5.11.公開 Web サーバ

5.11.1.定義

インターネットを通して情報コンテンツの配信を行うWebサーバ。主に国民・企業等への情報公開での利用を想定している。24 時間×7 日間/週、多様な場所、不特定のクライアントからアクセスされうることから、悪意をもった様々な攻撃(データ改ざん、サービス妨害、情報漏えい、アクセス権限の不正昇格、否認等)を受ける可能性がある。従って、それらの攻撃から資産を防御し、セキュリティ事件・事故を防止するための策が施される。また、外部ネットワーク(インターネット)と内部ネットワークとの間にファイアウォールで仕切られた安全性の高いセグメント(DMZ: DeMilitarized Zone:非武装地帯)内に設置される。

なお、IPv4 アドレスの枯渇問題を踏まえ、IPv4 と IPv6 の共存や併用が適切に行える様、公開 Web サーバ関連の各種機器に関して、設計時及び機材調達時のみならず、運用・管理・監視・保守等の内容やセキュリティ対策についても、あらかじめ考慮しておくこと。

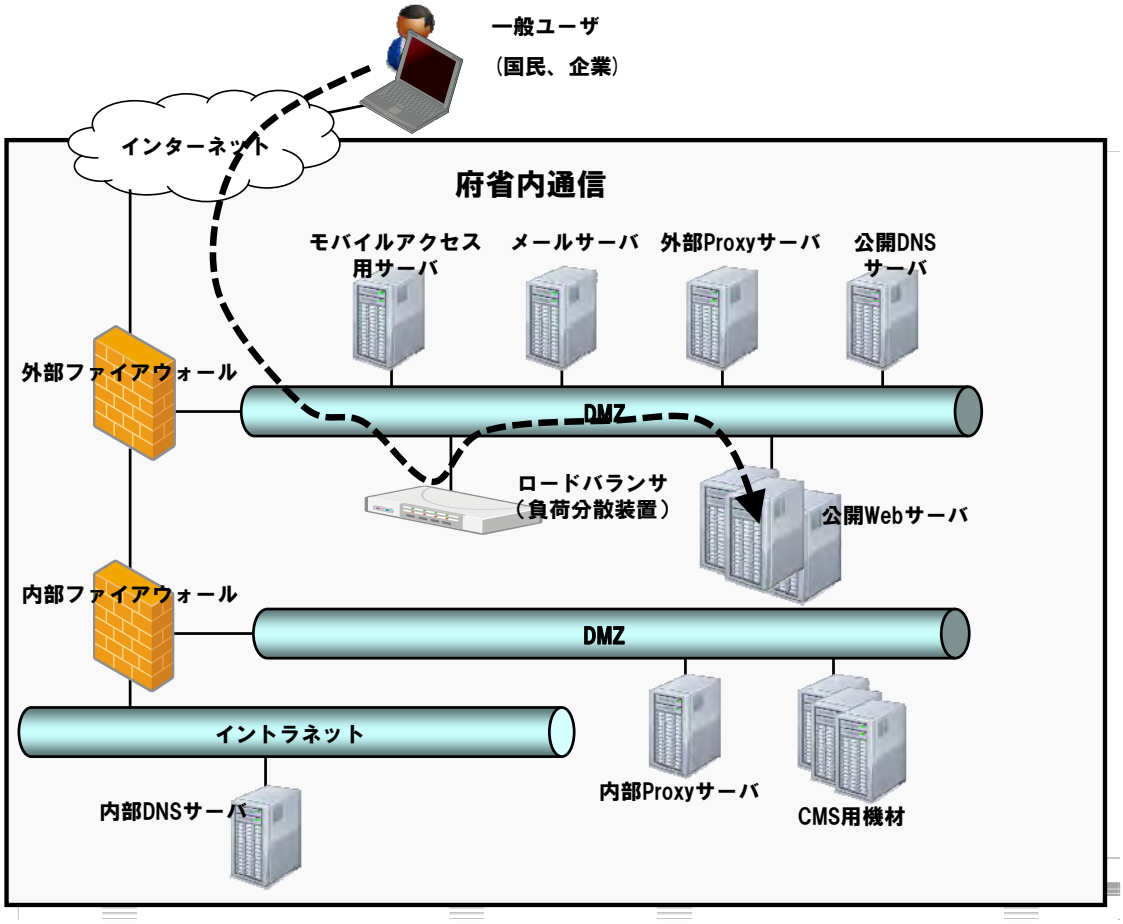

図 5.11-1 公開 Web サーバの配置

公開 Web サーバの機能・サービス	
機能・サービス	定義
WWW サービス	HTTP プロトコルを利用して、主に国民・企業等への情報公開のためのコンテンツ(文書・画像・その他データ)の配信を行うサービス。
FTP サービス	FTP プロトコルを利用して、府省外の端末と公開 Web サーバ間でファイルの送受信(アップロード・ダウンロード)を可能にするサービス。主に大容量又は頻繁に版が更新されるファイル群の配信や、アップロードを行う場合に利用される。
コンテンツ・マネジメント・システム(CMS)	コンテンツ・マネジメント・システム(CMS)とは、公開 Web サーバ上の WWW サービスから公開・配信する Web ベースのデジタルコンテンツ(テキストや画像等)の制作、管理、公開 Web サーバへの配信、維持・保守を行うサービス。内部統制やアクセシビリティへの対応や配慮を行うことを想定した機能を有する。

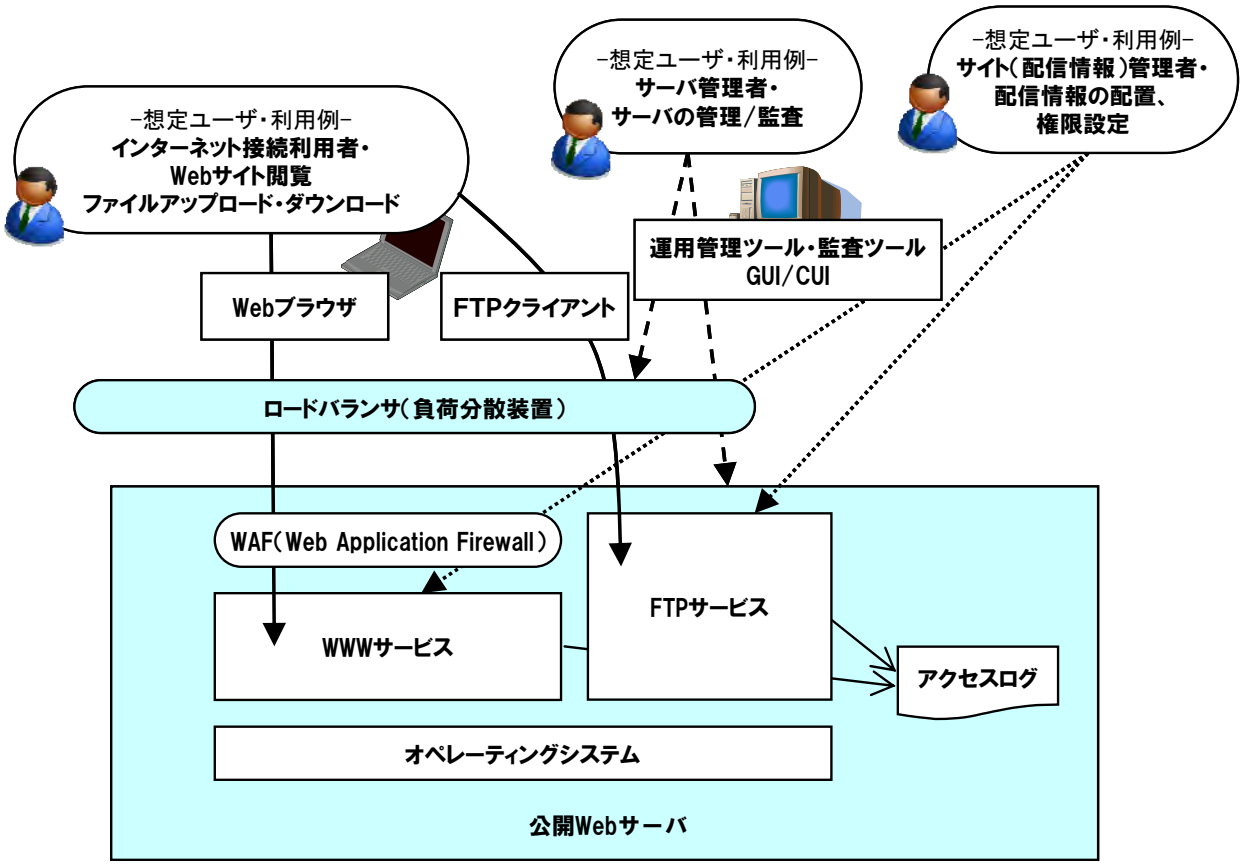

図 5.11-2 公開 Web サーバ概念図

5.11.2.WWW サービス

機能要件		
1	基本	Web ブラウザ等のクライアントからの要求に対して、Web サーバ上に格納されたコンテンツを返送する。加えて、コンテンツに埋め込まれたサーバサイドスクリプト言語【SSI 等】に従いデータ【HTML 等】を変換して送信する機能及びサーバ上で外部プログラムを実行することによって動的にデータを整形(HTML、XML、画像データ等)して送信する機能を有すること。
2	基本	利用者認証・認可:利用者からの公開サイトへのアクセスに対して、個人を特定し、認証(事前に利用を許されている者に対してはサイトの利用・アクセスを許可し、それ以外の者は拒否する)を行う機能を有すること。認証方式は、経路暗号化と基本認証の組み合わせや、ダイジェスト認証等、認証情報の漏えいやなりすましを防げる方式を利用すること。また、利用者ごとに公開 Web サイト内でアクセスできるコンテンツの範囲や操作の権限の設定及び認可を行えること。またこれら認証・認可を外部のディレクトリサービスと連携できること。
3	基本	WAF(Web Application Firewall)と密接に連携してセキュリティを確保する機能を有すること。
4	加点	サーバ証明書と経路暗号化:サーバ証明書(サーバの公開鍵とサーバの情報)をインストールし、SSL や TSL プロトコルで転送データを暗号化できる機能を有すること。電子政府推奨暗号リストに対応する暗号強度を有するものを適用すること。
5	基本	配信ファイル形式の管理:Web サイトから配信を許可するファイルの形式(フォーマット)の組み合わせを事前に設定しておき、設定に存在しないファイルの形式は配信できないように構成できること。
6	基本	配信ファイルの配置:Web サイト管理者が、イントラネットや公開 Web サイトから配信するコンテンツの配置及びアクセス権限の設定、コンテンツの更新情報の確認・テストの作業を速やかに実施できること。
7	基本	アクセスログ記録:誰が、何時、何を閲覧したか、最後に情報が閲覧されたのはいつか等の履歴をログファイルとして蓄積できること。ログ情報は、HTTP 通信に関する記録情報のタイプと順序を選択・指定することができ、また W3C 拡張ログファイル形式又は NCSA 共通ログファイル形式で出力できること。
8	加点	監査:アクセスログの中から、監査イベント別、時間別、アクセスユーザ別等の様々な切り口で集計したレポートを出力して、監査の目的で閲覧できること。
9	加点	効率測定:WWW サイトの要求量【同時接続数、平均リクエスト頻度 等】、処理効率【HTTP 処理スループット、レスポンスタイム 等】や資源の消費状況【CPU 利用率 等】を測定する機能を有すること。
10	基本	セッション管理:Web アプリケーションが安全性の高いセッション管理を行うために必要なセッション ID の発行及びセッション情報の維持の機能を提供できること。
11	基本	管理インタフェース:各種管理操作【利用者のアカウントの追加・編集・削除、サイトの権限の設定、配信できるファイルタイプの設定、監査、パフォーマンスモニタリング 等】を内部ネットワーク上の管理者端末から行うための、GUI(Graphical User Interface)又は CUI(Character-based User Interface)ツールの機能を提供すること。また、プログラムから管理タスクを呼び出すための API(Application Program Interface)を提供すること。

注記 WAF:公開 web サイト上のアプリケーションや web ページに対する送信情報の内容を検査して SQL インジェクションやクロスサイトスクリプティング等の攻撃につながる不正なデータを検出しアクセスを遮断する機能。

非機能要件（個別の要件がある場合のみ記述）		
性能	基本	クライアント(主に Web ブラウザ)からの要求を処理できる十分な処理性能【同時接続数、SPECweb 値　等】を有すること。
可用性	基本	サーバハードウェアやミドルウェアの障害が発生した場合であっても正常な後続の要求処理を継続できる構成【クラスタリング　等】を有すること。
処理能力の拡張性	基本	同時接続数、アクセス量が増加、又は減少した際に、サービスを止めずにサーバの資源の増強/削減、サーバの増設/削減等を行い適切な処理能力を確保できること。
暗号化・復号性能拡張性	基本	プロトコルの暗号化・復号の処理性能を向上させる機構【SSL アクセラレータ　等】を追加できる構成であること。
定期的なミドルウェア・OS へのセキュリティパッチの情報配信	基本	情報セキュリティサービスベンダーの情報提供対象ソフトウェアに含まれ、情報提供サービス等への加入により脆弱性やセキュリティパッチの情報が定期的{月に 1 回程度}にサーバ管理者に配信されること。
ミドルウェア・OS へのセキュリティパッチの適用作業	基本	オペレーティングシステムや Web ページ配信ミドルウェアへのセキュリティパッチの適用、テスト・検証、状況に応じた取り消し(削除)の作業が行えること。
サービス提供時間帯	基本	{24 時間×7 日間/週}の時間帯でサービスを提供できること。
バックアップ・復旧	基本	公開 Web サイト上のデータ(配信コンテンツ及びサーバの構成情報)のバックアップを、Web サイトを停止することなく行え、またそのバックアップデータからサイトの復旧を速やかに行えること。
リモート管理	基本	内部ネットワーク上の管理者端末から公開 Web サイトの管理タスクを実行できる構成を有すること。
負荷分散	基本	公開 Web サーバの前面に配置された負荷分散機能(装置)によって、負荷分散が可能な構成がとれること。

関連する技術	
Web サーバ・クライアント(Web ブラウザ)間通信プロトコル	HTTP(Hyper Text Transfer Protocol)
Web ページ記述言語	HTML(Hyper Text Markup Language) HTML 4.01 仕様(W3C 勧告 1999 年 12 月 24 日)として規格化されている。 CSS(Cascading Style Sheets) CSS2.1 仕様(W3C 勧告 2009 年 9 月 8 日)として規格化されている。
サーバ上で外部プログラムを実行する技術	CGI(Common Gateway Interface) CGI は、RFC3875 として規格化されている。 Java Servlet ASP.NET(Active Server Pages for .NET)
サーバサイドスクリプト言語	SSI(Server Side Include) PHP(Hypertext Preprocessor) JSP(Java Server Pages)
Web 処理効率測定単位	SPECweb
認証方式	基本認証(Basic Authorization) ダイジェスト認証(Digest Authorization)
ディレクトリサービスプロトコル	LDAP(Lightweight Directory Access Protocol)
経路暗号化プロトコル	SSL(Secure Socket Layer)、TLS(Transport Layer Security)
様々な形式のファイルを電子メール又は HTML プロトコルで送受信するための規格	MIME(Multipurpose Internet Mail Extension)
ログファイル形式	W3C 拡張ログファイル形式 NCSA 共通ログファイル形式
監視・制御機構/プロトコル	SNMP(Simple Network Management Protocol) WBEM(Web-Based Enterprise Management)

5.11.3.FTP サービス

機能要件		
1	基本	クライアント PC と公開 Web サーバの間でのファイル転送を行う際のサーバ側のファイル送受信サービスを提供できること。
2	基本	利用者認証・認可：利用者を特定し、それぞれの権限に合わせて許可される操作や、その対象となるファイルやフォルダへの操作の許可や拒否を行う仕組みを有すること。またこれら認証・認可を OS のアクセス制御機能や外部のディレクトリサービスと連携して行えること。
3	基本	送受信データ暗号化：送受信するファイルのデータや利用者識別子やパスワードを暗号化することができること。電子政府推奨暗号リストに対応する暗号強度を有するものを適用すること。
4	基本	ユーザ分離：利用者ごとにアップロード・ダウンロードできる領域(フォルダ)を分離し、ほかの利用者のフォルダから隔離することができること。 利用者用フォルダを指定された構造で作成することができること。また、利用者単位に利用できるフォルダ容量や転送できるファイルの最大サイズを指定できること。
5	基本	アクセスログ記録：誰が、何時、何を、どのような操作を行ったか等の履歴をログファイルとして蓄積できること。ログ情報は、FTP 通信に関する記録情報のタイプと順序を選択・指定することができ、また W3C 拡張ログファイル形式又は NCSA 共通ログファイル形式で出力できること。
6	基本	監査：利用状況ログの中から、監査イベント別、時間別、アクセスユーザ別等の様々な切り口で集計したレポートを出力して、監査の目的で閲覧することができること。
7	基本	クライアントアクセス：クライアント PC から FTP サイトへのアクセスは、Web ブラウザ又は CUI(Character-based User Interface)を利用して行えること。
8	加点	効率測定：FTP サイトの処理要求【同時接続数 等】、処理効率【転送速度 等】やサーバの資源の消費状況【CPU 使用率、I/O キュー待ち数 等】を測定する機能を有すること。
9	基本	管理インタフェース：各種管理操作【利用者のアカウントの追加・編集・削除、サイトの権限の設定、配信できるファイルタイプの設定、監査、パフォーマンスモニタリング 等】を内部ネットワーク上の管理者端末から行うための手段を提供すること。また、管理手段が GUI(Graphical User Interface)又は CUI(Character-based User Interface)ツールである場合は、プログラムから管理タスクを呼び出すための API(Application Program Interface)を提供すること。

非機能要件（個別の要件がある場合のみ記述）		
性能	基本	ファイルのアップロード及びダウンロード処理要求量を処理できる十分な性能【同時接続数、データ転送能力　等】を有すること。
データ許容量	基本	アップロード・ダウンロードするファイルを格納するディスク領域の容量が十分確保されていること。
可用性	基本	単一のサーバのサーバハードウェアや OS、ミドルウェアの障害が発生した場合であっても正常なサーバが後続の要求処理を継続できる構成を有すること。
ディスク領域の拡張性	基本	アップロード・ダウンロードするファイルを格納するディスク領域の空き容量が不足した際に、事前に指定した時間以内に空(あ)き領域の拡張を行えること。
処理能力の拡張性	基本	同時接続数、データ転送要求量が増加、又は減少した際に、サービスを止めずにサーバの資源の増強/削減、サーバの増設/削減等を行い適切な処理能力を確保できること。
定期的なミドルウェア・OS へのセキュリティパッチの情報配信	基本	情報セキュリティサービスベンダーの情報提供対象ソフトウェアに含まれ、情報提供サービス等への加入により脆弱性やセキュリティパッチの情報が定期的{月に 1 回程度}にサーバ管理者に配信されること。
ミドルウェア・OS へのセキュリティパッチの適用作業	基本	オペレーティングシステムや FTP サービスミドルウェアへのセキュリティパッチの適用、テスト・検証、状況に応じた取り消し(削除)の作業が行えること。
サービス提供時間帯	基本	{24 時間×7 日間/週}の時間帯で提供できること。
バックアップ・復旧	基本	FTP サイト上のファイル格納領域のデータのバックアップを、サービスを停止することなく行え、またそのバックアップデータからサイトの復旧を速やかに行えること。
リモート管理	基本	内部ネットワーク上の管理者端末から公開 FTP サイトの管理タスクを実行できる構成を有すること。
負荷分散	加点	複数のサーバを束ねて単一の FTP サイトを構築し、かつデータ通信量の実績が最小のサーバに要求を割り当てることによってファイル転送要求の負荷を分散できる構成を有すること。

関連する技術	
ファイル転送プロトコル	FTP(File Transfer Protocol)
ディレクトリサービスプロトコル	LDAP(Lightweight Directory Access Protocol)
ファイル転送におけるデータ暗号化プロトコル	FTPS (File Transfer Protocol over SSL/TLS) SFTP(Secure File Transfer Protocol)
ログファイル形式	W3C 拡張ログファイル形式 NCSA 共通ログファイル形式
監視・制御機構/プロトコル	SNMP(Simple Network Management Protocol) WBEM(Web-Based Enterprise Management)

5.11.4.コンテンツ・マネジメント・システム(CMS)

機能要件		
1	加点	コンテンツの制作作業において、既存の Web サイトのコンテンツを取り込むことができること。
2	加点	テキスト、画像等のコンテンツ群に対して検索を行い、一覧として閲覧・参照を行いながら効率的にコンテンツの制作を行えること。
3	加点	Web ページのひな形等のテンプレートを活用し、サイト全体で標準化又は統一化したページデザインやアクセシビリティの規格に準拠したコンテンツ作成や統制が容易に行えること。
4	基本	HTML ファイルの編集による更新作業が可能であること。
5	加点	【PDF、Flash、テキスト、Microsoft Office ドキュメント 等】の形式のデータをコンテンツファイルとして扱えること。
6	加点	コンテンツに対する操作の権限を特定の利用者又は利用者グループごとに設定する権限管理及び認証・認可の機能を有すること。また認証・認可の機能はほかのディレクトリサービスと連携することができること。
7	基本	公開予定のコンテンツファイルを登録して、公開後の Web ページのイメージを閲覧できる機能を有すること。
8	加点	公開予定のコンテンツの承認及び公開を自動化又は支援するワークフロー機能を有すること。
9	加点	事前に公開予定のコンテンツファイル及び公開開始日時を指定しておくと、公開開始日時になった時点から、そのコンテンツを自動的に公開 Web サーバから公開の状態にさせる機能を有すること。
10	加点	過去の更新履歴を参照し、また任意の時点の状態でのコンテンツの公開イメージの閲覧や、その時点にコンテンツの内容を戻す等の操作が行えること。
11	加点	コンテンツの制作・保守・運営を行う担当者が実施したファイルへの操作の履歴(誰が、何時、何を行ったのか)を閲覧できること。
12	加点	更新情報配信技術【RSS フィード、ATOM フィード 等】による Web ページ更新情報の配信が可能であること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	CMS が停止しても WWW サービスによるコンテンツの配信が継続できること。
バックアップ・復旧	加点	Web コンテンツのバックアップを制作作業又は配信している最中に実施できること。またバックアップから復元する際には任意の時点のコンテンツに戻せること。

関連する技術	
Web アクセシビリティの確保基準	JIS X 8341-3 W3C WCAG(Web Content Accessibility Guidelines) 1.0/2.0
ディレクトリサービスプロトコル	LDAP(Lightweight Directory Access Protocol)