desknet'sクラウド　クラウドサービスレベルチェックリスト

設問項目は、「クラウドサービスレベルのチェックリスト」（経済産業省）に準拠しています。

2021/4/1 提示

No.	種別	サービスレベル項目別	規定内容	測定単位	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 （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週間前までにメール、ウェブサイトで通知
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 2ヶ月前までにメール、ウェブサイトで通知2
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	現時点ではサービス停止時の第三者へのデータ預託等の措置は定められておりません。
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（%）	SLA：９９% 過去実績値 2018年度　99.991% 2019年度　99.998% 2020年度　99.999%
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	有 別ロケーションへにてバックアップデータから復旧を行います。 ６時間以内に復旧が見込める場合は、 復旧作業を優先し、２４時間以上障害が継続する可能性があると判断した場合にシステムの切り替えを実施する体制なっております。 また、サービス約款に定める通り、災害に起因する障害に関しては損害賠償の対象となりません。
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 DRサイトにてバックアップデータから復旧を行います。 なお、アプリケーション上で登録データのCSVダウンロードが可能です。
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）	アプリケーション上で登録データCSVダウンロードが可能です。
9		アップグレード方針	バージョンアップ／変更管理／パッチ処理の方針	有無	有 実施頻度：年１－２回 告知：２週間以上まえ 影響範囲：アップデート内容により異なりますが、約30-１時間の停止が伴います。
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 （修理時間の和÷故障回数）	時間	障害内容により復旧時間が異なりますが、およそ30-2時間ほどとなります。
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	障害内容により復旧時間が異なるため、RTOは設けておりません。
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	回	なし
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 システム監視：24時間365日 監視内容：ハードウェア、ネットワーク、システムパフォーマンス、サーバリソース　など
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 障害発生時は担当者にアラートが通知されます。 お客様へはメール、ウェブサイト、電話等で報告いたします。
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	時間	通常15-30分ほどで通知いたします。 ※弊社営業時間外の場合は、翌営業日に通知する場合があります。
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）	5分間隔で監視しています。
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	時間	障害発生時のみ当社ウェブサイトへ都度掲載いたします。
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）	時間	アプリケーション操作ログは機能にて実装しており、お客様側よりご確認いただけます。 ※システムやネットワーク等のログ提供は行っておりません。
19	性能	応答時間	処理の応答時間	時間（秒）	データ登録、検索等のアプリケーション上の通常操作は3秒以内 ※データ量により応答が遅延する場合もあります。
20		遅延	処理の応答時間の遅延継続時間	時間（分）	データセンタ内の応答時間が3秒以上となる遅延の継続時間が1時間以内 ※データ量により応答が遅延する場合は除く
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）	およそ1-2時間 ※データ量により異なります
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 ログイン画面やポータルコンテンツなどアプリケーション上の仕様範囲での画面変更は可能 ※製品仕様を変更するカスタマイズは不可
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 一部機能にて提供
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）	同時利用者数に制限はありません。 ※クラウド上の共用サーバで稼動しているため、過度な負荷が発生する際は環境移設等メンテナンスを実施する場合があります。
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	1TB ※ご契約に応じて上限が異なります
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	営業時間内（電話・メール） 月～金曜日(※祝日を除く) 9:00～12:00、13:00～17:30

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	営業時間内（電話・メール） 月～金曜日(※祝日を除く) 9:00～12:00、13:00～17:30
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 日次で差分バックアップを実施し、一世代を保管します。 お客様側からのデータ取得は行えません。
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	AM1:00以降に開始された時点でのデータ ※利用環境により実施時間が異なります。
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	日次により更新を行うため、データとして保持される期間は1日となります。
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 サービス解約後、一定期間経過後にデータを削除します。
32		バックアップ世代数	保証する世代数	世代数	1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	保存データはパスワードのみ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要件の有無、内容	有無／内容	無 ストレージに対して直接アクセスすることはできません。
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／保険の有無	有無	有 サービス利用約款に定める範囲での補償となります。
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を整えており、外部の漏えいの懸念のない状態が構築できていること	有無／内容	有 データ返却に関しては、別途有償対応となります。また解約時はデータを消去する体制を整えています。
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 特性上、データ不整合が生じる可能性のある機能に関しては、整合性を維持するための機能を実施しています。
38		入力データ形式の制限機能	入力データ形式の制限機能の有無	有無	有 不正データを制限する仕組みとなっております。
セキュリティ					
39	セキュリティ	公的認証取得時の要件	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 ISO27001／ISMS認証取得
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 アプリケーションアップデート、システム変更時等に脆弱性診断を実施。
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 端末認証および公開鍵認証等で運用者を限定したうえで、FWにて弊社ネットワーク内にアクセスを制限しています。
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	有無	有 TSL1.2
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SAS70T y pe2監査報告書」 「最新の18号監査報告書」	有無	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	有無	有 パーミッションにより管理データ領域を制限しています。
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等な制約が実現できていること	有無／設定状況	有 利用者データへのアクセスは、運用管理者のみに限定しています。
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されるか	設定状況	運用者のIDおよび操作ログを一定期間保存しています。
47		ウィルススキャン	ウイルススキャンの頻度	頻度	日次
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
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	把握している