クラウドサービスレベルのチェックシート

No.	種別	サービスレベル項目	質問内容	回答
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についてお答えください。 (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)	24時間365日です。
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はどのような仕様ですか？ (事前通知のタイミング/方法の記述を含む)	2週間前迄にメールもしくは本サービス等のウェブサイトで通知します。
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はどのような仕様ですか？ (事前通知のタイミング/方法の記述を含む)	90日前までにメールもしくは本サービス等のウェブサイトで通知します。
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についてお答えください。	第三者の預託等の措置は実施していません。
5		サービス稼働率	サービス稼働率についてお答えください。((計画サービス時間-停止時間)÷計画サービス時間)	99.9%を下回らないことを目標に運用しています。
6		ディザスタリカバリ	災害発生時のシステム復旧/サポート体制についてお答えください。	冗長化しておりますが、詳細は非公開とさせていただきます。
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についてお答えください。	バックアップデータの提供は行っておりません。日常的にお客様にて①Excel形式でのデータ取得、②バックアップの保存をお願いしています。
8		代替措置で提供するデータ形式	トラブル時における弊社提供データの取得形式についてお答えください。	同上
9		アップグレード方針	バージョンアップ/変更管理/パッチ管理の方針についてお答えください。	年に複数回のバージョンアップを実施しています。
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についてお答えください。(修理時間の和÷故障回数)	サービスレベル目標では6時間以内としていますが、実績は公開しておりません。
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についてお答えください。	公開しておりません。
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)要した障害件数についてお答えください。	サービス稼働実績をご確認ください https://pr.asset-force.com/support/availability/
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についてお答えください。	・運用保守監視のシステム運用ではAWS Client VPN(インターネットVPN))に加え、多要素認証(AWS-MFA仮想デバイス)を利用しています。
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)についてお答えください。	平日9時~17時の場合、速やかに指定された連絡先にメール或いはお電話で通知（土日祝日等の休日を除く）もしくはサービス内の「お知らせ」メニューからの通知となります。
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についてお答えください。	速やかに通知します。
16		障害監視間隔	障害インシデントを収集/集計する時間間隔についてお答えください。	5分間隔で実施しています。
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/時間間隔についてお答えください。	月に一度、プロダクトサイト上で公開しています。 https://pr.asset-force.com/support/availability/
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)についてお答えください。	各種ログは1年間を目途に保管していますが、お客様への提供はお約束していません。
19	性能	応答時間	処理の応答時間についてご回答下さい。	非公開となります。
20		遅延	処理の応答時間の遅延継続時間についてご回答下さい。	非公開となります。
21		バッチ処理時間	バッチ処理(一括処理)の応答時間についてご回答下さい。	処理内容に大きく依存するため非公開としています。
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についてご回答下さい。	管理項目の追加、削除、変更等が設定画面から可能です。
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)についてご回答下さい。	ご要望を頂いたお客様に対してAPIを公開しています。JSON形式でのデータ授受に対応しています。
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についてご回答下さい。	特に上限は設定しておりません。
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についてご回答下さい。	ディスク容量はご利用の契約の種類ごとに異なります。 ページビューの上限は定めておりません。
サポート				
26	サポート	サービス提供時間帯(障害対応)	障害対応受付業務の時間帯についてご回答下さい。	メール受付：24時間365日 ※メールの回答は平日9~17時に限る ※土日・年末年始を除く
27		サービス提供時間帯(一般問合せ)	一般問合せ受付業務の時間帯についてご回答下さい。	メール受付：24時間365日 ※メールの回答は平日9~17時に限る ※土日・年末年始を除く
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についてご回答下さい。	バックアップは行っておりますが、詳細は非公開とさせていただきます。
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についてご回答下さい。	バックアップは取得しておりますが、データの保証は行っておりません。
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についてご回答下さい。	媒体による持ち出しやデータの移動はありません。
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についてご回答下さい。	一定期間経過後に弊社の判断でデータを削除いたします。削除通知は行っておりません。
32		バックアップ世代数	保証する世代数についてご回答下さい。	非公開となりますが、複数世代の保管は実施しています。
33		データ保護のための暗号化要件	保管データ及び、格納データを暗号化していますか？	データ暗号化を実施しています。
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についてご回答下さい。	手順を定め管理を実施しています。 詳細は非公開とさせてください。
35		データ漏えい・破壊時の補償/保険	データ漏えい・破壊時の補償/保険についてご回答下さい。	債務不履行責任、不法行為責任、その他法律上の請求原因の如何を問わず、本サービス等またはサービス利用契約に関して、当社がお客様に対して負う損害賠償責任の範囲は、当社の責に帰すべき事由または当社がサービス利用契約に違反したことが原因でお客様に発生した損害に限定され、損害賠償の額は、本サービスの利用料金の１か月分を上限としています。
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が整備され、外部への漏洩の懸念のない状態が構築できていますか？	データの返却対応は行っておりません。お客様側でのデータエクスポートをお願いしています. 解約後1か月以内にすべてのデータを物理削除します。
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、検証報告の確認が行われていますか？	検証手法を実装し、検証報告の確認を行っています。
38		入力データ形式の制限機能	入力データ形式の制限、誤謬機能はありますか？	ありません。
セキュリティ				
39	セキュリティ	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)を取得していますか？	本番環境を所管する運用チームがISMS認証を取得しています。
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ますか？	リリースの都度、OWASP ASVSベースで第三者によるセキュリティ診断を実施しています。
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ますか？	暗号化は導入済みです。 詳細は非公開とさせてください。
42		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についてご回答下さい。	TLS1.2です
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」	無
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についてご回答下さい。	お客様ごとにテナントを分離しています。
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ますか？	お客様からの依頼がある場合を除いてお客様データへのアクセスは原則禁止となっています。また、利用者のデータへのアクセスは、管理者権限を有するユーザーに限定しています。 全てのアクセスは承認のもと、規定の教育を完了した者だけが実施します。
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可能ですか？	メールアドレス単位でのID発行となります。ログはお客様に提供しておりません。
47		ウイルススキャン	ウイルススキャンの頻度についてご回答下さい。	常時実施となっています。
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ますか？	AWS　SaaS 利用のため物理機器の所管はありません。
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ますか？	データ保管場所は、国内のみのため、国内法律に準拠し運用しています。