるため、サーバ、記憶装置等を冗長化する機能を設けること。 ・一部のハードウェアが故障しても、縮退運転が可能なハードウェア構成を設けること。
	RPO （目標復旧地点）	・平常時、営業停止を伴う障害が発生した際には、障害発生地点（日次バックアップ＋アーカイブからの復旧）までのデータ復旧を目的とすること。
性能要件	オンライン レスポンスタイム	・オンラインレスポンスタイムは、3秒以内を目標とすること。なお、業務に支障のない状態を確保できるよう構築すること。
セキュリティ要件	セキュリティポリシー等	・本システムの構築・運用に際しては、本市の「福岡市情報セキュリティ管理規程」及び「福岡市情報セキュリティ対策基準」といった情報関連規程等を遵守し、万全の対策を講じること。
	機密性の確保	・庁内外からの不正な接続及び侵入、行政情報資産の漏えい、改ざん、消去、破壊、不正利用等を防止するための対策を講じること。
	ウイルス対策	アンチウィルスソフトウェアを活用する等により、以下の不正プログラム対策を講じること。 ・定時スキャン設定のみならず、個別ファイルをアクセスする都度スキャンが可能な機能を設けること。 ・データ送受信時にウィルスチェックが可能な機能を有すること。 ・最新のエンジン及びパターンファイルの自動更新が可能な機能を有すること。 ・常時監視機能の設定が可能であること。 ・ウィルス感染・検疫・駆除の一元監視機能を有すること。 ・本ホームページは、ウイルスやマルウェア等に対する対策を講じること。
	ドメイン管理	・ホームページのURLにて使用しているドメイン情報は本市専用のものとすること。
	セキュリティレベルの維持	・確保すべきセキュリティ実装の詳細に関しては、「参考３ 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」にて提示するので、必要な対策を講じること。
	暗号化	・通信データに対して暗号化を行う機能を設けること。 ・通信経路上の暗号化（SSL暗号化通信）を行うこと。 ・個人情報を含む等、機密性の高い情報を取り扱う場合、蓄積データ（データベース含む）や職員への通報経路を含め暗号化を行うこと。なお、暗号化の各機能や強度については、設計時に決定する。
	ログ対応	・サーバログについて、取得できること。 ・システムログ及びアプリケーションログを取得し、取得したログの漏えい、改ざん、消去、破壊等を防止できる機能を設けること。 ・Webサイトへの負担を考慮した上でアクセスログを取得し、本市が要請した場合、直ちにアクセスログの提示が可能な機能を設けること。
運用・保守性	バックアップ	・障害時等にシステムを復旧できるようなバックアップを実施すること。 ・作成したWebサイトコンテンツファイル等関連データは、環境変更時（情報更新時）バックアップを取得すること。
	世代管理	バックアップデータは業務上の必要性を加味した上で、複数世代で取得すること。
	復元	RPO（目標復旧地点）までデータを復元できるよう構築すること。
	監視	セキュリティ機能の稼働状況監視や、エラー監視を実行し、必要に応じて警告等を発する機能を設けること
使用性・ 効率性	アクセシビリティ対応	総務省の「みんなの公共サイト運用ガイドライン」に準拠した本サイトのウェブアクセシビリティ方針を作成し、公開すること。ウェブアクセシビリティ方針には、JIS規格「JIS X 8341-3:2016」の適合レベルを明記すること。 ■みんなの公共サイト運用ガイドライン https://www.soumu.go.jp/main_sosiki/joho_tsusin/b_free/guideline.html
	SEO対応	利用者の多い検索エンジンにおいて、図書館等に関連するキーワードについて本市ホームページが上位に表示されるように対策を講じること。

「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。

別紙「個人情報・情報資産取扱特記事項」

1　基本的事項

受託者は、この契約に基づき委託された業務（以下「委託業務」という。）を実施するに当たっては、個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号。以下「番号法」という。）、福岡市情報セキュリティに関する規則（平成23年福岡市規則第51号）及び情報セキュリティ共通実施手順その他関係法令を遵守し、個人情報及び情報資産の機密性、完全性、可用性を損なうことのないよう、個人情報及び情報資産を適正に取り扱わなければならない。

特に個人情報については、法第66条第２項において、受託者に行政機関等と同様の安全管理措置が義務付けられていることから、その保護の重要性を認識し、適正に取り扱わなければならない。

2　定義

（1）個人情報

法第２条第１項に規定する個人情報をいう。

（2）情報資産

次に掲げるものをいう。

・ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

・ネットワーク及び情報システムで取り扱う情報（ＯＡソフトウエアで取扱われるファイルを含む）並びにそれらを印刷した文書

・ネットワーク及び情報システムに関連する文書

（3）機密性

情報の利用を認められた者だけがその情報を利用することができることをいう。

（4）完全性

情報が破壊、改ざん又は消去されていないことをいう。

（5）可用性

情報の利用を認められた者が、必要な場合に中断されることなく、情報を利用することができることをいう。

3　秘密保持

受託者は、委託業務に係る個人情報並びに情報資産及び情報資産に関する情報を他人に知らせてはならない。この契約が終了し、又は解除された後においても同様とする。

4　従業者の監督等

受託者は、その従業者に委託業務に係る個人情報及び情報資産を取り扱わせるに当たっては、当該個人情報及び情報資産の安全管理が図られるよう、次に掲げる事項を周知し、その他必要かつ適切な監督を行わなければならない。

・委託業務に係る個人情報及び情報資産について、その適正な取扱い及び機密性、完全性、可用性の維持に必要な事項を遵守すること。

・個人情報を正当な理由なく利用したり、他人に提供したり、盗用した場合、法に規定する罰則が適

用される場合があること。
・上記の各事項は、委託業務に従事中のみならず、従事しなくなった後も同様であること。
・従業者の情報資産へのアクセス権限は、担当業務の内容に応じた最小限の権限に限定するとともに、取扱う情報資産の重要度に応じて複数人による確認の実施等を行うこと。

5　作業場所の制限

受託者は、定められた履行場所以外で委託業務に係る個人情報及び情報資産を取り扱ってはならない。ただし、福岡市（以下「市」という。）の書面による承認があるときは、この限りではない。

6　収集に関する制限

受託者は、委託業務の実施に当たって個人情報を収集するときは、この契約の目的を達成するため必要な範囲内で、適法かつ公正な手段により行わなければならない。

7　使用及び提供に関する制限

受託者は、委託業務以外の目的のために委託業務に係る個人情報及び情報資産を利用し、又は第三者へ提供してはならない。ただし、市の書面による承認があるときは、この限りではない。

8　安全確保の措置

受託者は、委託業務に係る個人情報及び情報資産の適切な管理のために、市が求める個人情報保護及び情報セキュリティの体制を備えるとともに、その他必要な措置を講じなければならない。

9　複写、複製又は加工の制限

受託者は、委託業務に係る個人情報及び情報資産が記録された文書、電磁的記録等を複写、複製又は加工してはならない。ただし、市の書面による指示又は承認があるときは、この限りではない。

10　再委託の制限

受託者は、委託業務に係る個人情報及び情報資産については、自ら取り扱うものとし、第三者に当該個人情報及び情報資産の取扱いを委託してはならない。ただし、市の書面による承認があるときは、この限りでない。なお、市の承認により第三者に委託する場合は、当該第三者に対して、契約書及び特記事項に規定する個人情報及び情報資産の取扱いの義務を遵守させるものとする。

11　委託業務終了時の返還、廃棄等

受託者は、この契約が終了し、又は解除されたときは、委託業務に係る個人情報及び情報資産を、市の指示に従い、市に返還し、若しくは引き渡し、又はその廃棄、消去等をしなければならない。なお、廃棄又は消去等をしたときは、廃棄又は消去等を行った旨の証明書を提出しなければならない。

12　報告及び監査・検査の実施

市は、受託者における委託業務に係る個人情報及び情報資産の取扱いの状況について、契約内容の遵守を確認するため、定期的に書面による報告を求め、必要に応じて監査又は検査をすることができる。

13　事故等発生時の報告

受託者は、個人情報及び情報資産の機密性、完全性、可用性を損なう、又は損なうおそれのある事故並びに欠陥及び誤動作を発見したときは、直ちに市に報告し、市の指示に従わなければならない。

14　事故等発生時の公表

市は、個人情報及び情報資産の機密性、完全性、可用性を損なう事故等が発生した場合、市民に対して適切な説明責任を果たすために必要な当該事故等の情報の公開を行うことができる。

15　契約の解除及び損害の賠償

市は、受託者がこの特記事項の内容に違反したときは、この契約の解除及び損害賠償の請求をすることができる。この場合において、受託者に損害を生じることがあっても、市はその責めを負わないものとする。