No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	ご回答欄
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）	計画停止時間は提供者が個々に設定	24時間365日メンテナンス等により計画的にサービスを一時停止する場合には、事前にメールにてご連絡いたします。
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確認（事前通知のタイミング／方法の記述を含む）	有無	30日前にメール／ホームページで通知		メンテナンス等により計画的にサービスを一時停止する場合には、事前にメールにてご連絡いたします。
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確認（事前通知のタイミング／方法の記述を含む）	有無	15ヶ月前にメール／ホームページで通知		通知期間などは具体的に設定しておりません。メール、ホームページにて通知いたします。
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	有無	第三者へのプログラムの預託を実施	サービス提供企業が倒産等した場合にもサービスを継続できるように、プログラムを第三者に預託していることが望ましい	預託はありません。突然の停止となった場合は、再開までお時間いただくこととなります。
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（%）	99.9%以上（基幹業務） 99%以上（基幹業務以外）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討 ※「計画サービス時間」は、サービス提供時間と計画停止時間の両方を含む。	99.9%となります。(2024年実績)
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	遠隔地のバックアップ用データセンタで保管している日次バックアップデータと予備システム切替時間は半日～1日	データセンタ構成、復旧までのプロセス／時間、費用負担についても明示されていることが望ましい また、適用する業務の重要性に応じた「ディザスタリカバリ」のレベルにより設定内容は変わる	Amazon AuroraとS3を使用しており、事実上、災害によって影響されることはないと考えております。東京の複数AZが被災する状況では、日本のインターネットや通信が途絶していると考えられます。
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	バックアップデータの取得が可能なホームページを用意		重大障害の実績がないため明確に答えかねますが状況に応じて検討させていただきます。
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）	CSVあるいはExcelファイル	データ保護の観点からは、クラウド・コンピューティング・サービス提供者だけでなく利用者側でもバックアップを実施しておくことが望ましい。また、システムの信頼性、サービス継続性の観点からは、サービス提供者は十分に対策を行っていると考えられるが、トラブル時に備えて、預託データのダウンロードが可能かどうかを確認することが望ましい	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	有無	年2回の定期バージョンアップを実施	頻度、事前通知方法、履歴管理／公開、利用者の負担についても明示されていることが望ましい	主要なOSなどにアップデートがあった場合に、メンテナンスが実施。サービス提供システムのOSおよびミドルウェアに関して、ベンダーが提供するセキュリティパッチやアップデートが速やかに適用され、最新の状態に保たれる仕組み。システム構成要素（アプリケーション、サーバー、ネットワーク機器）に対する定期的な脆弱性検査（第三者によるスキャンを含む）が実施され、脆弱性が発見された場合は改善措置が取られます
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	1時間以内（基幹業務） 12時間以内（上記以外）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討	4.4時間
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	3時間後 3日後	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討	できるだけ速やかな復旧を目標としています。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	ご回答欄
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	1回以内（基幹業務） 3回以内（上記以外）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討	3回
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	ハードウェア／ネットワーク／パフォーマンス監視	詳細な監視項目は提供者が個々に設定	End-to-EndでHTTPリクエストによりサービスダウンを検知しております。
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	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	初期対応後の経過報告の方法・タイミングについても明示されていることが望ましい	障害の内容によって異なるため明確に回答しかねます。
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	15分以内（基幹業務） 2時間以内（上記以外）	営業時間内／外で異なる設定を行う場合がある	障害の内容によって異なるため明確に回答しかねます。
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）	1分以内（基幹業務） 15分（上記以外）	営業時間内／外で異なる設定を行う場合がある	5分ごとに監視しております。
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	月に一度ホームページ上で公開	報告内容／タイミング／方法は提供者が個々に設定	ありません。
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	セキュリティ（不正アクセス）ログ／バックアップ取得結果ログを利用者の要望に応じて提供	提供内容／方法は提供者が個々に設定	ログの提供はさせていただいておりませんが必要に応じて確認できる範囲でお答えさせていただきます。
19	性能	応答時間	処理の応答時間	時間（秒）	データセンタ内の平均応答時間3 秒以内	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討	現在、設定はありません。
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	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討	現在、設定はありません。
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）	4時間以下	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討	現在、設定はありません。
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	利用画面上の項目配置変更や新規項目の追加が設定画面より可能		項目の追加などは設定可能です。
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）	有無	API（プログラム機能を外部から利用するための手続き）を公開	APIがインターネットの標準技術で構成され、仕様が公開されており、APIの利用期限や将来の変更可能性が明記されていることが望ましい	Zapier連携機能のためにAPIを公開しています。
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	有無（制約条件）	50ユーザ（保証型）	同時接続の条件（保証型かベストエフォート（最善努力）型か）、最大接続時の性能について明示されていることが望ましい	特に上限なく接続できます。
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 40,000ページビュー		特に上限はありません。
アプリケーション運用							
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	24時間365日（電話）	受付方法（電話／メール）や営業時間外の対応は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる	平日10～18時　（電話／メール）
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）（年末年始・土日・祝祭日を除く） 24時間365日（メール）	受付方法（電話／メール）や営業時間外の対応は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なる	平日10～18時　（電話／メール）
データ管理							

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	ご回答欄
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、作業前後の差分のみバックアップし、週次でフルバックアップを取る。遠隔地のデータセンタにテープ形式保管。アクセス権はシステム管理者のみに制限。復旧／利用者への公開の方法は別途規定）	保証要件を設定している場合は、具体的に明示。バックアップ内容は対象業務の重大性およびサービス内容／特性／品質に応じて状況が異なるまた、クラウド・コンピューティング・サービスベンダの民事再生、破産等によりサービス継続が出来ない場合についても明示されていることが望ましい	1日1回Amazon Auroraのバックアップ機能を使ってAmazon Web Services内に保存しています。マルチテナント型ですので、利用者へのアクセス権はありません。
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	前日朝6時までただし、災害発生時は1週間前まで	データ破損、システム障害時において、どの時点のデータを最低限保証すべきか示すこと	毎日23時にバックアップを行っています。
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	5年以上（証跡として残すべきもの、法定のもの）3ヶ月以上（その他）	対象業務の重大性を考慮しつつサービス内容／特性／品質に応じて個々に検討する 証跡として残すべきだと思われるものとしては、アクセスログ等のセキュリティに関係するログ情報が挙げられる。法定のものとしては、帳票関係が挙げられる	ご解約後5年保管し、データ廃棄します。
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	サービス解約後1ヶ月以内にデータおよび保管媒体を破棄	解約時には、CSVなどの一般的なフォーマットでデータ出力ができることが望ましい	ご解約前にCSVにてデータの排出は可能です。またご希望時は画像のデータもお渡しします。ご解約後はデータにアクセス不可能となります。弊社プライバシーパークに規定により一定期間保管されたのちにデータ破棄となります。
32		バックアップ世代数	保証する世代数	世代数	3世代	ロールバックを必要と迫られた際にどの時点のバックアップデータまで遡ることが可能であるかを明確にしておくことが望ましい	7世代です。
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	個人情報や、業務において重要かつ暗号化せねば信頼性に欠けるデータを対象とする	保存データの暗号化は行っていません。
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	有複数のキーを使用することで、不正アクセス等の影響範囲を限定する	マルチテナントストレージの場合のキー管理の方法について、全顧客がひとつのキーを使うのか/顧客別にひとつのキーが割り当てられるのか/顧客別に複数のキーを使えるのか明確にしておくことが望ましい	無し
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	個人情報を扱う場合には、クラウド・コンピューティング・サービス提供者との間で個人情報取り扱いに関して合意を形成して契約事項の中で責任の割り当てを行っておくべきであるが、万が一の個人情報漏えいに備える意味でサービス提供者における損害賠償保険加入の有無を確認しておくことが望ましい	無し
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	有返却する場合は、テープ媒体にデータを保管し、提供する消去する場合は、証明書を送付する（第三者機関発行の証明書が望ましい）	外部への漏えいをいかに防ぐ仕組みが出来ているか	ご解約後はデータにアクセス不可能となります。弊社プライバシーパークに規定により一定期間保管されたのちにデータ破棄となります。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	ご回答欄
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	入力データ、算出データ等がハードウェア/プラットフォーム/アプリケーションの問題や不正な操作により改ざんされていないこと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	無し
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	金額、住所、電話番号等の文字種、データ形式が制限されるフォームにおいて、想定外のデータ入力を検出し、不正なデータをデータベースに格納しないようにする仕組みを提供していること	有り
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）が取得されていること	有無	ISMS認証取得プライバシーマーク取得	ITサービスマネジメントのベストプラクティスであるITILやJISQ20000、JIS Q 27001:2006をベースとした情報セキュリティ監査の実施等の取得状況も確認することが望ましい	プライバシーマーク取得　ISMS認証取得のデータセンターへ格納
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（サービス提供前に、セキュリティホールの有無等について第三者機関（又は内部機関）により検査を受け、また、検査が定期的かつ適切に行われていることを年１回、外部機関により評価を受ける。また、速やかに指摘事項に対して対策を講じる。）	セキュリティ監査、システム監査、ペネトレーションテスト等ネットワークからの攻撃に対する検証試験、ハードウェア/プラットフォーム/ウェブアプリケーションの脆弱性検査、データベースセキュリティ監査などを想定	プライバシーマーク取得し、継続して更新しております。
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（運用者が限定されていること）		開発・保守担当と運用担当の業務分離がされております。※基本的に確認のためのアクセスは可能ですが開発技術部からでないとアクセスできないものもあります。
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	3DES/RSA/SHA-1	SSLの場合は、SSL3.0/TLS1.0（暗号強度128ビット）以上に限定	TLS1.2対応
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	有		無し
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	データ認証のアクセスコントロールについて明記		フレームワークで、データにアクセスするさいに保有する企業のIDとユーザIDをチェックして制限する機構を組み込んでおります。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	ご回答欄
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（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）	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るかどうかを確認すること。クラウド・コンピューティング・サービスにおけるハードウェア/プラットフォーム/アプリケーションで用意されているロール（管理者、一般ユーザ等の役割を意味する）に制約がある場合には、ユーザを既存のロールの範囲でグルーピングする等の工夫により対応できるかどうかを確認する。 クラウド・コンピューティング・サービスではマルチテナントを採用しているため、他の顧客と一つのデータベースを共有する場合があることに配慮すること	有
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	権限に沿ったID管理が行われていること（1人1ID発行）		権限に沿ったID管理が行われています（1人1ID発行）
47		ウイルススキャン	ウイルススキャンの頻度	頻度	週次		無し
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	・権限者のみアクセス可・廃棄時には、データを完全に抹消する・暗号化、認証機能を用いる・遠地へ運ぶ際は、施錠されたトランクで運ぶこと		すべてクラウド上にあるので該当なし
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	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		日本に保存されているので、日本法に準拠して運営しております。
追加項目							
50		認証機能	多要素認証への対応	有無／設定状況	多要素認証対応有り ・クライアント証明書 ・OTP（メール／SMS／アプリ） ・物理キー ・グローバルIPアドレス制限 ・SAML認証		有　SAML認証
51		クラウドサービスの実績	クラウドサービスがどの程度利用されているか	時間／導入社数	サービス提供期間：10年 導入社数：1000社利用中		サービス提供期間：17年 導入者数：500社利用中
52		データ保管先リージョン	データ保管先リージョンが通知されるか	有無／設定状況	データ保管先リージョンが明確であり、通知される ・東京 ・大阪		セキュリティ上開示しかねます。
53		再委託先の管理（責任範囲）	再委託先および再委託時のデータの取り扱いや責任範囲が明確か	有無／契約内容	再委託有（契約書に再委託範囲が明記されている）		委託先はプライバシーマーク規定に従って管理しております。

No.	種別	サービスレベル項目例	規定内容	測定単位	設定例	備考	ご回答欄
54		再委託先の管理（データ消去）	再委託業務の終了後にデータの消去または返却されたことを確認しているか	有無／契約内容	データの消去または返却されたことを確認し記録に残している		委託先はプライバシーマーク規定に従って管理しております。
55		スケーラビリティ	リソース不足時にスケーリングの仕組みがあるか	有無／設定状況	追加契約を結ぶことでスケーリングが可能 （別途オートスケールオプション有り）		無
56		運用・セキュリティログの取得と保管期間	どのような種類のログが記録されどのくらい保管されるか	ログ種類／時間	アクセスログ、操作ログがそれぞれ5年間保管される （別途保管期間延長オプション有り、最大10年間）		ログの提供はさせていただいておりませんが必要に応じて確認できる範囲でお答えさせていただきます。 契約期間内はログを残しており、プライバシーパークに規定により一定期間保管されたのちにデータ破棄となります。