GIHOZセキュリティチェックシート

2024/3/4発行

No.	種別	サービスレベル項目	規定内容	測定単位	設定
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日です。（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	有 1週間前を目途にサービス内・メール・Webサイトで通知します。
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 現時点で終了の予定はありませんが、1ヶ月前を目途にサービス内・メール・Webサイトで通知する予定です。
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 現時点で終了の予定はなく、プログラムや各種データの預託の措置について定義しておりません。
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 (%)	SLOは公開していません。 参考値として、2022年度の正常稼働率は99.72%となっています。
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 AWSにて複数リージョンで冗長化しています
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 ユーザが当サービスで作成したデータはファイルとしてダウンロードできます。重大障害発生時は代替手段として一般的な表計算ソフトや画像編集ソフト等を用いることで、事前にダウンロードしたデータを閲覧・編集できます。
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)	有 CSV形式、PNG形式、SVG形式
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 機能追加等のバージョンアップは随時行っています。ユーザへの影響が大きい変更については、影響の大きさに応じて、事前にWebサイト・メール・サービス内での告知を行います。 サービスのソースコードレベルの変更管理はGitHubを利用して行なっています。 セキュリティ上必要なアップデートについては、Dependabotによりアップデートの検知を自動化し、随時アップデートを適用しています。
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	公開していません。
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	時間	公開していません。
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	回	1年間に発生した障害件数は公開していませんが、対応に1日以上要した障害はありません。
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 社内基準に則り監視を実施しています。
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	お客様への通知は必要に応じてサービス内、Webサイト、メールにて報告します。
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	影響の大きい障害の場合、1営業日以内を目途に、サービス内およびWebサイトで通知を行います。
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)	時間間隔は非公開ですが、随時監視を行っております。
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	必要に応じてサービス内、Webサイト、メールにて報告します。
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	有 ビジネスプランでは、操作ログを閲覧する機能を提供しています。
19	性能	応答時間	処理の応答時間	時間 (秒)	ページやデータのサイズによって左右されますが、おおむね0.5秒程度です。負荷状況によっては遅延が生じる場合があります。
20		遅延	処理の応答時間の遅延継続時間	時間 (分)	公開していません。
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)	定期的なバッチ処理はありません。
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	無 サービスの個別のカスタマイズには対応していません。
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	無 同時接続利用者数の制限はありません。
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 提供リソースの制限はありません。
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 ※時刻の表記は日本時間（JST）です。 ※年末年始、祝日は除きます。
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 ※時刻の表記は日本時間（JST）です。 ※年末年始、祝日は除きます。
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 日次でバックアップを取得し、AWS上に保管しています。利用者データへのアクセスは開発チームの一部のメンバーのみに制限しています。
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	毎日0時ごろに取得します。
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	7日間分保管しています。
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削除します。バックアップは保管期間経過後に削除します。
32		バックアップ世代数	保証する世代数	世代数	7世代を保管しています。
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 データベースをAES-256暗号化アルゴリズムにて暗号化しています。
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	無 ストレージの分離は行なっていません。ユーザによるデータへのアクセスの制御は、アプリケーション側で実施しています。
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	有 利用規約に損害賠償について規定しています。
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削除します。
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 フロントエンドでのデータ入力時、バックエンドでのデータ受信時にデータの検証を行っています。通信経路はTLSにより暗号化し、データの改ざんを防いでいます。
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 フロントエンドでのデータ入力時、バックエンドでのデータ受信時にデータの検証を行っています。
39		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	データは国内および米国に保存しており、各地域の標準ルールに従います。

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 開発チームとは独立した部門による脆弱性診断を年一回実施し、指摘事項について対応しています。
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 データへのアクセスは、業務上必要な開発チームの一部のメンバーに制限しています。
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 ユーザーとシステム間の通信はTLS1.2を利用して暗号化しています。
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、 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
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	無 データベースやサーバーのテナントごとの分離は行っていません。 データへのアクセス制御はアプリケーションにて行っています。
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 利用者側の管理者による、データへのアクセス制限の設定が可能です。
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	IDは個人単位で付与しており、ログの検索に利用可能です。ログは2年間分を保存します。利用者が閲覧可能な操作ログは１年間保存となります。 利用者へのログの提供について、ビジネスプランではサービス上で操作ログを閲覧する機能をご用意しています。閲覧可能なログの内容は以下をご覧ください。 https://gihoz.com/help/organizations/log
48		ウイルススキャン	ウイルススキャンの頻度	頻度	以下のように対応しています。 サーバ → コンテナイメージのスキャンを随時実施 開発・運用に利用する端末 → ウイルス対策ソフトを導入しスキャンを随時実施
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 バックアップはクラウド上に保存しており、持ち出し可能な外部記憶媒体へは保存していません。

改訂履歴

No.	発行年月日	改訂内容
1	2023/9/22	初版
2	2024/3/4	サービスのアップデートに伴いデータの外部保存方針を更新