DocBase セキュリティチェックシート

経済産業省が公開している「クラウドサービスレベルチェックリスト」を参考にしています。

No.	種別	サービスレベル項目	規定内容	測定単位	設定内容	備考
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（メンテナンス等の計画停止を除く）	
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	7日前にヘルプセンターとサービス内お知らせエリアで通知します。 https://help.docbase.io/groups/654	
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	3ヶ月前までにヘルプセンターで通知します。	
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：現状、システムやデータを第三者預託の予定はございません。	
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は未設定ですが2024年の実績は99.94%です。	2022年 99.93% 2023年 99.97%
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	有無	有：日次で20世代分バックアップしています。サーバは異なる物理的な場所 (Availability Zone)に配置してあり、冗長化して運用しています。	
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：即時復旧が可能なように、データセンターの冗長化、及びバックアップの世代管理を行っております。	
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)	有：投稿された情報（添付ファイル含む）は全てMarkdown、またはJSONでエクスポート可能です。	
9		アップグレード方針	バージョンアップ/変更管理/パッチ管理の方針	有無	有：月に2回程度の機能追加や不具合修正のリリースを行っております。緊急度の高い脆弱性などの場合は適宜実行します。サービス稼働に影響が出るようなアップグレードの場合は事前に告知の上、実行します。	
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	63分（アクセス不可となる障害からの平均復旧時間）	
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	2時間	
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年間に発生した障害件数：3件 対応に長時間要した障害件数：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	有無	有：死活監視、パフォーマンス監視、リソース監視、アプリケーションエラー監視を常時行っております。	
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	有：メール、Slackにて運用担当者、開発者に通知されます。サービス稼働に影響が出ていると判断した場合、ヘルプセンターやSNSで告知します。	
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	運用担当者、開発者へは即時通知されます。 お客様へは可能な限り迅速に告知します。	
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)	モニタリングする対象によって異なります。 1～5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	定期的にサービス提供状況を報告はしておりません。	
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	操作履歴ログを提供可能です。	https://help.docbase.io/posts/1580775#%E6%93%8D%E4%BD%9C%E3%83%AD%E3%82%B0%E3%81%AE%E4%BF%9D%E5%AD%98

19	性能	応答時間	処理の応答時間	時間 (秒)	平均1秒未満	
20		遅延	処理の応答時間の遅延継続時間	時間 (分)	平均1分以内の応答を目指しています	
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)	エクスポートデータの作成はバッチ処理で行っていますが、お客様のデータ容量に変わるため答えられません。	
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	有：セキュリティ機能をアドオンできます。詳しくはヘルプセンターをご確認ください。	https://help.docbase.io/posts/250561
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：公開APIを用意しています	https://help.docbase.io/groups/1472
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：同時接続利用者数に制限はありません。	同時編集機能については10名まで同時に編集可能です。
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	有：プランに応じて利用可能なストレージ容量に上限があります。	
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	24時間・365日（メール、カスタマーサポートフォーム）	
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	月～金曜日 10：00 ～ 18：00（年末年始、夏期休暇、祝日等は除く）となります。	
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：日次バックアップで20世代を保存しています。限られた一部の担当者のみがバックアップデータへアクセス可能です。	
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	バックアップする対象によって異なります。 毎日午前1時～4時頃に取得します。	
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	最大20日間となります。	
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：サービス解約時にデータを物理的に削除します。必要に応じてデータエクスポート可能です。	
32		バックアップ世代数	保証する世代数	世代数	20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：文書や個人情報などの機密性の高いデータを暗号化しています。暗号化はお客様毎に異なる秘密鍵で行われています。	https://help.docbase.io/posts/1580775#%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E6%9A%97%E5%8F%B7%E5%8C%96
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：お客様単位で情報を管理するためキー管理を行っています。またお客様毎に異なる鍵で暗号化を行っています。	
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：利用規約に定められた範囲でお客様のデータ保護に最大限の注意を払います。	
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：サービス解約時にデータを物理的に削除します。お客様は必要に応じて投稿データや添付ファイルをデータエクスポート可能です。	
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：機能リリースなどのアップグレード前にデータ整合性の検証・テストをし、不整合がないよう務めています。	
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：入力項目の要件に応じて、不正文字列、形式、長さなどをチェックしています。	
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：ISMSを取得済みです。	https://help.docbase.io/posts/1580775#iso-27001%E5%8F%96%E5%BE%97
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：脆弱性診断を定期的に実施しています。	https://help.docbase.io/posts/1580775#%E8%84%86%E5%BC%B1%E6%80%A7%E8%A8%BA%E6%96%AD
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：データへのアクセスは一部の担当者に限定され、またアクセス元も制限しています。	
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：TLSv1.2以上で通信を暗号化しています。	
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：実施しておりません。	
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：お客様毎に異なる鍵で暗号化を行っています。	
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一部の担当者に限定されています。またアカウントについても見直しを定期的に実施しています。	
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	有：IDは個人ごとに発行し管理しています。操作履歴ログは半年間保存され、お客様がダウンロードし閲覧可能です。またシステムログなどは1年間保存しています。	
47		ウイルススキャン	ウイルススキャンの頻度	頻度	日次でスキャンを行っています。	
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：二次記憶媒体への利用を禁止しています。	
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	把握しております。	
50		開発、構成変更時のテスト	新規、またはプログラム改修時、構成変更時にソースコードレビューやテスト等を開発者とは別に第3者が実施していること	第3者の確認内容	全てのソースコードに対して、開発者以外がレビューを行う体制となっています。また構成変更も同様に複数人でレビュー、検証を行っています。	
51		開発、構成変更時のリリース判定	新規、またはプログラムリリース、構成変更前に事前に承認者による確認とリリース判断を行っていること	承認者確認事項	行っております。	
52		脆弱性診断	定期的に脆弱性診断を実施し、不正な侵入、操作、データ取得等の脆弱性について、第三者の客観的な評価を得ていること	最終実施時期/ 実施した脆弱性診断の種類 （内部・外部ネットワーク、Webアプリ、スマホアプリ等）/ 発見された脆弱性への対応状態	年に一度、外部のセキュリティ専門会社による脆弱性診断を実施しております。 最終実施時期は2026年1月にWebアプリケーション診断、プラットフォーム診断を行っています。緊急、重要に該当するような問題はなく、修正が必要な問題はありませんでした。	https://help.docbase.io/posts/1580775#%E8%84%86%E5%BC%B1%E6%80%A7%E8%A8%BA%E6%96%AD