クラウドサービスレベルのチェックリスト（経済産業省）に基づくセキュリティチェックシート

ITRA株式会社　2022/6/1

No.	種別	サービスレベル項目	規定内容	測定単位	設定等
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。実施の5営業日前までにメンテナンス情報のページにて通知
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。1年以上前に契約者宛にメールまたは郵便にて通知
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
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
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。災害時規定に基づき、システム復旧ならびにサポート実施
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	無
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
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。機能追加などは随時実施し、お客様への影響が大きいものについては事前にメール等で連絡。パッチ管理は適宜
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（パフォーマンス監視、死活監視、エラー監視）
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で連絡
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	可能な限り迅速に行う
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
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	非公開
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	有。操作履歴

19	性能	応答時間	処理の応答時間	時間（秒）	非公開
20		遅延	処理の応答時間の遅延継続時間	時間（分）	非公開
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）	非公開
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。可能な範囲や仕様等を記載したマニュアルを提供
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。APIを公開
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）	制約は無（ベストエフォート）
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	有。プランによる
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	24時間365日（フォーム）
27		サービス提供時間帯(一般問い合わせ)	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	24時間365日（フォーム）
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。同一データセンター内に日次でフルバックアップ。アクセス権は、必要な管理者に割り当てられ、その者が復旧も行う
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	24時間
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	72時間
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。サービス解約後、適宜データを削除
32		バックアップ世代数	保証する世代数	世代数	3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	有。共通のキーを使用し、ストレージはテナントごとに分離
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	無
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。お客様自身でデータのダウンロードが可能。サービス解約後、弊社にて適宜データを削除
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	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（登録番号17001388-05）
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
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		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。TLS 1.2
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SAS70Type2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。テナントごとにデータスペースは完全に分離
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。利用者データにアクセスできる利用者を制限するための仕組みがあり、お客様側で設定が可能。詳細情報はマニュアルで提供
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管理を実施。1年以内のログを確認することが可能
47		ウイルススキャン	ウイルススキャンの頻度	頻度	リアルタイムスキャンをオプションにて提供
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。二次記憶媒体は使用せず、データセンター内のみに案誤化した状態で保管
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	データの保存地ならびに法制度等による制約条件は適切に把握