



ゲンバトはセキュリティ対策を徹底した
クラウドサービスなので
多くの企業に安心して選ばれています



第三者による
セキュリティ診断



データの
バックアップ



障害発生時の
データ復旧



データの暗号化



最新の脆弱性への
速やかな対応



WAFによる攻撃の遮断



悪意のあるアクティビ
ティや不正な行動を継
続的にモニタリングし
脅威検出



ISO27001に基づく情報
セキュリティの管理

1. 第三者によるセキュリティ診断

セキュリティの専門家による脆弱性診断を定期的
に実施し、発見された脆弱性は速やかに対策を行
っています。

2. データのバックアップ

クラウド上のデータは毎日バックアップを取
得しており、7世代分保管しています。

3. 障害発生時のデータ復旧

障害が発生しても、発生直前のデータまで復
旧できるシステム構成としています。

4. データの暗号化

ゲンバトにアップロードするファイル、パス
ワードは全て暗号化しています。

5. 最新の脆弱性への速やかな対応

ソフトウェアの脆弱性を自動的に検出し、リ
スクを判断するツールを導入しており、リス
クの高い脆弱性は速やかに対策を行って
います。

6. WAFによる攻撃の遮断

WAFを導入しており、サイバー攻撃を遮断
しています。

7. 悪意のあるアクティビティや不正な行動を継続的にモニタリングし脅威検出

環境全体の潜在的な脅威を継続的に監視す
る仕組みを導入しており、見つかった脅威
の根本原因を速やかに排除します。

8. ISO27001に基づく情報セキュリティの管理

情報セキュリティマネジメントシステムに関
する国際規格であるISO/IEC 27001を取
得しており、ISO27001に基づいた情報
セキュリティの管理を徹底しています。


クラウドサービスセキュリティチェックシート

| No. | 種別 | サービスレベル項目例 | 規程内容 | 対応/可否 | 内容 |
|-------------------|------------------|------------------------|--|---|--|
| アプリケーション運用 | | | | | |
| 1 | 可用性 | サービス停止時間 | 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） | ○ | サービス提供は24h365dです。 ただし、サービスのメンテナンスによる停止が必要な場合、事前に通知いたします。ただし、緊急の障害の場合はその限りではありません。 |
| 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） | ○ | 実施5営業日前までに以下の公式WEBサイトのお知らせページから通知いたします。 https://genbato.jp/ |
| 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） | ○ | Genbato利用規約に記載しています。 サービス終了12ヶ月前までに通知いたします。但し、緊急の必要がある場合は通知なしでの終了もあります。 |
| 4 | | 突然のサービス提供停止時の対処 | 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 | × | 現時点で予定はありませんが、データを抽出して提供するなど何らかの対応を検討しています。 |
| 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） | ○ | 公開していません。2024年9月時点の稼働率実績は99.8%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 | ○ | 日次でデータのバックアップを実施し、バックアップしたデータは二次記憶媒体を使用せず、データセンター間でバックアップを取っています。 また、一定距離以上離れたデータセンターにてバックアップを実施しております。 |
| 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 | × | 複数のデータセンターで冗長化されており、システムデータの同期をとっているため、早期復旧が目指せる体制となっています。 |
| 8 | | 代替処置で提供されるデータ形式 | 代替処置で提供されるデータ形式の定義を記述 | × | 上記の通り早期復旧を可能としているため、データの提供はしていません。 |
| 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 | ○ | バージョンアップやアップグレード作業は随時実施しています。サービス停止を伴うアップグレード作業の場合のみ原則3営業日前までに公式Webサイトのお知らせページに通知いたします。 |
| 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） | ○ | 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 | ○ | 12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 | ○ | 過去1年間に発生した回数は1件です。1年間に発生した対応に長時間（1日以上）要した障害件数は0件です。 |
| 13 | | システム監査基準 | 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 | ○ | インフラ基盤のパフォーマンス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） | ○ | サービス停止を伴う障害発生時は早急に対応を行います。お客様へは公式Webサイトを通じて通知・報告いたします。 |
| 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 | ○ | 定めていませんが、ベストエフォートで対応します。 |
| 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 | ○ | 監視収集1分 集計5分 |
| 17 | | サービス提供状況の報告/間隔 | サービス提供状況を報告する方法／時間間隔 | ○ | 個別の報告はしていません。通知が必要な場合は公式Webサイトを通じて通知・報告いたします。 |
| 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） | ○ | アクセスログ、API実行履歴ログ、証跡ログ等は取得し保管していますが、提供はしていません。 |
| 19 | 性能 | 応答時間 | 処理の応答時間 | ○ | 公開していません。 |
| 20 | | 遅延 | 処理の応答時間の遅延継続時間 | ○ | 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 | ○ | 公開していません。 |
| 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 | ○ | 原則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） | ○ | 外部APIは存在していません。 |
| 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 | ○ | 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 | ○ | ご利用サービスごとに利用可能なストレージ容量には上限があります。（有料オプションにて増設可能） |
| サポート | | | | | |
| 26 | 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 | ○ | メール・問い合わせフォーム：24時間365日 電話：平日 09:30-12:00 13:00-17:00 | |
| 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 | ○ | メール・問い合わせフォーム：24時間365日受付しています。 電話：平日 09:30-12:00 13:00-17:00 通常のサポート業務の対応時間は、平日09:30-12:00 13:00-17:00（祝日、年末年始等弊社休日を除く） 内容を確認のうえ3営業日以内にご返答いたします。 | |

| データ管理 | | | | |
|--------|----------------------------|--|---|---|
| 28 | 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 | ○ | データバックアップは、国内の離れたデータセンターに日次間隔でバックアップしています。アクセスは当社システム管理者のみ可能となっております。 |
| 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リ、データを保証する時 | ○ | DBについては、当日午前1時バックアップ終了時には7世代までバックアップしています。 |
| 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 | ○ | お客様の契約期間保管されます。アクセスや認証ログは3年分保管しております。 |
| 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 | ○ | お客様が退会手続を行った場合、当社は、退会日から4カ月以内に、お客様が本サービス上で登録を行った情報を含む一切のデータについて削除いたします。本サービスの解約のみを行い、本サイトの退会を行わなかった場合には、解約日から30日以内に限り、当該サービスの再契約時に復元できるよう本サービス上のデータは当社で保持いたします。ただし、完全なデータの復元を保証するものではありません。また、本サービスの解約から30日経過した後は、当社は、お客様が本サービス上で登録を行った情報を含む一切のデータについて削除することができるものとします。 |
| 32 | バックアップ世代数 | 保証する世代数 | ○ | データバックアップの保証はしていません。ただし、当社ではシステム運用に必要な措置として、日次のバックアップは毎日1:00に実行され、保管世代は7世代管理としています。 |
| 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 | ○ | 通信はTLS1.3およびTLS1.2で暗号化しています。ストレージはAES256の規格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 | ○ | お客様の契約スペースごとに論理的に分離されたデータ領域で運用しています。 |
| 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 | ○ | 損害賠償保険には加入していません。ゲンバト利用規約でお客様データ管理はお客様の責任でお願いしています。補償については、ゲンバト利用規約をご確認ください。 |
| 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 | ○ | ゲンバトで利用するデータは、サービス解約時にCSVファイルで返却することが可能です。その後、当社ではデータ削除操作を実施します。 |
| 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 | ○ | データはお客様の責任でデータ内容の確認をいただきます。 |
| 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 | ○ | 入力項目の要件に合わせて形式や長さのチェックを行っています。 |
| セキュリティ | | | | |
| 39 | 公的認証取得の要件 | 第三者によ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認証（ISO27001）を取得しています。 |
| 40 | アプリケーションに関する第三者評価 | 第三者によるウェブアプリケーション脆弱性評価実施 | ○ | 定期的に、第三者による脆弱性検査を受け、その報告を受け、評価及び対応を実施しています。 |
| 41 | 情報取扱い環境 | 提供者側でのデータ取扱い環境が適切に確保されていること | ○ | 情報セキュリティ管理者がアクセス権を管理しており、通常はサーバーにアクセスする権限はありません。ただし、メンテナンス等でアクセスする必要がある場合は、許可を得たスタッフのみがアクセスできるようになります。 |
| 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 | ○ | TLS1.3およびTLS1.2にて通信を暗号化しています。TLS1.0、TLS1.1は使用していません。 |
| 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」 | ○ | 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 | ○ | お客様の契約スペースごとに論理的に分離されたデータ領域で運用しています。 |
| 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 | ○ | 利用者のデータにアクセスできる社員等は情報セキュリティ管理者の許可を得た者に限っております。 |
| 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 | ○ | ユーザーIDごとにログを取得し、記録を確認することが可能ですが、お客様に提供することはできません。 |
| 47 | ウイルススキャン | ウイルススキャンの頻度 | ○ | 接続端末すべてにはウイルス対策ソフトを導入して、常時チェックを行っています。システム側も常時チェックを行っています。 |
| 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 | ○ | 二次記憶媒体を使用せず、データセンター間でバックアップを取っています。また、バックアップへのアクセスは管理者権限をもって情報セキュリティ管理者が管理しております。スタッフの端末にはモバイルデバイス管理を導入し、外部記憶媒体の使用を原則として禁止しています。 |
| 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 | ○ | ISMSで法令チェックしています。 |