A-SaaS サービス サービスレベル指標一覧

第1版(2010年9月1日)

アカウンティング・サース・ジャパン株式会社

◆アプリケーション運用

種別	サービスレベル項目	項目説明	内容
可用性	サービス時間	サービスを提供する時間帯	24時間365日 (計画停止／定期保守を除く)
	計画停止予定通知	定期的な保守停止に関する事前連絡確認	14日前にメール／ホームページで通知
	サービス稼働率	サービスを利用できる確率((計画サービス時間－停止時間)÷計画サービス時間)	99.8%以上(停止時間の目標値:年間10時間以内)
	サービス継続のため対策	サービスをダウンさせず、継続するためのハードウェアの多重化等	データベースサーバー、アプリケーションサーバー、電源等を冗長化済、様々な障害時にもサービスを継続
	重大障害時の代替手段	早期復旧が不可能な場合の代替措置	代替サーバーで継続利用可能
	アップグレード方針	バージョンアップ／変更管理／パッチ管理の方針	お客様のインストールを伴うバージョンアップは年1回程度、軽微なバージョンアップはその都度実施

◆サービスレベル

種別	サービスレベル項目	項目説明	内容
信頼性	平均復旧時間	障害発生から修理完了までの平均時間 (修理時間の和÷故障回数)	8時間以内(縮退運転によりサービス継続可能) ※インフラレベルでの復旧時間
	システム監視基準	システム監視基準(監視内容／監視・通知基準)の設定に基づく監視	常時ハードウェア／ネットワーク／パフォーマンス/リソースの監視を行う(詳細な監視項目は個々に設定)
	障害通知プロセス	障害発生時の連絡プロセス(通知先／方法／経路)	指定された緊急連絡先にメール／電話で連絡し、併せてホームページで通知
	障害通知時間	異常検出後に指定された連絡先に通知するまでの時間	3時間以内
	障害監視間隔	障害インシデントを収集／集計する時間間隔	5分
	サービス提供状況の報告方法／間	サービス提供状況を報告する方法／時間間隔	月に一度ホームページ上で公開報告
	ログの取得	利用者に提供可能なログの種類	不正アクセス対策のためにアクセスログを監視、ユーザー要望により提供予
性能	オンライン応答時間	オンライン処理の応答時間	平均応答時間3秒以内(データセンター内)
拡張性	カスタマイズ性	カスタマイズ(変更)が可能な事項／範囲／仕様等の条件とカスタマイズに必要な情報	利用画面上の項目配置変更など
	同時接続利用者数	オンラインの利用者が同時に接続してサービスを利用可能なユーザ数	全利用会員の申請使用ID数のすべて

◆サポート

サービスレベル項目	項目説明	内容
サービス提供時間帯(一般問合せ)	一般問合せ時の問合せ受付業務を実施する時間帯	9時～12時、13時～17時(電話) (年末年始・土日・祝祭日を除く) 24時間365日(メール)
サービス提供時間帯(障害対応)	障害対応時の問合せ受付業務を実施する時間	24時間365日(電話)

◆データ管理

サービスレベル項目	項目説明	内容
バックアップの方法	バックアップ内容（回数、復旧方法など）、データ保管場所／形式、利用者のデータへのアクセス権など、利用者に所有権のあるデータの取扱方法	有 （常時クラスタリングでデータ多重化。1日1回データセンタ内でバックアップ保管。アクセス権はシステム管理者のみ。） （復旧／利用者への公開の方法は別途規定）
バックアップデータの保存期間	データをバックアップした媒体を保管する期限	7年間
データ消去の要件	契約終了後の、データ消去の実施有無	サービス解約後1ヶ月以内にデータを破棄
契約終了時のデータ返却	契約終了時のユーザーデータの返却	ユーザー自身によるローカル環境へのバックアップ CSV、XML等汎用形式での取得も可能とする予定

◆セキュリティ

サービスレベル項目	項目説明	内容
なりすまし対策	第三者による利用者を装ったなりすましに関する対策	・ユーザID、パスワードによるログイン認証により不正なアクセスを防止、指紋認証も利用可能 ・A-SaaSサービスに接続された端末とユーザーの組み合わせをサーバー側で記録し、通常ではないアクセスを把握して、なりすましなど不正アクセスを防止(開発予定) ・SSL証明書により通信を暗号化、ウェブサイトの正常性を確保する ・サーバはセキュリティ制限をかけたIDC内に設置し、第三者から保護する
データ盗聴防止	データへの不正なアクセスによる盗聴に対する対策	・ファイアーウォールを設置し、外部からの盗聴を防止する ・利用可能ユーザ、利用可能ポートを限定し、外部からの進入を防止
データ改ざん防止	データへの不正なアクセスによるデータ改ざんに対する対策	・IDパスワードによる認証、アクセスコントロールリストを使用し、データ改ざんを防止 ・ベリサインSSLサーバ証明書にてサーバのセキュリティを確保
動作妨害	不正なアクセスによるサービスの妨害に対する対策	・ファイアーウォールによりDos攻撃を防止 ・ネットワーク監視により管理者に警告
脆弱性対策	システムに脆弱性が発見された場合の対策	・アプリケーション、ファームウェアの脆弱性が発表された場合には、早期にセキュリティパッチを導入し脅威に対する予防を行う。 （緊急パッチに関しては1ヶ月以内、その他は調査後半年以内）
ウィルス対策	コンピュータウィルスに対する対策	・ウィルス対策ソフトウェアを導入し、ウィルスの進入/蔓延を防止 ・ウィルス検出に関しては運用管理者により警告を実施
通信の暗号化レベル	システムとやりとりされる通信の暗号化強度。	SSL3.0 ベリサイングローバルIDEV（暗号化強度最短128bit、最長256bit） ベリサインセキュアID（暗号化強度最短40bit、最長256bit）
公的認証取得状況	JIPDECやJQA等で認定している情報処理管理に関する公的認証（ISMS、プライバシーマーク等）の取得状況。	プライバシーマーク取得準備中
情報取扱者の制限	利用者のデータにアクセスできる利用者が限定されていること。	有（通常は一切アクセスできない設定。利用者の承諾を受けてアクセスする場合に利用者のデータにアクセスできる社員等はセキュリティ管理者の許可を得た者に限る。）
情報取扱い環境	提供者側でのデータ取扱環境が適切に確保されていること。	有（データはセキュリティチェックのあるIDC内に保管。社内保管のバックアップは金庫内に保管。利用者は限定）

◆サーバ設置場所

種別	サービスレベル項目	項目説明	内容
施設建築物	建物形態	データセンター専用建物か否か	併用型。データセンター利用目的に改装。
	所在地	国名（日本の場合は地域ブロック名（例：関東、東北）	関東
	耐震・免震構造	耐震数値	SRC耐震構造（新耐震基準） 300gal～400gal
非常用電源設備	無停電電源	無停電電源装置（UPS）の有無と、UPSがある場合は電力供給時間	UPS有N+1構成 3,500KVAの負荷に対して10分間の電力供給
	非常用電源	非常用電源（自家発電機）の有無と、非常用電源がある場合は連続稼働時間の数値	有 自家発電機による電源供給により約36時間の連続稼働可能
消火設備	サーバルーム内消火設備	自動消火設備の有無と、ある場合はガス系消火設備か否か	有 不活性ガス（アルゴナイト）消化設備
	火災感知・報知システム	火災検知システムの有無	有
避雷対策設備	直撃雷対策	直撃雷対策の有無	有
	誘導雷対策	誘導雷対策の有無と、対策がある場合は最大対応電圧の数値	設計上に誘導雷耐対策をしており対応
空調設備	十分な空調設備	空調設備（床吹き上げ空調、コンピュータ専用個別空調等）の内容	床下吹き出し方式
サービス保証・継続	サービスダウンしない仕組み	サービスが停止しない仕組み（冗長化、負荷分散等）	冗長化、負荷分散、自家発電装置、UPS
サービス通知・報告	障害・災害発生時の通知	障害発生時通知の有無	有

◆セキュリティ（サーバ設置場所）

サービスレベル項目	項目説明	内容
入退館管理等	入退室記録の有無	有
	監視カメラの有無と、カメラがある場合は監視カメラ稼働時間、監視カメラの監視範囲、映像の保存期間	有り 稼働時間：24時間365日 監視範囲：データセンター内（ｻｰﾊﾞﾙｰﾑ、通路、ｴﾚﾍﾞｰﾀ他、入口、建物外周等）
	個人認証システムの有無	有
媒体の保管	紙、磁気テープ、光メディア等の媒体の保管のための鍵付きキャビネットの有無	有
	保管管理手順書の有無	有
管理者認証	サーバ運用側（サービス提供側）の管理者権限の登録・登録削除の正式な手順の有無	有
その他セキュリティ対策	その他特筆すべきセキュリティ対策を記述（破壊侵入防止対策、防犯監視対策等）	オペレーションルーム：虹彩認証 サーバルーム前室：共連防止： エレベータ：ICｶｰﾄﾞとの連携（登録階の利用制限）
IDC運営事業者の公的認証取得状況	JIPDECやJQA等で認定している情報処理管理に関する公的認証（ISMS、プライバシーマーク等）の取得	Pマーク取得 ISMS27001取得