SmartPBXカスコンシステム

機能設計書

第2.2版

NTTコミュニケーションズ株式会社

|  |  |  |
| --- | --- | --- |
| 発行日 | 有効期限 | 発行者 |
| 2016/06/30 | 次回改版まで | NTTソフトウェア |

|  |
| --- |
| 本ドキュメントの一部または全部を許可なく複写、複製することは、その形態を問わず禁止します。 |

改版履歴

| 項番 | 改版日 | 版 | 事由 | 変更内容等 | 変更者 |
| --- | --- | --- | --- | --- | --- |
| 1 | 2014/03/31 | 1.0 | 新規作成 |  | NTTソフトウェア |
| 2 | 2014/04/25 | 1.1 | 端末自動設定機能の追加に伴う変更 | 対象となる端末自動設定機能について記載 | NTTソフトウェア |
| 3 | 2014/05/30 | 1.2 | VM支障移転機能の追加に伴う変更 | 対象となるVM支障移転機能について記載 | NTTソフトウェア |
| 4 | 2014/09/26 | 1.3 | Web設定機能改善に伴う変更 | 一定期間経過した通話ログ、トラフィック情報のDBレコードを削除する機能について記載  特殊文字対策の対象文字を追加 | NTTソフトウェア |
| 5 | 2014/09/03 | 1.4 | ユーザ拠点情報管理機能追加に伴う変更 | 対象となるユーザ拠点情報管理機能について記載 | NTTソフトウェア |
| 6 | 2014/09/11 | 1.4 | ユーザ拠点情報管理機能の画面追加に伴う変更 | ユーザ拠点情報管理機能の設定確認画面を追加 | NTTソフトウェア |
| 7 | 2014/12/19 | 1.5 | UNO接続機能追加に伴う変更 | 対象となるUNO接続機能について記載 | NTTソフトウェア |
| 8 | 2015/03/20 | 1.6 | Step2.5開発に伴う変更 | 追加となる対応ブラウザのバージョンを記載  対象となる開通案内随時出力機能について記載  対象となる内線サーバ設定反映機能について記載 | NTTソフトウェア |
| 9 | 2015/06/30 | 1.7 | Step2.6開発に伴う変更 | 対象となる外線情報検索機能ついて記載 | NTTソフトウェア |
| 10 | 2015/09/18 | 1.8 | Step2.7開発に伴う変更 | Tomcatのバージョンを変更 | NTTソフトウェア |
| 11 | 2015/12/22 | 1.9 | Step2.8開発に伴う変更 | Strutsのバージョンを変更  IP Phone MACアドレス管理機能の追加 | NTTソフトウェア |
| 12 | 2016/03/18 | 2.0 | Step2.9開発に伴う変更 | 対応ブラウザからIE8、9、10を除外  対応OSとしてWindows10を記載  機能一覧に保留音設定機能を追加 | NTTソフトウェア |
| 13 | 2016/3/22 | 2.1 | Step3.0開発に伴う変更 | Strutsのバージョンを変更 | NTTソフトウェア |
| 14 | 2016/5/16 | 2.2 | Step3.0開発に伴う変更 | Strutsのバージョンを変更 | NTTソフトウェア |

目　次

[1 はじめに 1](#_Toc450289861)

[1.1 はじめに 1](#_Toc450289862)

[1.2 機能設計書の構成 1](#_Toc450289863)

[1.3 用語の定義 2](#_Toc450289864)

[2 システム構成 3](#_Toc450289865)

[2.1 システム概要 3](#_Toc450289866)

[2.2 システム化範囲 3](#_Toc450289867)

[2.3 システム構成 5](#_Toc450289868)

[2.3.1 システム構成 5](#_Toc450289869)

[2.3.2 ハードウェア構成 6](#_Toc450289870)

[2.3.3 ソフトウェア構成 7](#_Toc450289871)

[2.3.4 開発環境 7](#_Toc450289872)

[2.3.5 対応ブラウザ 8](#_Toc450289873)

[2.3.6 文字コード定義 8](#_Toc450289874)

[2.4 機能一覧 9](#_Toc450289875)

[2.5 外部システムとの機能分担 13](#_Toc450289876)

[2.5.1 外部システム一覧 13](#_Toc450289877)

[2.5.2 外部インタフェース一覧 13](#_Toc450289878)

[3 システム設計方針 14](#_Toc450289879)

[3.1 機能性方針 14](#_Toc450289880)

[3.2 信頼性方針 14](#_Toc450289881)

[3.3 使用性方針 15](#_Toc450289882)

[3.4 保守性方針 15](#_Toc450289883)

[3.5 可搬性方針 15](#_Toc450289884)

[3.6 セキュリティ方針 16](#_Toc450289885)

[3.6.1 特殊文字対策 16](#_Toc450289886)

[3.6.2 不正アクセス対策 16](#_Toc450289887)

[3.7 性能方針 17](#_Toc450289888)

[3.7.1 性能目標 17](#_Toc450289889)

[3.7.2 性能実現方針 17](#_Toc450289890)

[4 SO系機能 18](#_Toc450289891)

[5 カスコン系機能 19](#_Toc450289892)

[6 管理系機能 20](#_Toc450289893)

[6.1 DBレコード保管機能 20](#_Toc450289894)

[6.2 通話ログ、トラフィック情報のDBレコード削除機能 21](#_Toc450289895)

# 

# はじめに

## はじめに

本書は、SmartPBXカスコンシステム（以下、本システムと記す）の機能設計について記載する。

## 機能設計書の構成

機能設計書および関連する設計書・仕様書の全体構成を以下に示す。

表 1.2‑1 機能設計書の構成

|  |  |  |  |
| --- | --- | --- | --- |
| 項番 | 設計書名称 | 内容 | 備考 |
| 1 | 機能設計書（本書） | システム全体の構成、共通事項、および、各機能について記述する。 |  |
| 2 | [別紙１]画面設計書 | 本システムの画面について記述する。 |  |
| 3 | [別紙２]ファイル設計書 | 本システムにて使用するファイル（内線サーバの設定ファイルや端末自動設定ファイル、一括処理用ファイル、スタティックルート設定ファイル、パケットフィルタ設定ファイル）について記述する。 |  |
| 4 | [別紙３]データベース設計書 | データベーステーブル設計について記述する。 | FD工程・DD工程共通で作成する。 |
| 5 | [別紙４]メッセージ・ログ設計書 | 本システムが出力するメッセージおよびログ出力について記述する。 | FD工程・DD工程共通で作成する。 |
| 6 | [別紙５]対向装置通信処理仕様書 | 本システムと外部システム（上位装置および内線サーバ、端末自動設定ファイル配置用WEBサーバ）との通信にともなう処理について記述する。 |  |

## 用語の定義

本書にて使用する用語の定義を以下に示す。

表 1.3‑1 用語の定義

| 用語 | 意味 | 備考 |
| --- | --- | --- |
| SmartPBX | * FMC（固定/携帯連携）に対応し、内線通話機能を具備したクラウドPBX型サービスである、Arcstar SmartPBX。 |  |
| カスコン | * カスタマーコントロールの略。 |  |
| Asterisk | * Digium, Inc.が開発しているオープンソースのIP-PBX。 |  |
| BHEC | * NTTコミュニケーションズ様が提供する、ネットワーク仮想化技術を活用した企業向けクラウドサービス。 |  |
| VPN | * 仮想的なプライベートネットワーク接続。 |  |
| Arcstar Universal One | * NTTコミュニケーションズ様が提供するVPNサービス。 |  |

# システム構成

## システム概要

本システムは、上位装置からのSO通知を受信する機能、SmartPBXのユーザ自身が内線設定を変更できるようにするためのカスコン機能、および、上位装置からのSO通知やユーザによるカスコン操作の内容を内線サーバに反映する機能を提供する。

## システム化範囲

本システムでのシステム化範囲を以下に示す。

端末自動設定ファイル  
配置用WEBサーバ

SO情報取得

Webエントリ  
システム

SO通知（新設/変更/廃止）

開案Web  
システム

本システム

内線  
サーバ

システム化範囲

処理結果通知（工事結果）

処理結果通知（SO取込）

内線サーバの設定

VM-IDの払い出し

端末自動設定ファイルの配置

開通案内情報ファイル送信

図 2.2‑1　業務フロー（SO通知）

端末自動設定ファイル  
配置用WEBサーバ

内線  
サーバ

本システム

ユーザ

システム化範囲

カスコン操作（HTTPS）

内線サーバの設定

端末自動設定ファイルの配置

図 2.2‑2　業務フロー（カスコン操作）

端末自動設定ファイル  
配置用WEBサーバ

内線  
サーバ

本システム

ユーザ

VM情報管理

システム化範囲

VM支障移転

VPN移転

内線サーバの設定

図 2.2‑3　業務フロー（VM情報管理）

## システム構成

### システム構成

以下に、システム構成を示す。

図 2.3‑1　システム構成

### ハードウェア構成

本システムのハードウェア構成を以下に示す。



**統合OSS網**

開案WEB

WEBエントリ

**BHEC**

内線サーバ  
（Asterisk）

FireWall（BHEC提供機能）

ACT-ACT構成

・・・

WEBサーバ

Load Balancer（BHEC提供機能）





本システム



0系

1系

・  
・  
・

DB負荷分散サーバ





端末自動設定ファイル  
配置用WEBサーバ

ACT-STB構成



ACT-ACT構成

DBサーバ

・・・



DBバックアップサーバ

0系

1系

図 2.3‑2 ハードウェア構成

本システムのハードウェア一覧を以下に示す。

表 2.3‑1 ハードウェア一覧

| 項番 | ハードウェア名 | 台数 | 割当CPU | 割当メモリ | 割当HDD | 備考 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | WEBサーバ | 2台※ | 1 | 1GB | 「基本領域：16GB　追加領域：なし」 |  |
| 2 | DBサーバ | 2台※ | 4 | 1GB | 「基本領域：16GB　追加領域：120GB」 |  |
| 3 | DB負荷分散サーバ | 2台※ | 1 | 1GB | 「基本領域：16GB　追加領域：なし」 |  |

※負荷状況によっては、今後、増設する。

### ソフトウェア構成

本システムのソフトウェア構成を以下に示す。

表 2.3‑2 WEBサーバ搭載ソフトウェア一覧

| 項番 | 種別 | ソフトウェア名 | バージョン | 備考 |
| --- | --- | --- | --- | --- |
| 1 | OS | CentOS | 6.5 |  |
| 2 | WEBアプリケーションサーバ | Apache Tomcat | 7.0.63 |  |
| 3 | 開発言語 | Java | 7 | ※OpenJDKを使用する。 |
| 4 | フレームワーク | Struts | 2.3.28.1  2016/3/28  Strutsのバージョンを変更 |  |

表 2.3‑3 DBサーバ搭載ソフトウェア一覧

2016/5/16

Strutsのバージョンを変更

2.3.28→2.3.28.1

| 項番 | 種別 | ソフトウェア名 | バージョン | 備考 |
| --- | --- | --- | --- | --- |
| 1 | OS | CentOS | 6.5 |  |
| 2 | DBサーバ | PostgreSQL | 9.2.7 |  |

表 2.3‑4 DB負荷分散サーバ搭載ソフトウェア一覧

| 項番 | 種別 | ソフトウェア名 | バージョン | 備考 |
| --- | --- | --- | --- | --- |
| 1 | OS | CentOS | 6.5 |  |
| 2 | DBレプリケーション | pgpool-Ⅱ | 3.3.2 |  |

### 開発環境

本システムの開発環境について、以下に示す。

表 2.3‑5 開発環境

| 項番 | 種別 | ソフトウェア名 | バージョン | 備考 |
| --- | --- | --- | --- | --- |
| 1 | OS | Windows | 7以降 | ※32bit |
| 2 | 開発言語 | Java | 7 |  |
| 3 | 統合開発環境 | Eclipse | 3.7以上 |  |
| 4 | フレームワーク | Struts | 2.3.28.1  2016/3/28  Strutsのバージョンを変更 |  |

2016/5/16

Strutsのバージョンを変更

2.3.28→2.3.28.1

### 対応ブラウザ

本システムの対応ブラウザは以下の通りである。

なお、Modern UIは保証対象外とする。

・Internet Explorer 11 拡張保護モードOFF（デフォルトではOFF）※

* + - Internet Explorer 10以降では、32bit版と64bit版が統合されており、“拡張保護モード”がOFFの場合は、親プロセスが64bitで動作し、子プロセスである各タブが32bitで動作する。“拡張保護モード”がONの場合は、子プロセスも64bitで動作する。  
      Internet Explorer 8、9とあわせ32bitで動作を確認するため、“拡張保護モード”OFFを対象とする。

対応OSは、以下の通りである。

・Windows 7

・Windows 8.1

・Windows 10

### 文字コード定義

本システムで使用する文字コードを以下に示す。

表 2.3‑6 使用文字コード一覧

| 項番 | サーバ名 | | 使用文字コード | 備考 |
| --- | --- | --- | --- | --- |
| 1 | WEBサーバ | OS | UTF-8 |  |
| WEBアプリケーション | UTF-8 |  |
| 2 | DBサーバ | OS | UTF-8 |  |
| DBMS | UTF-8 |  |

なお、本システムで取り扱うCSVファイルの文字コードについては、[別紙２]ファイル設計書を参照。

## 機能一覧

本システムの機能一覧を以下に示す。

表 2.4‑1 機能一覧

| **項番** | **大項目** | **中項目** | **小項目** | **概要** |
| --- | --- | --- | --- | --- |
|  | SO系機能 | SO通知 | － | 上位装置からのSO通知を受信する機能。 |
|  |  | SO情報取得 | － | 上位装置に対して、SO情報取得を要求する機能。 |
|  |  | 処理結果通知（SO取込） | － | 上位装置に対して、SO取込結果を通知する機能。 |
|  |  | 工事処理 | － | 各SOの工事日にSO処理（内線サーバの設定処理等）を行う機能。  バッチ処理。 |
|  |  | 処理結果通知（工事結果） | － | 上位装置に対して、工事処理結果を通知する機能。 |
|  |  | 内線サーバ設定機能 | － | 内線サーバの設定ファイルを生成、および、内線サーバへ設定ファイルを反映する機能。 ※本機能は、カスコン系機能でも使用する。 |
|  |  | 端末自動設定機能 | － | Asteriskの設定情報からPanasonic端末（KX-UT136N, KX-UT123N）の自動設定用のファイルを作成する。 ※本機能は、カスコン系機能でも使用する。 |
|  |  | スタティックルート設定機能 | － | スタティックルート設定ファイルを生成、および、内線サーバへ設定ファイルを反映する機能。 |
|  |  | パケットフィルタ設定機能 |  | パケットフィルタ設定ファイルを生成、および、内線サーバへ設定ファイルを反映する機能。 |
|  | カスコン系機能 | ログイン機能 | － | ユーザがログイン、ログアウトを行うための機能。  アカウントIDとパスワードの組み合わせにより、不正アクセスを防止する。 |
|  |  | メニュー機能 | － | 各ユーザの権限向けのメニューを表示する機能。 |
|  |  | トップ機能 | － | トップ画面を表示する機能。 |
|  |  | パスワード変更機能 | － | ユーザがパスワードを変更するための機能。 |
|  |  | 初期設定機能 | － | 初期設定時に、内線一覧を表示する機能。 |
|  |  | 着信グループ設定機能 | 着信グループ設定機能(一覧表示) | 着信グループの一覧を表示する機能。 |
|  |  |  | 着信グループ設定機能(追加) | 着信グループを追加する機能。 |
|  |  |  | 着信グループ設定機能(変更) | 着信グループを変更する機能。 |
|  |  |  | 着信グループ設定機能(削除) | 着信グループを削除する機能。 |
|  |  |  | 着信グループ設定機能(設定確認) | 着信グループの設定を表示する機能。 |
|  |  | 外線着信設定機能 | 外線着信設定機能(一覧表示) | 外線着信の一覧を表示する機能。 |
|  |  |  | 外線着信設定機能(追加) | 外線着信を追加する機能。 |
|  |  |  | 外線着信設定機能(変更) | 外線着信を変更する機能。 |
|  |  |  | 外線着信設定機能(削除) | 外線着信を削除する機能。 |
|  |  | 外線発信設定機能 | 外線発信設定機能(一覧表示) | 外線発信の一覧を表示する機能。 |
|  |  |  | 外線発信設定機能(設定) | 外線発信を設定する機能。 |
|  |  | 内線設定機能 | 内線設定機能(一覧表示) | 内線設定の一覧を表示する機能。 |
|  |  |  | 内線設定機能(変更) | 内線設定を変更する機能。 |
|  |  | 発信規制先設定機能 | － | 発信規制先を設定する機能。 |
|  |  | 通話ログ確認機能 | － | 通話ログを表示する機能。 |
|  |  | トラフィックレポート機能 | トラフィックレポート機能(一覧表示) | トラフィックレポートを一覧表示する機能。 |
|  |  |  | トラフィックレポート機能(グラフ化) | トラフィックレポートをグラフ表示する機能。 |
|  |  | PBX設定情報表示機能 | PBX設定情報表示機能(一覧表示) | PBXの設定情報を一覧表示する機能。 |
|  |  |  | PBX設定情報表示機能(詳細表示) | PBXの設定情報を詳細表示する機能。 |
|  |  | 不在時動作設定機能 | － | 不在時動作を設定する機能。 |
|  |  | N番検索機能 | － | N番を検索し一覧表示する機能。  VM残数が閾値を下回った時には、メッセージを表示する。 |
|  |  | 設備管理情報確認機能 | － | 設備管理情報の表示および情報取り込みを行う機能。 |
|  |  | お知らせ設定機能 | － | お知らせを設定する機能。 |
|  |  | アカウント管理機能 | アカウント管理機能(一覧表示) | アカウントを一覧表示する機能。 |
|  |  |  | アカウント管理機能(登録) | アカウントを登録する機能。 |
|  |  |  | アカウント管理機能(ロック解除) | アカウントのロックを解除する機能。 |
|  |  |  | アカウント管理機能(パスワード変更) | アカウントのパスワードを変更する機能。 |
|  |  |  | アカウント管理機能(削除) | アカウントを削除する機能。 |
|  |  | 英語化対応 | － | カスコン画面の英語版の作成と、日本語版と英語版を切り替える機能。 |
|  |  | 統合CP対応 | 利用者権限のフィルタリング | １つのポートでのアクセスでは、１つのユーザ権限でのみ、使用可能とする機能。  ユーザ権限ごとにポートを分け、それぞれTomcatインスタンスを起動する。 |
|  |  |  | シングルサインオン対応 | 統合CPとのシングルサインオンを実現する機能。 |
|  |  | VM支障移転 | － | VM故障時に、故障したVMの内線サーバ情報を他の正常VMに移転する機能。 |
|  |  | VPN移転 | － | インタネット接続用VMからVPN接続可能なVMへ内線サーバ情報を移転する機能。 |
|  |  | ユーザ拠点情報管理機能 | オフィス構築セット情報設定機能(一覧表示) | オフィス構築セット情報の一覧を表示する機能。 |
|  |  |  | オフィス構築セット情報設定機能(追加) | オフィス構築セット情報を追加する機能。 |
|  |  |  | オフィス構築セット情報設定機能(変更) | オフィス構築セット情報を変更する機能。 |
|  |  |  | オフィス構築セット情報設定機能(削除) | オフィス構築セット情報を削除する機能。 |
|  |  |  | オフィス構築セット情報設定機能(設定確認) | オフィス構築セット情報の設定を表示する機能。 |
|  |  | 開通案内随時出力機能 | － | 画面からの操作契機に開通案内ファイルを出力し、上位装置（開通案内WEBシステム）へ送信する機能。 |
|  |  | 内線サーバ設定反映機能 | － | 画面からの操作契機に内線サーバ設定ファイル、端末自動設定ファイルを出力し、内線サーバおよび端末自動設定ファイル配置用WEBサーバへ流通、反映する機能。 |
|  |  | 外線情報検索機能 | － | 画面から外線情報を検索し、表示する機能。 |
|  |  | IP Phone MACアドレス管理機能 | － | IP Phone用のMACアドレス情報の編集、出力を行う機能。 |
|  |  | 保留音設定機能 | － | 保留音の登録と、内線サーバへの保留音ファイルの配置を行う機能。 |
|  |  | 例外機能 | － | システムエラーを表示する機能。 |
|  | 管理系機能 | DBレコード保管機能 | － | DBレコードを定期的にバックアップする機能。 |
|  |  | 通話ログ、トラフィック情報のDBレコード削除機能 | － | 一定期間経過した通話ログ、トラフィック情報のDBレコードを定期的に削除する機能。 |

VM残数の閾値や、アカウントロックするログイン失敗回数などは、アプリケーション設定ファイルにて任意の値を設定できる。

本システムが出力するログレベルやログの出力先などは、ログ設定ファイルで設定できる。

アプリケーション設定ファイル、ログ設定ファイルについては、[別紙２]ファイル設計書を参照。

## 外部システムとの機能分担

### 外部システム一覧

本システムにおける外部システムの一覧を以下に示す。

**表2.5‑1 外部システム一覧**

|  |  |  |
| --- | --- | --- |
| **分類** | **名称** | **概要** |
| 上位装置 | WEBエントリシステム | 本システムに対してSO通知を送信し、本システムがSO情報の取得を要求する先の上位装置。 |
| 上位装置 | 開通案内WEBシステム | 本システムが新規SO情報を設定した後に、開通案内情報を送付する、送付先の上位装置。  開案WEBシステムと表記する場合もある。 |
| 内線サーバ | Asterisk | 本システムで登録/変更/削除した内線設定が反映されるサーバ。 |
| バックアップサーバ | DBバックアップサーバ | DBデータをバックアップする保存先のサーバ。 |
| WEBサーバ | 端末自動設定ファイル配置用WEBサーバ | 本システムで生成した端末自動設定ファイルを配置する先のサーバ。 |

### 外部インタフェース一覧

本システムと外部システム間のインタフェースの一覧を以下に示す。

**表2.5‑2 外部インタフェース一覧**

|  |  |  |
| --- | --- | --- |
| **外部システム** | **インタフェースプロトコル** | **概要** |
| WEBエントリシステム | REST | 本システムへのSO通知や、本システムが実施するSO情報取得など、REST通信にて要求/応答を行う。 |
| 開通案内WEBシステム | FTP | 開通案内情報（CSVファイル）を開通案内WEBシステムにFTPにてアップロードする。 |
| 内線サーバ | SFTP  AMI | 本システムが作成した内線設定ファイルをSFTPで内線サーバにアップロードした後、AMIにて設定リロードを実行する。 |
| 端末自動設定ファイル配置用WEBサーバ | SFTP | 本システムが作成した端末自動設定ファイルをSFTPで配置する。 |

# システム設計方針

## 機能性方針

■適切さ

* + 機能設計書にて記載する全機能を具備する。
  + 無効な操作等においては、[別紙４]メッセージ・ログ設計書に記載したメッセージを出力する。
  + データ間の矛盾を防止するため、トランザクションを考慮する。

■正確性

* + 該当ユーザを収容する内線サーバ以外の設定が行えない。
  + 処理失敗時にはDBへのデータ反映は行わず、ロールバックにより処理前の状態に戻る。
  + SO処理およびユーザ操作による更新処理（新規、変更、削除）については、実行したSQL文をログに出力する。
  + SO処理およびユーザ操作による参照処理については、エラー発生時のみ、実行したSQL文をログに出力する。

■相互運用性

* + DBテーブルに各内線サーバ（Asterisk）のバージョン情報を保持するカラムを用意し、今後、異なるバージョンでの運用が必要になった時に備える。  
    ※本Stepではバージョン情報を保持するのみ。

■セキュリティ

* + セキュリティに関しては、3.6 セキュリティ方針 を参照。

■機能性関連適法性

* + 特に考慮しない。

## 信頼性方針

■成熟度

* + UT、DB1、DB2を実施する。

■フォールトトレランス

* + WEBサーバについては、BHECのロードバランサを使用し、冗長化を行う。
  + DBサーバについては、DBの冗長化ミドルウェアを使用し、冗長化を行う。
  + DB内の全データのバックアップを定期的に行う機能（6.1 DBレコード保管機能 を参照）を具備する。

■復元力

* + リカバリ時には、運用にて対処する。  
    リカバリ時の主な手順は以下の通りである。  
    　１．定期バックアップからのリカバリを実施。  
    　２．定期バックアップ以降のSOの再実施。  
    　３．定期バックアップ以降のカスコン画面のログから、DBの更新処理のSQL文を取得し、手動実行。

■信頼性関連適法性

* + 特に考慮しない。

## 使用性方針

■理解のしやすさ

* + 設定不備等の時には、[別紙４]メッセージ・ログ設計書に記載したメッセージを出力する。
  + インストールが容易に行える設計とする。

■学習のしやすさ

* + 特に考慮しない。

■操作のしやすさ

* + [別紙１]画面設計書 の画面設計方針を参照。

■魅力

* + 特に考慮しない。

■使用性関連適法性

* + メジャーなOSSを利用することで、開発停止や致命的なバグFIXが行われない等の問題発生の可能性を軽減する。

## 保守性方針

■分析のしやすさ

* + [別紙４]メッセージ・ログ設計書に記載したメッセージをログに出力する。
  + ログの出力にはTRACE、DEBUG、INFO、WARN、ERROR、FATALの6段階のレベルを設ける。  
    通常はINFO以上のログを出力するが、より詳細な情報はDEBUGで出力可能とする。  
    TRACEは試験時のみに使用する。  
    レベルの変更は設定ファイルの変更で可能とする。(反映にはアプリケーションの再起動が必要)

■変更のしやすさ

* + システム無停止でのバージョンアップを可能とする。  
    安全を考慮し、通常は利用が少ない時間帯に行うことを想定する。  
    なお、使用しているミドルウェアにも影響する変更の場合は、システム全体を一時的に停止する必要がある。

■安定性

* + DB2にて、長期安定化試験を実施する。

■試験のしやすさ

* + DB1/DB2用の試験環境を構築する。

■維持管理性

* + 構成ソフトウェアとそのバージョンを、本書に記載する。

## 可搬性方針

■順応性

* + 対応WEBブラウザを本書に明記する。

■インストールのしやすさ

* + インストールが容易に行える設計とする。

■共存力

* + 本システムが必要とするサーバ以外とは通信を行わない。

■置換性

* + 特に考慮しない。

■可搬性関連適法性

* + 特に考慮しない。

## セキュリティ方針

### 特殊文字対策

画面から入力された文字列に特殊文字が含まれていた場合、その文字列を空文字扱いとする。本システムが画面入力に対して対応する文字列を以下に示す。

**表3.6‑1 HTMLおよびSQLの特殊文字**

|  |  |
| --- | --- |
| **種別** | **内容** |
| HTMLの特殊文字 | 「<」、「>」、「&」、「"」、「'」 |
| SQLの特殊文字 | 「'」、「\」、「:」、「|」、「;」、「--」、「/\*」、「\*/」 |

WEBアプリケーションに対する攻撃の大半は使用言語、プロトコルの仕様、および、DBにとって特別な意味を持つ文字(特殊文字)の扱いによるものである。例えば次のような攻撃が挙げられる。

* SQLインジェクション
* クロスサイドスクリプティング
* OSコマンドインジェクション
* HTTPヘッダインジェクション

一般的には特殊文字を単なる文字に変換するサニタイジング(無害化)を行うが、それだけでは防げない攻撃も存在し対策としては不十分であるため、本システムでは前述のセキュリティ対策を行う。

ただし、上記は不特定多数のユーザに対するセキュリティ上の対策であり、システム管理者(オペレータ)に対しては不要のため、システム管理者の専用画面では本方針の適用は任意とする。

### 不正アクセス対策

本システム以外も含めたWebサイトにスクリプトや自動転送を仕込み、そのWebサイトへアクセスしたユーザが意図せず本システムの画面操作を行ってしまうクロスサイトリクエストフォージェリ(CSRF)という攻撃が存在する。

本システムでは画面表示時にCookieにランダムな文字列を払出し、画面遷移等の操作実行時に払いだされた値と同一であるかを確認することで、アクセスの一貫性を確認する対策を行う。

## 性能方針

### 性能目標

BHECのVMについて、最小構成（1CPU、メモリ1GB、ストレージ10GB）で簡易なサンプルWEBアプリケーションにて性能測定を行った。

性能測定では、ミドルウェアにはJDK7、Tomcat7を使用し、外部からのリクエストを受け付けるのみの性能測定用の簡易なサンプルWEBアプリケーションを用意した。ディスクI/Oを使用しない条件で、最大負荷(CPU使用率が100%)に達するまで受け付けられるリクエスト数を計測したところ、計測結果は秒間1000スループットであった。

実際のシステムでは、今回のサンプルWEBアプリケーションよりも複雑な処理を行うため、この測定結果通りの性能が出ない可能性があるが、アプリケーションのチューニングやBHECのVMリソースの拡充などにより、性能向上を図る。

### 性能実現方針

WEBアプリケーションのチューニングと運用環境の設計で対応する。

WEBアプリケーションは、性能劣化を招く可能性がある処理(文字列を複数"+"で連結する等)をコードレビュー時に改善する。

運用環境は次の方法で改善を行う。

1. WEBサーバとDBサーバの負荷分散

WEBサーバの負荷分散にはBHECのロードバランサを使用し、DBサーバの負荷分散にはpgpool-Ⅱを使用する。

1. VMリソースのスペックをアップグレードする

VMのマシン構成は変更が可能であるため、必要に応じてスペックを変更することで対応する。

変更可能かつ性能に影響するのはCPUとメモリである。

図 3.7‑1 運用環境イメージ

# SO系機能

※SO系機能については、[別紙５]対向装置通信処理仕様書 を参照。

# カスコン系機能

※カスコン系機能については、[別紙１]画面設計書 を参照。

# 管理系機能

## DBレコード保管機能

PostgreSQLのpg\_dumpコマンドを使用してDBデータのバックアップを行う。ファイル名の形式は”pg\_dump\_YYYYMMDD.sql.gz”(YYYYは年、MMは月、DDは日を表す)であり、ディスクスペース節約のためgzipで圧縮する。

具体的には次のコマンドを実行する

|  |
| --- |
| $ pg\_dump 「DB名」 -h 「pgpool-Ⅱホスト」 -p 「pgpool-Ⅱポート番号」 -U 「DBユーザ」 | gzip -c > pg\_dump\_"`date '+%Y%m%d'`".sql.gz" |

定期的な実行にはcronを用い、世代管理を行う。管理する世代は変更可能とする。バックアップファイルはバックアップごとに古いファイルから削除される。

|  |
| --- |
| **実行イメージ**  **(5世代管理かつ1日1回バックアップする例)**  **~~pg\_dump\_20130801.sql.gz~~** ←　削除  **pg\_dump\_20130802.sql.gz**  **pg\_dump\_20130803.sql.gz**  **pg\_dump\_20130804.sql.gz**  **pg\_dump\_20130805.sql.gz**  **pg\_dump\_20130806.sql.gz** ←新規生成 |

pg\_dumpコマンドに指定するバックアップ先サーバのアドレスにはDBクラスタサーバ(pgpool-Ⅱ)の仮想アドレスを使用することにより、DBノードまたはDBクラスタサーバが全損しない限りバックアップを正常に行えるようにする。

バックアップを実施するサーバとDBサーバの負荷および障害対策を考慮し、バックアップ専用のサーバを用意することが望ましい。

図 6.1‑1 DBバックアップ環境イメージ

## 通話ログ、トラフィック情報のDBレコード削除機能

※通話ログ、トラフィック情報のDBレコード削除機能については、[別紙５]対向装置通信処理仕様書 [CDRログ収集アプリケーション（概要）]シート、[トラフィックログ収集アプリケーション（概要）]シートを参照。