クラウドサービス
セキュリティガイドライン

おまかせロボ

Version 1.0

2026年1月

株式会社テックハブ

目次

はじめに

本ガイドラインは、株式会社テックハブ（以下「当社」）が提供するSaaS型AI業務自動化サービス「おまかせロボ」（以下「本サービス」）のセキュリティ対策について説明することを目的としています。

本ガイドラインは、JIS Q 27017:2016（ISO/IEC 27017:2015）「JIS Q 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」に準拠して作成しています。

お客様が安心して本サービスをご利用いただけるよう、クラウドサービス固有のセキュリティ管理策について明記しています。

1. お客様との責任分界点

本サービスは、SaaS（Software as a Service）型のクラウドサービスとして提供されます。本章では、お客様と当社の責任範囲について説明します。

1-1. 責任分界

本サービスにおける責任分界は以下のとおりです。

項目	お客様	当社
利用環境	●	
端末のセキュリティ対策	●	
ネットワーク環境の整備	●	
サービス基盤		●
アプリケーションの開発・保守		●
インフラストラクチャの運用		●
セキュリティパッチの適用		●
データ管理		●
データの暗号化（保存時・通信時）		●
データのバックアップ		●
監視・運用		●

システム監視		●
インシデント対応		●
脆弱性管理		●

1-2. お客様の責任範囲

お客様には以下の責任を担っていただきます。

- 利用端末のセキュリティ対策
- 不審な活動を発見した場合の速やかな報告

1-3. 当社の責任範囲

当社は以下の責任を担います。

- サービス基盤の安全な運用
- お客様データの適切な保護
- セキュリティインシデントへの対応
- サービスの可用性の確保
- 法令・規制への準拠

2. 情報セキュリティのための方針群

2-1. 情報セキュリティのための方針群（項番：5.1.1）

当社は、情報セキュリティ基本方針を定めて運用しています。

情報セキュリティ基本方針には以下の内容を含みます。

- 情報セキュリティの目的と原則
- 経営層のコミットメント
- セキュリティ管理体制
- 従業員の責任と義務
- 法令・契約上の要求事項の順守
- 継続的な改善

情報セキュリティ基本方針は、定期的（年1回以上）または重大な変更が生じた場合にレビューし、必要に応じて改訂します。

3. 情報セキュリティのための組織

3-1. 情報セキュリティの役割及び責任（項番：6.1.1）

当社は、情報セキュリティに関する役割と責任を明確に定義し、適切な要員を割り当てています。

役割	責任
経営層	情報セキュリティ方針の承認、リソースの確保
情報セキュリティ責任者	セキュリティ施策の統括、インシデント対応の指揮
システム管理者	システムのセキュリティ設定・運用
開発担当者	セキュアな開発の実施

3-2. 関係当局との連絡（項番：6.1.3）

セキュリティインシデント発生時に備え、以下の関係当局との連絡体制を整備しています。

- 所管官庁
- JPCERT/CC（JPCERTコーディネーションセンター）
- IPA（独立行政法人情報処理推進機構）

データ保管場所

本サービスのお客様データは、以下の場所に保管されます。

項目	内容
クラウドプロバイダー	Amazon Web Services（AWS）
リージョン	アジアパシフィック（東京）リージョン（ap-northeast-1）
所在国	日本国内

3-3. クラウドコンピューティング環境における役割及び責任の共有及び分担（項番：CLD.6.3.1）

本サービスはSaaS型クラウドサービスとして提供され、お客様と当社の責任分界は「1. お客様との責任分界点」に記載のとおりです。

当社は、クラウドサービスプロバイダー（AWS）との間でも責任を分担しており、AWSは以下の責任を担います。

- 物理的なインフラストラクチャのセキュリティ
- ハイパーバイザーレベルのセキュリティ
- ネットワークインフラストラクチャのセキュリティ

4. 資産の管理

4-1. クラウドサービスカスタマの資産の除去（項番：CLD.8.1.5）

契約終了後、お客様データは適切な期間内に削除します。

5. 利用者アクセスの管理

5-1. 利用者登録及び登録削除（項番：9.2.1）

本サービスにおけるユーザーアカウントの登録・削除は、当社のシステム運用者が実施します。

- ユーザー登録時は、必要最小限の情報のみを取得します
- ユーザー削除時は、関連するデータも適切に処理されます
- 削除されたユーザーの認証情報は無効化されます

5-2. 利用者アクセスの提供（項番：9.2.2）

本サービスは、ロールベースアクセス制御（RBAC）を採用しています。

ロール	権限概要
管理者	すべての機能へのアクセス
その他	ロボごとに取り決め

5-3. 特権的アクセス権の管理（項番：9.2.3）

管理者権限を持つユーザーについては、以下の管理を行います。

- 管理者アカウントは必要最小限の人数に制限することを推奨します
- 管理者アカウントには多要素認証の有効化を強く推奨します
- 管理者による操作は監査ログに記録されます

5-4. 利用者の秘密認証情報の管理（項番：9.2.4）

本サービスにおける認証情報の管理は以下のとおりです。

パスワード管理

- パスワードは業界標準のハッシュアルゴリズム（bcrypt）で保存されます
- パスワードポリシーにより一定以上の強度を要求しています
  - 最小文字数：12文字以上
  - 英大文字・小文字・数字の組み合わせ

多要素認証（MFA）

- TOTP（Time-based One-Time Password）に対応しています
- すべてのユーザーに多要素認証の有効化を推奨しています

5-5. 特権的なユーティリティプログラムの使用（項番：9.4.4）

本サービスの運用において、特権的なユーティリティプログラムへのアクセスは、承認された運用担当者のみに制限しています。

- 特権操作はすべてログに記録されます
- 特権アカウントの使用は定期的にレビューされます

6. 暗号

6-1. 暗号による管理策の利用方針（項番：10.1.1）

本サービスでは、お客様データを保護するために以下の暗号化を実施しています。

通信の暗号化

項目	内容
プロトコル	HTTPS（HTTP over TLS）
TLSバージョン	TLS 1.2以上（TLS 1.3推奨）
暗号スイート	最新の安全な暗号スイートを使用
証明書	信頼された認証局発行の証明書を使用

- HSTS（HTTP Strict Transport Security）を有効化しています

- 脆弱な暗号スイートは無効化しています

保存データの暗号化

- 暗号アルゴリズム：AES-256
- お客様データはすべて暗号化して保存されます
- バックアップデータも同様に暗号化されます

7. 運用セキュリティ

7-1. 変更管理（項番：12.1.2）

本サービスへの変更は、以下の管理プロセスに従って実施されます。

- 変更内容のレビューと承認
- テスト環境での検証
- ステージング環境でのリリース前確認
- 本番環境へのデプロイ
- デプロイ後の監視

緊急性の高い変更（セキュリティパッチ等）についても、簡略化された承認プロセスを経て実施されます。

7-2. 情報のバックアップ（項番：12.3.1）

本サービスでは、以下のバックアップを実施しています。

項目	内容
バックアップ頻度	日次（自動）
保持期間	30日間
保管場所	同一リージョン内の異なるアベイラビリティゾーン
暗号化	AES-256で暗号化して保管

- バックアップからのリストアテストを定期的に実施しています
- 障害発生時には、直近のバックアップからデータを復旧可能です

7-3. クロックの同期（項番：12.4.4）

本サービスのすべてのシステムは、NTP（Network Time Protocol）を使用して時刻を同期しています。

7-4. 技術的ぜい弱性の管理（項番：12.6.1）

本サービスでは、以下の脆弱性管理を実施しています。

- 定期的な脆弱性スキャン（週次）
- 依存ライブラリの脆弱性監視（継続的）
- 発見された脆弱性の重要度に応じた対処
  - 緊急（Critical）：24時間以内
  - 高（High）：7日以内
  - 中（Medium）：30日以内
  - 低（Low）：次回定期メンテナンス時

8. システムの取得、開発及び保守

8-1. 情報セキュリティ要求事項の分析及び仕様化（項番：14.1.1）

本サービスの開発において、セキュリティ要求事項を以下のとおり定義しています。

- 認証・認可機能の実装
- 入力値の検証（バリデーション）
- 出力値のエスケープ処理
- セッション管理
- エラーハンドリング（情報漏洩の防止）
- ログ記録

8-2. セキュリティに配慮した開発のための方針（項番：14.2.1）

本サービスの開発は、以下の方針に従って実施されます。

セキュアコーディング

- OWASP Top 10を考慮した開発
- コードレビューの実施
- 静的コード解析ツールの使用

開発環境の分離

- 開発環境、テスト環境、本番環境を分離
- 本番データの開発環境での使用禁止
- アクセス権限の環境ごとの分離

テスト

- 単体テスト、結合テストの実施
- セキュリティテストの実施
- リリース前の脆弱性診断

9. 供給関係者

9-1. 供給関係者のための情報セキュリティ方針（項番：15.1.1）

当社は、サービス提供に関わる供給者（クラウドプロバイダー等）に対し、以下の要件を定めています。

- 情報セキュリティに関する方針・手順の整備
- 適切なセキュリティ認証の取得
- インシデント発生時の報告義務
- 契約終了時のデータ取り扱い

9-2. 供給者との合意におけるセキュリティの取り扱い（項番：15.1.2）

主要な供給者であるAWSは、以下のセキュリティ認証を取得しています。

認証・規格	内容
SOC 1/2/3	サービス組織の内部統制
ISO 27001	情報セキュリティマネジメントシステム
ISO 27017	クラウドサービスのセキュリティ
ISO 27018	パブリッククラウドにおける個人情報保護
PCI DSS	ペイメントカード業界データセキュリティ基準

当社は、供給者のセキュリティ状況を定期的にレビューしています。

10. 情報セキュリティインシデントの管理

10-1. 責任及び手順（項番：16.1.1）

当社は、セキュリティインシデント対応手順を整備しています。

インシデント対応フロー

1. **検知・報告**: システム監視またはユーザー報告による検知
2. **初動対応**: 影響範囲の特定、被害拡大の防止
3. **調査・分析**: 原因の特定、影響の評価
4. **復旧**: サービスの復旧、データの復元
5. **事後対応**: 根本原因の解消、再発防止策の実施

お客様への通知

お客様データに影響を及ぼすインシデントが発生した場合、以下のとおり通知します。

- 発覚後速やかに第一報を通知
- 調査の進捗に応じて続報を通知
- 対応完了後に最終報告を通知

10-2. 証拠の収集（項番：16.1.7）

インシデント発生時の証拠収集について、以下のとおり対応します。

- インシデントに関連するログの保全
- 証拠の完全性を維持するための手順
- 法的手続きに備えた証拠の管理

ログは改ざん防止措置を講じて保管されています。

11. 法令及び契約上の要求事項の順守

11-1. 記録の保護（項番：18.1.3）

本サービスでは、以下の記録を保護・保管しています。

記録の種類	保管期間	目的
アクセスログ	30日間	セキュリティ監視、インシデント調査

操作ログ	30日間	監査証跡、トラブルシューティング
認証ログ	30日間	不正アクセスの検知
システムログ	30日間	システム運用、障害対応

11-2. 暗号化機能に対する規則（項番：18.1.5）

本サービスで使用する暗号化は、以下の規則に準拠しています。

用途	暗号方式
通信暗号化	TLS 1.2以上
保存データ暗号化	AES-256
パスワードハッシュ	bcrypt

電子政府推奨暗号リスト（CRYPTREC暗号リスト）に記載された暗号方式を使用しています。

11-3. 情報セキュリティの独立したレビュー（項番：18.2.1）

当社は、情報セキュリティの取り組みについて、以下のレビューを実施しています。

- 内部監査（年1回以上）
- 脆弱性診断（年1回以上）
- 情報セキュリティ方針の定期レビュー（年1回以上）

お問い合わせ

セキュリティに関するご質問・お問い合わせは以下までご連絡ください。

株式会社テックハブ

項目	内容
メールアドレス	info@tech-hub.co.jp
Webサイト	https://tech-hub.co.jp

改訂履歴

版数	改訂日	改訂内容
1.0	2026年1月	初版発行
