エンゲージメントコンパス_クラウドサービス利用チェックシート

チェックリスト基準： SaaS対応SLAガイドライン（経済産業省）

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
サービス運用					
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・定期保守は除く）
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 5営業日前までに専用管理画面で通知します。
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確認 （事前通知のタイミング／方法の記述を含む）	有無	有 2か月前にメール/専用管理画面で通知します。
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	有無	無 現時点で終了予定はなく、プログラムやデータの預託も未定で
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	稼働率（ ）	99.9%を目標に運用（計画停止・定期保守は除く）
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 Webサーバ・DBサーバは冗長化して運用しています。また、1日1回データのバックアップを行っています。
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 復旧に必要な全リソースをバックアップしておるため早期に完全復旧が可能になっています。
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 システム利用できない場合の代替措置提供がないため、未定義となります。
9		アップグレード方針	バージョンアップ／変更管理／パッチ管理の方針	有無	有 バージョンアップ、機能追加は随時実施いたします。
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	非公開
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	非公開
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	非公開
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 ハードウェア／ネットワーク／リソース／パフォーマンスの各監視を常時実施しています。
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）	有無	有 指定された緊急連絡先にメール／電話で通知され対応を実施します。利用者へは適宜専用管理画面を通じて報告を行います。
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	数分程度 異常検出後に指定連絡先に自動通知される仕組みを構築してい
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
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	報告事項が有る場合に限り随時、専用管理画面/公式ホームページ上で告知します。
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）	有無	無 各種ログは非公開となります。
19	性能	オンライン応答時間	処理の応答時間	時間（秒）	目標応答時間を3秒以内に設定。 ただし、データ量や検索条件等により目標時間を超過する場合がございます。
20		遅延	処理の応答時間の遅延継続時間	時間（分）	遅延継続時間の設定はしておりませんが、アクセスログからWebサイトの応答時間を収集し、遅延の監視や定期的な分析を行っております。
21		バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	データ量・処理内容により異なるため設定しておりません。
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	有無	無 ただし、一部のサーベイ回答取得項目において任意の設定が可
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	無
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	無
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	無
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	平日10:00～17:00 祝祭日・年末年始・弊社が別途休日と認めた日を除く
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	平日10:00～17:00 祝祭日・年末年始・弊社が別途休日と認めた日を除く
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 日次にてバックアップを取得し、国内のクラウド上に保管しています。 復旧方法は運用責任者および運用責任者が指定する担当者がクラウド上のインフラ管理画面より対応いたします。
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	時間	具体的な時点は公開しておりませんが、24時間以内のデータを保証致します。
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	7日間

エンゲージメントコンパス_クラウドサービス利用チェックシート

チェックリスト基準： SaaS対応SLAガイドライン（経済産業省）

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
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 サービス利用停止があった場合に論理削除を行います。利用者様のご要望があれば個別に物理削除を承ります。 ※サーベイデータは他社比較データとして活用するため継続保持いたします ※今後、サービス利用停止から一定期間経過後、物理削除を自動実行ことも検討中です
32		バックアップ世代数	保証する世代数	世代数	7日分
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	webサーバーもDBサーバーもAES-256という方式で暗号化しています。
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	有 テナント固有のIDでデータを論理的に分離しています。
35		データ漏えい・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	無 補償は原則行っておりません。
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 サービス利用停止があった場合に論理削除を行います。利用者様のご要望があれば個別に物理削除を承ります。 ※サーベイデータは他社比較データとして活用するため継続保持いたします ※今後、サービス利用停止から一定期間経過後、物理削除を自動実行ことも検討中です
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 データ入力時、送信時に検証、通信経路での盗聴、改ざんを防止するためにTLSにより保護しています。
38		機密性の高いデータの要件	個人情報や機密性の高い情報が含まれている場合、それぞれの取扱い規則との整合性を確認できること	有無	有 ログインパスワードは入力中マスクし、保存時は不可逆暗号化を実施しています。
39		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 データ入力時・送信時での検証、DBカラムの型指定により不正なデータが入りにくい構造としています。
セキュリティ					
40	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	有 プライバシーマークを取得しています。
41		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 定期的に第三者（自動ツール）による脆弱性診断を受ける
42		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 アクセス可能な利用者を限定すると共に、職務内容に応じた権限を設定しています。
43		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 WEBアプリケーション上の通信はTLS1.2以上の暗号化を強制しています。
44		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監査基準に対する資料提供・監査受入れができるか。監査報告書の公開できるか 「最新のSAS70Type2監査報告書」「最新の18号監査報告書」	有無	無
45		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 テナント固有のIDでデータを論理的に分離しています。
46		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 データへのアクセスは管理者権限をもった保守運用要員のみに制限しています。
47		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	無 個人ごとに発行したIDに紐づいたアクセスログ解析の仕組みを導入しています。
48		ウイルススキャン	ウイルススキャンの頻度	頻度	随時 リアルタイムスキャンを可能とする仕組みを導入しています。
49		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 バックアップデータは暗号化されております。 外部メディア等への保管はしておりません。 二次記憶媒体の利用を禁止・制限しています。
50		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	日本国内にデータ保存しており、日本の法制度に則っています
確認事項					
51	データセンター	データの所在地	サーバーおよびデータ保管先の所在地はどこか。	所在地	国内リージョンのデータセンターにて提供しております。
52		データの再委託	各顧客データ・顧客が入力したデータ取扱いの第三者委託はあるか。	有無	無
53		データセンター入館管理	入退室管理されたコンピュータルームの施錠管理されたラック等、明示的に許可された者以外は触れない環境に設置されているか。	有無	有 データセンター・クラウドサービスの規定を考慮し選定し設置している。
54		データセンター監査	ユーザーによるデータセンター訪問、監査を受け付けるか。	可否	否

エンゲージメントコンパス_クラウドサービス利用チェックシート

チェックリスト基準： SaaS対応SLAガイドライン（経済産業省）

No.	種別	サービスレベル項目例	規定内容	測定単位	回答
55	セキュリティ	脆弱性への対応	セキュリティパッチを適用する等、サーバの脆弱性対策を遅滞なくかつ定期的に実施しているか。	頻度	有 必要に応じて随時行っています。
56		アクセス経路の制限	ファイアウォール等のアクセス制御を行い、公開する必要のない通信ポートは閉じているか。	有無	有 レイヤー毎に必要範囲の通信を許可するよう制御しておりま
57		不正なアクセスに対する対策	侵入・改ざん・Dos攻撃を検知し制御する仕組みがあるか。	有無	有 FW・WAF・統合セキュリティソフトにて検知・制御していま
58		不要な表示の有無	公開する必要のないディレクトリ・ファイル・設定情報は外部から不可視とし、必要のない機能は、停止する等の措置がされているか。	有無	有
59		セキュリティ検査	公開前にセキュリティ検査を実施し、提供に適した状態であることを確認し報告を提出できるか。	有無	無 リリース前のコードレビュー、該当技術者以外による社内テストを実施しています。いずれのテストにおいても、テスト内容/脆弱性結果/修正内容の公表、提供はしておりません。
60		ログの保持	利用者の活動、セキュリティ事象と関連するログ期間はどのくらいか。	期間	30日
61	体制	内部不正についての対策1	人的な対策はどのようなものを行っているか。	対応状況	入社時および定期的にセキュリティ情報を教育・周知しております。
62		内部不正についての対策2	従業員が契約者のデータへ不必要に、許可なくアクセスすることへの抑止力はあるか。	対応状況	運営者を限定するとともに、ID・PWや接続元IP制限によりアクセスを限定しています。
63		内部事故についての対策	データの持ち出し・紛失への対策はあるか。	対応状況	セキュリティポリシーを規定したうえで、社内勉強会を実施しています。 データ持ち出しについては、従業員PCにおける操作ログを取得することで抑止に繋げているほか、プリントアウトを禁止してデータをクラウドストレージで管理する運用を徹底することで紛失を防止しています。
64		ユーティリティ表示	現在のシステム稼働状況を視認できるページは準備されているか。	有無	有 リソース監視を実施し、一定の閾値を超える場合はアラートがあがる仕組みを運用しています。
65		セキュリティ領域の確保	オフィスの物理的セキュリティ領域を設け、出入りを管理しているか。	有無	無
66		セキュリティに関する外部からの指導	契約者の指示による情報管理体制の改善等の指導を受け入れられるか。	可否	否 指導に対しては要否を検討のうえ、最大限善処いたします。
67		事故発生時の外部監査	セキュリティインシデント発生時、契約者による外部監査を受け入れられるか。	可否	否 指導に対しては要否を検討のうえ、最大限善処いたします。
68	機能	パスワード定期変更	パスワードに有効期限を設け、再発行を強制する仕組みがあるか。	有無	無 総務省推奨方法に準じ強制変更の仕組みは未導入です。
69		パスワード強度	十分な強度のパスワード文字列が設定できるか。	有無	有 運営管理者向けとして、8文字以上・複数文字種の混合必須としています。
70		多要素認証	ID/PW以外の本人認証の仕組みを設けているか。	有無	有 運営管理者向けとして、IPアドレスでのアクセス制限を実施しています。
71		多要素認証（クラウド基盤）	クラウド認証基盤との連携機能（AzureAD連携等）	有無	無
72		スマートフォンアプリ	スマートフォンアプリでサービス利用ができるか。利用制約について特記事項はあるか。	有無	無
73		アカウントロック	一定回数ログインに失敗した場合に、アカウントを無効化またはロックする機能が提供されているか。	有無	有 運営管理者向けとして、１分以内で連続失敗６回目以降はロックが掛かる仕様となっています。
74		アクセス制限	利用環境において、第三者がアクセス出来ない仕組みがあるか。IPアドレス制限ができるか。	有無	有 運営管理者向けとして、IPアドレスでのアクセス制限を実施しています。
75		アクセス権限管理	管理者毎のアクセス権限を制御する機能があるか。	有無	有 運営管理者・ユーザー管理者ともにアクセス権限範囲をロールごとに規定しています ※アクセス権限ごとに任意で権限制御する機能はありません
76		個人情報・企業秘密情報	個人情報や機密性の高い情報がシステム内に保管されるか。	有無	有 ユーザー管理者の個人情報をシステム内で保持しています ※サーベイ回答者の個人情報は保持しておりません