クラウドサービスレベルのチェックリスト

記入日：2026/03/18
会社名：株式会社ベーシック

No.	種別	サービスレベル項目例	規定内容	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 （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（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 （事前通知のタイミング／方法の記述を含む）	【有】 7日前までにメールにて通知
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】 現時点で終了の予定はありませんが、サービス終了する場合は90日以上前にメールにて通達。
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	【無】 プログラム等の第三者への預託は実施しません。
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）	99.9%以上を目標に運用
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 クラウド管理されているバックアップデータより対応エンジニアが復旧対応を実施。
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　バックアップが存在する場合は、バックアップから新規環境を構築して復旧を実施。
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　障害時など特別な場合にのみ.sql形式で提供。
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 ベストエフォート型で対応。
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）	定めておりません
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	定めておりません
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	直近3ヶ月では1件。復旧に長時間（1日以上）要した障害件数は0件。
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　24時間ハードウェア及びネットワークのパフォーマンス監視。
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　メールにて影響のあったご契約者に通達。
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	弊社担当者への通知は1分以内。影響が□きい障害に関しては、お客様への通知を可能な限り迅速に実施。
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	営業時間内/1分以内　営業時間外/実施なし
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	必要に応じて、メールにて通知。
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）	原則ログの提出不可。重大な障害発生時に限り応相談。
19	性能	応答時間	処理の応答時間	平均1秒以内
20		遅延	処理の応答時間の遅延継続時間	1分
21		バッチ処理時間	バッチ処理（一括処理）の応答時間	3時間以内
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	無
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の接続仕様（API、開発言語等）	有　外部サービスからwebhookを受け取ることが可能なエンドポイントを提供。
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	ベストエフォート型
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	ベストエフォート型
	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	弊社営業日 10時~18時　メール または サービス内チャット
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	弊社営業日 10時~18時　メール または サービス内チャット
	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 1日1回クラウドサービス（AWS）上に保存　クラウドサービス上から復旧操作を実施。サーバー管理者のみがアクセス権を保有。
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	12:00-13:00
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	7日間
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	workrun組織削除時に即時削除
32		バックアップ世代数	保証する世代数	7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
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	無
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	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

クラウドサービスレベルのチェックリスト	記入日：2026/03/18 会社名：株式会社ベーシック

No.	種別	サービスレベル項目例	規定内容	回答
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
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　システムへ入出力されるデータは脆弱性の特性をもとにサニタイジングされる仕組みを実装。新たに脆弱性が発覚した場合も随時追加の対策を実施。
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	ISMS（ISO/IEC 270001:2022）を取得
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	1年に1回実施を目安に第三者によるアプリケーション脆弱性診断を実施
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
42		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
43		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	アクセスログによる追跡のみ可能。保存期間は1年間。
44		ウイルススキャン	ウイルススキャンの頻度	デプロイ時にDockerコンテナイメージの脆弱性スキャンを都度実施
45		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	二次記憶媒体を利用していない。
46		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	日本以外に保存していない。
ユーザー管理				
48	ユーザー管理	アカウントの付与	利用者の管理者／運用者／ユーザに対して一意なアカウントを付与できるか。	可　メールアドレス単位でユーザーの招待が可能。
49		アカウント付与の承認	利用者がアカウントを発行・変更・削除する際およびアカウントに対して権限を付与する際、作業者とは別の人間が確認・承認をすることは可能か。	不可　管理者が招待したアカウントに対して別の第三者が承認を挟めない。
50		アカウント権限	①業務上の役割に応じて、サービス利用企業側で、自由にアカウントを発行することは可能か。 ②各アカウントに対して、個別に権限を設定することは可能か。	可　workrun内のメンバー管理画面にてメンバー招待により招待者のアカウントの発行が可能。同画面にて権限付与が可能。
51		アカウント情報の出力	サービス利用者のアカウントの利用状況およびアカウントの権限を一覧で出力することは可能か。	不可　サービス内でアカウントの一覧は確認可能。CSVなどでの出力は不可。
52		パスワード管理	システムへの初回ログイン時、初期パスワードを強制変更させることは可能か。	対象外　パスワードでのログイン機能なし
53		パスワードポリシー	任意のパスワードポリシーを設定可能か。	対象外　パスワードでのログイン機能なし
54		パスワードの暗号化	パスワードはハッシュ化または暗号化（※）した上でシステム内に格納されるか。	対象外　パスワードでのログイン機能なし
通信の制御				
55	通信の制御	通信プロトコル	クラウドサービスを利用するための通信プロトコルとして、http,https以外に何を使用するか。	無　httpsのみ使用。
56		閉域網（VPN 等）での接続	クラウドサービスへの接続方式として、閉域網（専用線またはVPN）での接続に対応しているか。	無　対応なし
57		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　TLS1.2以上

項目番号	内容	チェック	備考・解説
1. 情報セキュリティに対する組織的な取り組み状況			
1-1	情報セキュリティに関する経営者の意図が従業員に明確に示されていますか？	○	
1-2	情報セキュリティ対策に関わる責任者と担当者が明示されていますか？	○	
1-3	管理すべき重要な情報資産を区分していますか？	○	
1-4	重要な情報については、入手、作成、利用、保管、交換、提供、消去、破棄における取り扱い手順を定めていますか？	○	
1-5	外部の組織と情報をやり取りする際に、情報の取り扱いに関する注意事項について合意を取っていますか？	○	
1-6	従業者（派遣を含む）に対してセキュリティに関して就業上何をしなければいけないかを明確にしていますか？	○	
1-7	情報セキュリティに関するルールの周知と、情報セキュリティに関わる知識習得の機会を与えていますか？	○	
2. 物理的セキュリティ			
2-1	重要な情報を保管したり、扱ったりする場所の入退管理と施錠管理を行っていますか？	○	
2-2	重要なコンピュータや配線は地震などの自然災害や、ケーブルの引っ掛けなどの人的災害に配慮し適切に配置・設置していますか？	○	
2-3	重要な書類、モバイル PC、記憶媒体などについて、整理整頓を行うと共に、盗難防止対策や確実な廃棄を行っていますか？	○	
3. 情報システム及び通信ネットワークの運用管理状況			
3-1	情報システムの運用に関して運用ルールを策定していますか？	○	
3-2	ウイルス対策ソフトをはじめとしたアプリケーションの運用を適切に行っていますか？	○	
3-3	導入している情報システムに対して、最新のパッチを適用するなどの脆弱性対策を行っていますか？	○	
3-4	通信ネットワークを流れる重要なデータに対して、暗号化などの保護策を実施していますか？	○	
3-5	モバイル PC や USB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などに備えて、適切なパスワード設定や暗号化などの対策を実施していますか？	○	
4. 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況			
4-1	情報（データ）や情報システムへのアクセスを制限するために、利用者 ID の管理（パスワードの管理など）を行っていますか？	○	
4-2	重要な情報に対するアクセス権限の設定を行っていますか？	○	
4-3	インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング、ISP サービス 等）を行っていますか？	○	
4-4	無線 LAN のセキュリティ対策（WPA2 の導入等）を行っていますか？	○	
4-5	ソフトウェアの選定や購入、情報システムの開発や保守に際して、情報セキュリティを前提とした管理を行っていますか？	○	
5. 情報セキュリティ上の事故対応状況			
5-1	情報システムに障害が発生した場合、業務を再開するために何をすべきかを把握していますか？	○	
5-2	情報セキュリティに関連する事件や事故等（ウイルス感染、情報漏えい等）の緊急時に、何をすべきかを把握していますか？	○	

参考　※IPAの提供する情報セキュリティ対策チェックリストより作成

https://www.ipa.go.jp/files/000014950.pdf