【経済産業省】クラウドサービスレベルのチェックリスト

対象サービス：Active! gate SS

No.	種別	サービスレベル項目	規定内容	測定単位	対応/可否	備考
アプリケーション運用						
1	可用性	サービス時間	サービスを提供する時間帯（設備やネットワーク等の点検／保守のための計画停止時間の記述を含む）	時間帯	24時間365日 （計画停止/定期保守等を除く）	
2		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（事前通知のタイミング／方法の記述を含む）	有無	【有】 2週間前までに障害・メンテナンス告知サイトにて連絡いたします。 緊急メンテナンスについてはその限りではありません。	https://notice.qualitia.com/
3		サービス提供終了時の事前通知	サービス提供を終了する場合の事前連絡確認（事前通知のタイミング／方法の記述を含む）	有無	【有】 現時点でサービス終了予定はありませんが、2か月前までに報告いたします。 但し、当社が緊急と判断した場合はこの限りではございません。	
4		突然のサービス提供停止に対する対処	プログラムや、システム環境の各種設定データの預託等の措置の有無	有無	【無】 プログラムの預託措置はありません。	
5		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）	稼働率（%）	サービス利用約款にてSLAを記載しています。	
6		ディザスタリカバリ	災害発生時のシステム復旧／サポート体制	有無	【無】 現時点では災害発生時のDR拠点はございません。 なお、早期復旧が困難な場合、本サービスとの連携解除手順をご案内いたします。	
7		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	有無	【有】 早期復旧が不可能と判断した場合、本サービスとの連携解除手順をご案内いたします。	
8		代替措置で提供するデータ形式	代替措置で提供されるデータ形式の定義を記述	有無 （ファイル形式）	【無】 メールゲートウェイサービスのため、データの代替提供はありません。	
9		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	有無	【有】 年数回の頻度でバージョンアップを行っております。 また適切に変更・パッチ管理しております。	
10	信頼性	平均復旧時間（MTTR）	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）	時間	障害内容により異なるため、明示できません。 障害発生から6時間以内の復旧を目標としております。 （物理的な多重障害の場合はこの限りではございません）	
11		目標復旧時間（RTO）	障害発生後のサービス提供の再開に関して設定された目標時間	時間	同上	
12		障害発生件数	1年間に発生した障害件数／1年間に発生した対応に長時間（1日以上）要した障害件数	回	過去1年間に1日以上の停止を伴う 長期間の障害は発生しておりません。	
13		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	有無	【有】 各種ハードウェア、及びアプリケーション等の監視を行っております。 詳細については、セキュリティ上非公開とさせていただきます。	
14		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）	有無	【有】 当社障害・メンテナンス告知サイト、及びメールにて告知いたします。	https://notice.qualitia.com/
15		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	時間	障害発生後40分以内での通知を目標としております。	
16		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	時間（分）	障害はリアルタイムで監視しております。	
17		サービス提供状況の報告方法／間隔	サービス提供状況を報告する方法／時間間隔	時間	通常稼働時のサービス提供状況の報告は承っておりません。	
18		ログの取得	利用者に提供可能なログの種類（アクセスログ、操作ログ、エラーログ等）	有無	【無】 ログを基に当社にて調査した結果をご案内いたします。 ログイン履歴についてはサービス画面から参照が可能です。 詳細はマニュアルをご確認ください。	
19	性能	応答時間	処理の応答時間	時間（秒）	詳細については、セキュリティ上非公開とさせていただきます。	
20		遅延	処理の応答時間の遅延継続時間	時間（秒）	詳細については、セキュリティ上非公開とさせていただきます。	
21		バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	詳細については、セキュリティ上非公開とさせていただきます。	
22	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	有無	【有】 保留ポリシーをはじめとした各種ポリシー等を設定いただけます。 アプリケーション自体の機能カスタマイズは承っていません。	詳しくは本サービスの 管理者マニュアルをご覧ください。
23		外部接続性	既存システムや他のクラウド・コンピューティング・サービス等の外部のシステムとの接続仕様（API、開発言語等）	有無	【有】 ユーザ専用の画面については、SAML2.0規格のシングルサインオンがご利用いただけます。	
24		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	有無 （制約条件）	【有】 本サービスを利用可能なユーザ数は契約により異なります。	
25		提供リソースの上限	ディスク容量の上限／ページビューの上限	処理能力	詳細については、セキュリティ上非公開とさせていただきます。	
サポート						
26	サポート	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帯	時間帯	障害時専用緊急連絡 24時間365日 電話にて受け付けております。 ※通常のお問合せには対応しておりません	
27		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	時間帯	当社営業時間 平日10:00～17:00 メール/電話にて受け付けております。 （年末年始・土日・祝祭日を除く）	
データ管理						
28	データ管理	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	有無/内容	【有】 システム保全を目的としたバックアップを日次7世代で取得しております。 またデータ領域のバックアップは、サービスが稼働している環境とは異なる拠点に保管しております。 なお、利用者要望によるリストアは承っておりません。	
29		バックアップデータを取得するタイミング（RPO）	バックアップデータをとり、データを保証する時点	時間	前日分	
30		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	時間	7日間	
31		データ消去の要件	サービス解約後の、データ消去の実施有無／タイミング、保管媒体の破棄の実施有無／タイミング、およびデータ移行など、利用者に所有権のあるデータの消去方法	有無	【有】 サービス利用約款に従いデータを論理消去いたします。 個別の消去証明書の発行は承っておりません。	
32		バックアップ世代数	保証する世代数	世代数	7世代	
33		データ保護のための暗号化要件	データを保護するにあたり、暗号化要件の有無	有無	【有】	
34		マルチテナントストレージにおけるキー管理要件	マルチテナントストレージのキー管理要件の有無、内容	有無／内容	【無】 マルチテナントストレージを使用していません。	

35		データ漏洩・破壊時の補償／保険	データ漏洩・破壊時の補償／保険の有無	有無	【有】 当社が取得した機密情報等を漏洩、破壊した際は、最大で当該事故発生日から過去1年間に当社が受領した料金の範囲で賠償いたします。 詳細は本サービスの利用約款をご確認ください。	
36		解約時のデータポータビリティ	解約時、元データが完全な形で迅速に返却される、もしくは責任を持ってデータを消去する体制を整えており、外部への漏洩の懸念のない状態が構築できていること	有無／内容	【有】 サービス利用約款に従いデータを論理消去いたします。 データの返却は承っておりません。 また、本番環境へのアクセスは社内の限られたメンバーのみ許可されています。	
37		預託データの整合性検証作業	データの整合性を検証する手法が実装され、検証報告の確認作業が行われていること	有無	【有】	
38		入力データ形式の制限機能	入力データ形式の制限機能の有無	有無	【有】	
セキュリティ						
39		公的認証取得の要件	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）が取得されていること	有無	【有】 以下の認証を取得し、運営しております。 ISO/IEC 27001（情報セキュリティマネジメントシステム：IS 586579） ISO/IEC 27017（ISMSクラウドセキュリティ認証：CLOUD 681574） ISO/IEC 27018（パブリッククラウド上の個人情報保護：PII 681575） ISO/IEC 27701（プライバシー情報マネージメントシステム：PM 757678）	
40		アプリケーションに関する第三者評価	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていること	有無/実施状況	【有】 アプリケーションは外部ツール、ネットワーク等のインフラについては年に1度第三者機関による脆弱性診断を受けております。 なお、具体的なツール名・機関の名称等はセキュリティ上非公開とさせていただきます。	
41		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	有無	【有】	
42	セキュリティ	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	有無	【有】 TLS1.2に対応しています。	
43		会計監査報告書における情報セキュリティ関連事項の確認	会計監査報告書における情報セキュリティ関連事項の監査時に、担当者へ以下の資料を提供する旨 「最新のSAS70Type2監査報告書」 「最新の18号監査報告書	有無	【無】 左記の監査は実施していません。 項番39の認証を取得し、運営しています。	
44		マルチテナント下でのセキュリティ対策	異なる利用企業間の情報隔離、障害等の影響の局所化	有無	【有】 顧客毎に隔離されています。	
45		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 利用者組織にて規定しているアクセス制限と同様な制約が実現できていること	有無/設定状況	【有】 管理者権限/一般ユーザー権限を設けております。 詳細はマニュアルをご参照ください。	
46		セキュリティインシデント発生時のトレーサビリティ	IDの付与単位、IDをログ検索に利用できるか、ログの保存期間は適切な期間が確保されており、利用者の必要に応じて、受容可能に期間内に提供されるか	設定状況	IDは顧客毎に付与 ID及びメールアドレスにて追跡可能です。 ログは3年間保管しており、ログからの調査が可能です。	
47		ウィルススキャン	ウィルススキャンの頻度	頻度	全ての従業員の端末にはウイルス対策ソフトが導入されており、常時スキャンが実施されております。 また、サーバー上ではメール送信時にスキャンを行っています。	
48		二次記憶媒体の安全性対策	バックアップメディア等では、常に暗号化した状態で保管していること、廃棄の際にはデータの完全な抹消を実施し、また検証していること、USBポートを無効化しデータの吸い出しの制限等の対策を講じていること	有無	【有】 二次記憶媒体へ利用者のデータを保存することはありません。	
49		データの外部保存方針	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握しているか	把握状況	把握しております。 なお、データの保管国は日本国内で、諸外国に保管することはありません。	