共用 Web サーバ運用支援業務提案仕様書

1　名称　　共用 Web サーバ運用支援業務

2　業務目的

福岡市が契約し、インターネット上で情報公開に使用しているサーバ群を共用 Web サーバとしている。

本業務は、共用 Web サーバの運用において、高度なセキュリティを実現し、業務利用に必要な作業や構成管理作業について支援を受けることにより、安全に情報提供を行うことで市民サービスの向上を図り、併せて行政事務の効率化を図ることを目的とする。

3　履行期間

令和７年 10 月１日から令和８年３月 31 日まで

※　令和７年度の履行状況が良好であった場合は、本事業の予算措置がなされた場合において、令和８年度及び前年度の履行状況を踏まえ令和 10 年度まで今回選定された事業者と契約を締結できるものとする。

その場合、業務内容については、令和７年度以降各年度の実施状況を踏まえ調整する。なお、市の施策の変更等により更新を行わない場合がある。

4　履行場所　　福岡市総務企画局 DX 戦略部情報システム課

5　基本要件

（１）　福岡市共用 Web サーバの概要

別紙１「福岡市共用 Web サーバの概要」のとおり。

（２）　福岡市共用 Web サーバのセキュリティ分担

別紙２「共用 Web サーバを利用したサイトのセキュリティ役割分担例」のとおり。

（３）　サイトの概要

運用サイト 41 サイト（うち、DB サーバとして個別サーバ 34 台を使用）。

6　機能要件

運用中の共用 Web サーバに関し、以下の機能及び役務を提供する。

（１）　共用 Web サーバの運用及び構成管理

インターネット上の Web サーバ及び DB サーバで構成しており、動的なコンテンツを運用するためのセキュリティが確保されたプラットフォームとして整備しているものであり、福岡市の契約により、現在カゴヤシステムで 41 サイトを運用中である。うち 34 サイトについては個別のサーバを割り当て、当面 DB サーバとして運用しているが、これらは Web サーバを含んでおり、今後全てのサイトを個別サーバに割り当て、運用することを計画している（別紙 3「個別 Web サーバ移行の概要」のとおり。）。

共用 Web サーバには概要に示すコンテンツに関する機能の他、サーバ内に設けているバックアップ領域に自動バックアップを行う機能があり、バックアップ以外にも領域の使用状況、稼働状況に関するログの取得及び集積といった構成管理機能を有している。

また、SSL に関してサーバ証明書を発行するサービスが提供されており、利用しているサイトがある。

なお、このサーバの FQDN については、LGPKI による「lg.jp」を基本的に使用している。

本業務では、以上の機能を有する共用 Web サーバについて、利用部署のセキュリティを担保しつつ、構築事業者における構築及び運用の支援を行うため、要件を以下のとおりとする。

① 日次処理

- 全バックアップ処理、バックアップ結果のログ取得及びバックアップ領域管理
- エラー監視及び発生時の通知

② 4 日ごと

- FTP サーバアクセスログの保存
- エラー及びワーニングログの取得及び保存

③ 月次処理

- Web アクセスログ及びサイト転送量の保存
- 解析ツール（Webalizer 等）によるコンテンツ別アクセス数解析
- 構成管理（リソース、トラフィック、プロセス、ディスク容量）レポートの提出及び異常時の報告
- IPS レポートの分析

（２） 高機能 WAF の導入及び運用

共用 Web サーバに高度なセキュリティを確保するため、クラウドベースの WAF を現在導入済みである。WAF はプロキシサーバ、接続先制御の機能により、共用 Web サーバのサイト別にアクセス制御を中心としたセキュリティを確保する。

本業務では、WAF の導入に関する一切の経費を含み、利用部署のコンテンツに対する設定、設定支援を行うものとし、WAF は以下の機能を要件とする。

- 検知エンジンは、ふるまい検知とし、シグネチャ方式、パターンマッチングによらないこと。
- ゼロデイ攻撃、DDoS 攻撃に対応していること。
- エンジンなどシステムのリージョンは、日本国内とする。
- サイト別に細かいチューニングが可能であること。
- 過去 1 年以上のレポートを提供できること。
- 月次で運用状況を確認すること。

（３） 個別サーバへのサイト移行支援

現在共用 Web サーバは単一の HTTP サーバにより各ディレクトリに振り分けたサイトを運用しているが、今後サイト別にカゴヤシステムの個別サーバ上へ移行する予定であるため、サイト移行支援業務として、移行作業における以下の技術支援及び作業支援を行う。

- サイトのディレクトリ構成に関する技術的事項の提供
- 移行するサイトの WAF 設定

7 非機能要件

（１） インシデント対応

インシデント対応については、表 1「インシデントレベル一覧表」に示す「福岡市サイバーセキュリティ・インシデント対応ガイドライン」に準じたレベルにより、以下のとおりとする。

① レベル 1

土、日、祝日、年末年始（12/29～1/3）を除く日の午前 8 時 45 分から午後 5 時 30 分まで。

② レベル 2 または 3

後述の連絡体制により協議のうえ、状況により緊急対応を行う。

表１「インシデントレベル一覧表」

影響度	情報セキュリティに係る分類		
	機密性の侵害	完全性の侵害	可用性の侵害
レベル１ （影響が軽微）	レベル２に満たない情報が開示された状況	－	利用者が短時間利用しづらくなる状況
レベル２ （影響が一部に限定）	暗号化された個人及び市の重要な情報が開示された状況	単一のサイトに対して意図しない変更が加えられた場合	市民及び市の基幹業務が短時間利用できなくなる状況
レベル３ （影響が重大）	暗号化されていない個人及び市の重要な情報が開示された状況	複数のサイトに対して意図しない変更が加えられた場合	市民及び市の基幹業務が長時間利用できなくなる状況

（２） 技術支援（月 10 回程度を予定）

各種問合せ、レンタルサーバ契約業者への問合せ代行支援作業、技術面での支援を伴う相談対応。

（３） 会議体

毎月１回定例会を実施する。

定例会では報告対象月の委託業務実施状況の情報共有に加え、IPA に掲載された脆弱性等に関する情報について報告する等、情報セキュリティにおける課題について発注者と受注者の話し合う場とする。開催方法は、市と協議の上、対面、Web 会議、書面開催のいずれかとする。なお、受注者は、①を電子情報で納品することとし、②～③については報告書等を作成し提出するものとする。

① WEB アクセスログ、エラーログ、FTP アクセスログ
② リソース監視（CPU、ディスクへの負荷等）
③ サイト転送量
④ アクセス数
⑤ ディスク使用状況
⑥ 不正アクセス等
⑦ システム障害、対応記録等
⑧ その他（IPA に掲載された脆弱性等に関する情報等）

（４） 連絡体制

連絡体制については、業務時間（土日祝日及び年末年始を除く日の８時 45 分から 17 時 30 分）及び業務時間以外の時間帯について、それぞれ担当者、電話番号、メールアドレスを提供し、管理する。

なお、管理用の様式については、協議により決める。

（５） 改善提案

以下について、随時提案を行う。

① セキュリティインシデント・障害対応

セキュリティインシデントや障害発生時（兆候がある場合を含む）の監視強化、影響範囲の調査、緊急対応、各コンテンツ所管課へのヒアリング実施、原因分析の支援、対応策の検討・提案等

② 本市稼働環境のセキュリティ対策の状況分析及び改善提案

各サイトに関すると考えられるミドルウェアの情報、新たな脅威などについて共有し、可能な限り提案を含めた情報の提供

（６） 施設等の利用

- この委託業務の履行に必要な、甲の施設、パソコン等の機器、帳票、資料等について甲の承認を得たうえで、これらを無償で使用できる。
- 使用を承認された施設等を委託業務の目的外に使用できない。
- 市庁舎内において、甲の作業時間を超えて業務の遂行を行う必要が生じた場合は、事前に甲の承認を受ける必要がある。
- 委託業務の履行のため、資料・機器等を庁舎内に持ち込む必要がある場合は、事前に甲の承認を受けなければならない。

（７） 資料の貸与

業務の実施にあたり、以下の資料を貸与する。貸与された資料は、紛失・破損することがないように保管・管理を厳重にし、業務完了後は全て速やかに返還する。

- 共用 Web の運用・管理に関する資料
- その他、必要と認めたもの

８ その他留意事項

（１）事業終了後のデータの廃棄

受注者は発注者が登録したデータや提供した媒体・書類など、発注者に関するすべてのデータは契約終了後に受注者が責任をもって受注者の環境から廃棄すること。

（２）使用料及びその支払い

四半期ごとに、受注者からの請求により支払う。

（３）機密保護

受注者は本事業遂行に当たって知り得た機密、機密と指定した事項及び事業の履行に際し知り得た機密（以下「機密情報」という。）を第三者に漏らし、又は不当な目的で利用してはならない。機密保護、情報公開に関わる全ての事項について、発注者の指示に従うこと。このことは、本契約が終了した後においても同様とする。

また、機密情報を取り扱う責任者及び従事者は、機密保持を誓約しなければならない。再委託先についても同様とする。

（４） その他

契約の解釈が日本法に基づくものであること。クラウドサービスの利用に関連して生じる一切の紛争も含め、日本の地方裁判所を専属的合意管轄裁判所とするものであること。

本仕様書に記載されていない事項または細部について疑義のある場合は、発注者と受注者とが協議して定める。

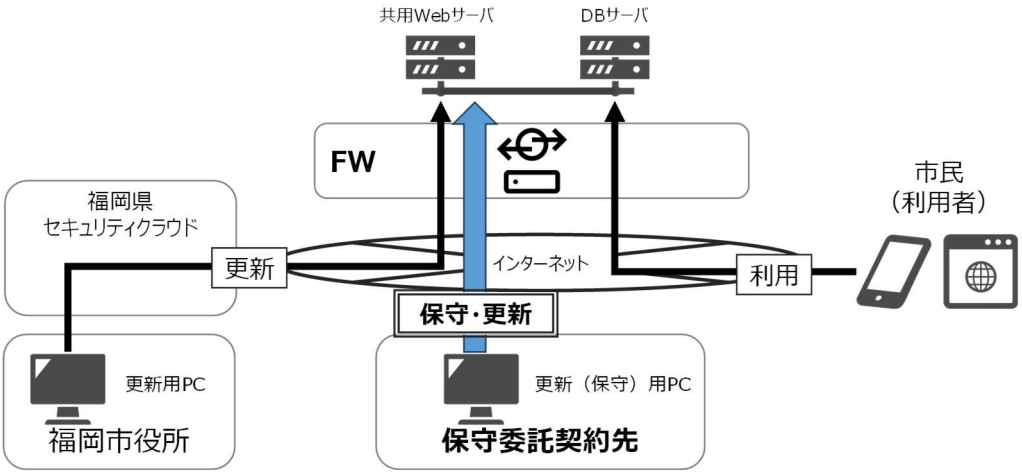
福岡市共用 Web サーバの概要

1 概要

共用 Web サーバは、Apache httpd のバーチャルホスト機能を利用し、本市の複数の部署で市民向けの Web サイトを提供するサーバである。

基盤部分を総務企画局情報システム課が管理し、各コンテンツ所管課へコンテンツ公開に必要な機能を提供している。

2 ネットワーク構成概要図



3 システム構成

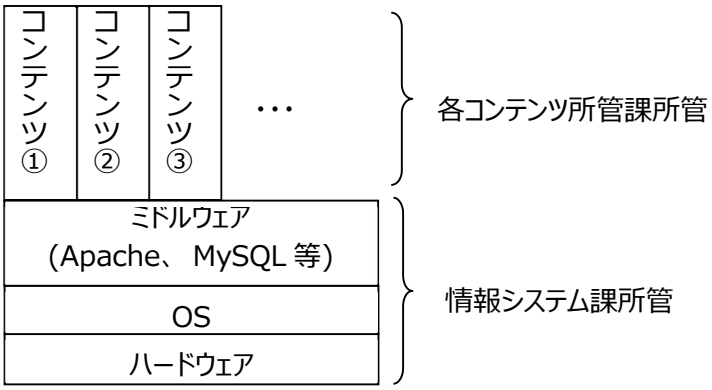
共用 Web サーバ（広義）は、共用 Web サーバ（狭義）と DB サーバからなる。

（１） 共用 Web サーバ（狭義）

① 全コンテンツで共有して利用する。

② Apache httpd や MySQL 等のミドルウェア以下の部分を情報システム課が管理し、その上で各コンテンツ所管課がコンテンツを公開する。

③ ハードディスク容量は約 2,000GB であり、各コンテンツでの最大利用可能容量は概ね 10GB である。



（２） DB サーバ

① コンテンツごとに設置される。

② DBMS は MySQL となる。

③ 各 DB サーバは http サーバを実装する。

④ 基本構成では、DB の最大容量は 1GB である。

4 インストール済みの主なソフトウェア

ソフトウェア名	バージョン	備考
Apache httpd	2.4.x	
PHP	8.2.x	
Perl	5.32.x	
MySQL	8.0.x	

※ソフトウェアのバージョンは変更となる場合がある。

5 運用

原則、定常的なコンテンツ更新作業等は、情報システム課設置のパソコンからのみ行う。ただし、コンテンツ構築やバージョン変更に伴う作業についてはリモートアクセスを許可する場合がある。

6 セキュリティ対策に関する留意事項

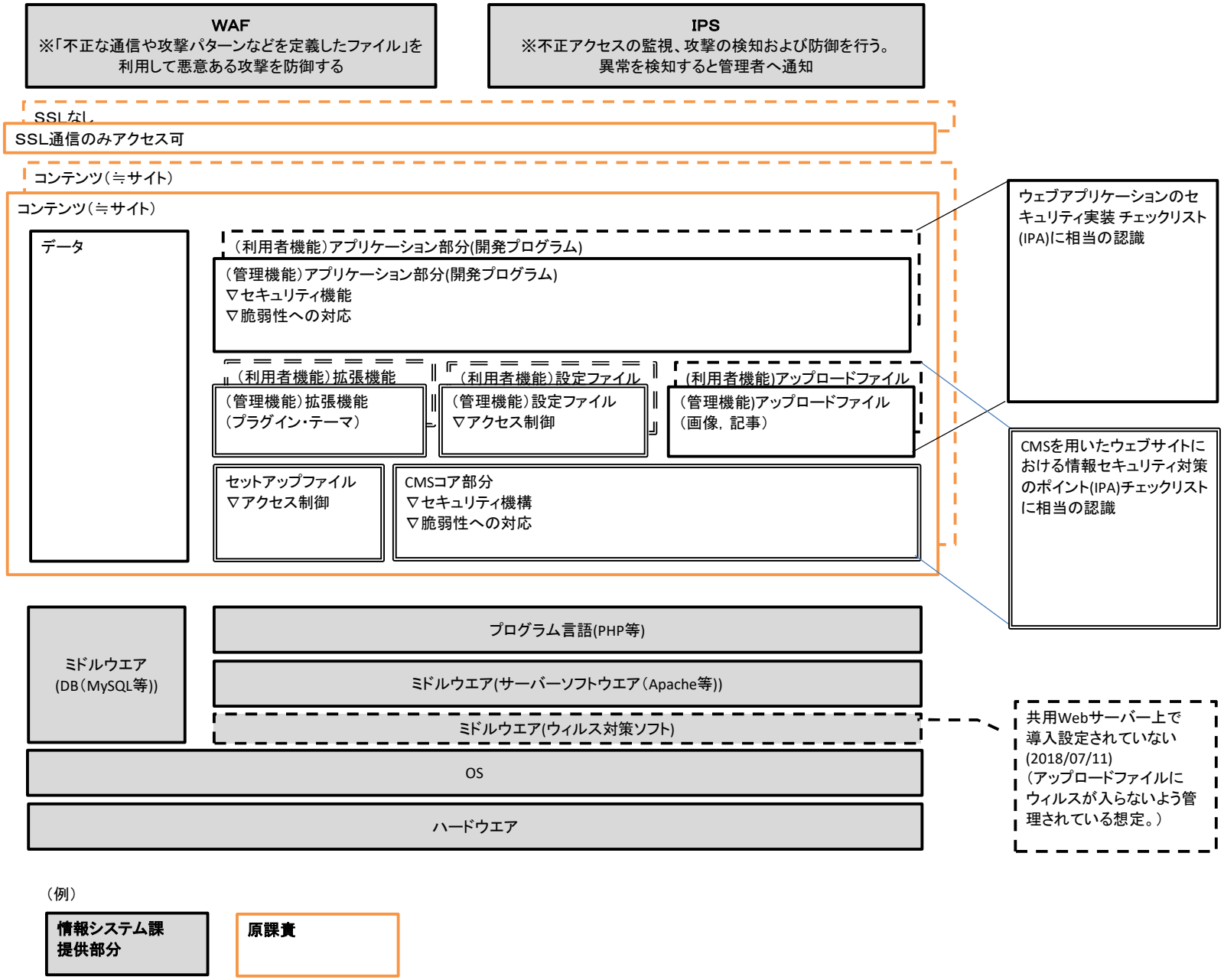
共用 Web サーバではセキュリティ対策として、IPS（侵入検知）及び WAF(Web アプリケーション・ファイアーウォール）を導入しているが、各コンテンツ所管課でも下記のようなセキュリティ対策を実施している。

- コンテンツ構築の際に、最新の脅威に対応したセキュリティ対策を行うこと。
- コンテンツで利用しているプログラム等に脆弱性が見つかった場合は、速やかに脆弱性に対応すること。
- 上記４のような OS、ミドルウェア等、全コンテンツで共有しているソフトウェアに脆弱性が見つかった場合は共用 Web サーバの利用所管課が同時に対応を行う必要があるが、その場合でも迅速に対応が可能な体制を整えること。

これらセキュリティに係る対応を速やかに実施する体制を各コンテンツ所管課にて整えておくことを共用 Web サーバの利用の条件としている。なお、セキュリティ対策は各 Web サイト管理者（コンテンツ所管課）の責務であり、セキュリティ上の問題を放置しているＷｅｂサイトについては、情報システム課にてサイトの閉鎖を実施する場合がある。

共用Webサーバを利用したサイトのセキュリティ役割分担例

別紙２



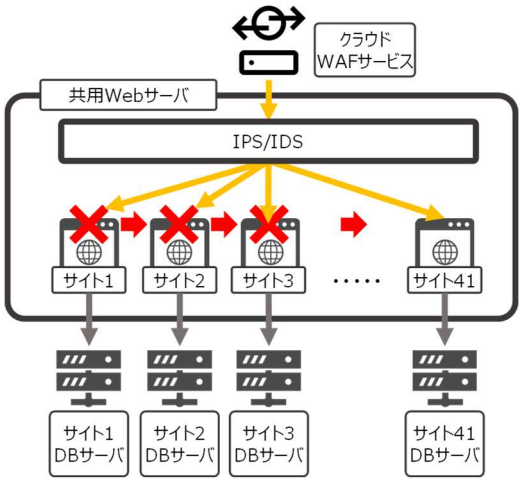
個別 Web サーバ移行の概要

1 概要

現在共用 Web サーバに含まれている複数のサイトについて、現在 DB サーバとして使用しているサーバにサイトを移行する。

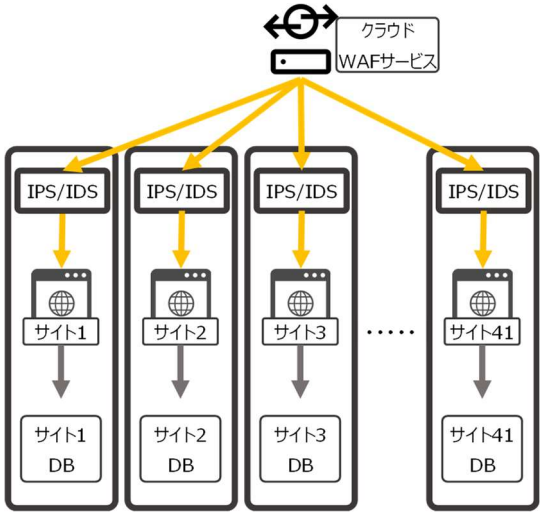
2 移行概念図

【現行】



同じ階層に各サイトのフォルダを設置する構成。
リソースやライブラリを共有しており、アカウント毎にアクセス制限を実施している。
各サイトに与えているアカウントにより相互にフォルダ参照や操作は行えない。
統一的に外部侵入を防ぐための管理が比較的行いやすいが、サイトごとのきめ細かい管理は難しく、時間がかかる。また、外部から脅威の侵入を許すと、全サイトに影響を及ぼす可能性が高い。

【移行後】



サイト別にサーバを占用する構成。
リソース、ライブラリ、アカウントは完全に独立しており、他のサーバ対する参照や操作は行えない。
各サイトは物理的に独立するため、他のサーバに対する参照や操作は行えない。
サイトに脅威が発生しても影響はサイト内に限られ、安全性が高い。統一的な直接的管理は難しくなるが、各サイトで個別に運用を行えるため、コンテンツに応じたセキュリティの高度化が見込める。

3 移行方法

各サイトのコンテンツ保守事業者での移行作業が可能となるようサーバの構成を準備し、移行先への移行は当該保守事業者が行う。移行完了後、当該サイトで使用していたディレクトリ及びコンテンツ資材を閉塞する。