No.	種別	サービスレベル項目例	規定内容	測定単位	回答欄
補足説明 →		サービス提供側に 確認すべき項目	サービス提供側に 確認すべき項目の内容	サービス提供側に 求める回答の単位	サービス提供側からの 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）	時間帯	24時間365日（計画停止／定期保守を除く） ※月次の自動評価は毎月1日に前月分を処理
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】 サービスに影響する計画停止や機能の変更を行う場合は、緊急時を除き、事前にメールで通知する。
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ないが、サービスを終了する場合は6か月前までにWebサイト／メールで通知する。
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】 プログラム等の第三者への預託は実施しない。 評価結果（レポート）はPDFでダウンロード可能。
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（%）	2026年10月提供開始のため、稼働率の実績値はなし。 基盤のAmazon Web Services（AWS）の各サービスは、AWSが定めるSLAに基づき提供されている。
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】 データの保管（Amazon S3）、認証（Amazon Cognito）、管理サイトは、AWS東京リージョンの複数のアベイラビリティゾーンで冗長化されたマネージドサービスを利用。 システム構成はコード（AWS CDK）で管理しており、再構築が可能。 ※復旧訓練は現時点で未実施
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	有無	【無】 現時点で代替措置の準備予定はなし。
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	【無】 現時点で代替措置の準備予定はなし。
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】 ソースコードとシステム構成をコードで管理し、自動テストを通過した変更のみを本番環境に反映する。 サービスに影響する変更は、事前にメールで通知する。
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	2026年10月提供開始のため、実績値はなし。
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	非開示

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	2026年10月提供開始のため、実績値はなし。
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】 Amazon CloudWatchでシステムのエラー・処理の失敗を監視し、異常を検知した場合は担当者へメールで自動通知する。
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】 障害発生時は、お客様のご担当者様へメールまたは電話で通知する。
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	当社への通知：検知後、数分以内（自動） お客様への通知：当社営業時間内に、メールまたは電話で可能な限り速やかに実施
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	時間（分）	1回／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	障害発生時はメールまたは電話で報告。障害が継続する場合は、必要に応じて1日1回を目安に報告。
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	【無】 利用者がログをダウンロードする機能はなし。 必要に応じて、当社で保管しているログから調査し報告する。
19	性能	応答時間	処理の応答時間	時間（秒）	非開示
20		遅延	処理の応答時間の遅延継続時間	時間（分）	非開示
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）	【目安】 手動評価：通話5分あたり数分程度 月次評価：毎月1日中に前月分の処理を完了
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】 取引先ごとに次の項目を設定可能。 ・評価項目と評価基準（お客様の評価シートに合わせた設定） ・採点の厳しさ（4段階） ・1か月あたりの評価件数 ・二段階認証（認証アプリ）の必須化
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】 YOMEL（Webhook・REST API）と連携可能。 その他の連携は担当者にお問い合わせください。
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		特に上限は設けていない（ご契約内容に基づく合理的な範囲）。
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	手動評価：取引先ごとに1か月あたりの利用時間（分）の上限を設定 アップロード：1回5ファイルまで、1ファイル200MB・60分まで

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9時～18時（メール・電話）　※当社休業日を除く
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9時～18時（メール・電話）　※当社休業日を除く
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】 ・Amazon S3のバージョニングにより、データを変更・削除する前の版を7日間保持し、誤操作や障害の際に当社が復元できる ・データはAWS東京リージョンの複数のアベイラビリティゾーンに自動で冗長保存される（AWSが公表する設計上の耐久性：99.999999999%） ・対象：通話のテキスト、評価結果、設定（手動評価の音声は評価後すぐに削除するため対象外）
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	随時（データを変更・削除する直前の版を保持）
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
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】 ・サービス解約後、30日以内にデータを削除 ・削除の完了は、必要に応じて書面で報告
32		バックアップ世代数	保証する世代数	世代数	7日間に作成されたすべての版（世代数の上限なし）
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】 保存データはAES-256で暗号化して保管。
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】 AWSが管理する暗号化キー（Amazon S3 SSE-S3）を使用。個別のキーの受け入れ等はなし。
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】 補償は利用規約に記載のとおり。サイバー保険に加入している。
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】 サービス解約時は、当社の手順に沿ってデータを削除する。 評価結果（レポート）は、ご契約期間中に管理サイトからPDFでダウンロード可能。
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	【無】 ただし、保管データの改ざん等の不正があった際の調査のためのログは確認できる。

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】 手動評価の音声ファイルは、形式（WAV／MP3／M4A）・サイズ・長さを制限。 その他の入力値もサーバー側で検証を実施。
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	有無	ISO/IEC 27001（ISMS）認証取得 ※本サービスの運営は当社の認証範囲に含まれる
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】 第三者による Web アプリケーション脆弱性診断実施（2026年10月、緊急・重大・高・中の検出なし）
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】 AWSのデータセンターを利用（物理的なセキュリティはAWSが管理。AWSはISO/IEC 27001、SOC等の第三者認証を取得）。
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】 通信はすべてTLS1.2以上で暗号化。
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】 ※AWSの第三者監査報告書（SOC報告書等）は、AWS Artifactから入手可能。
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】 データは取引先ごとに区分して保存し、アカウントに紐づく取引先以外のデータにはアクセスできないよう制御している。 ただし、同一の基盤で運用しているため、基盤の障害は共通して影響を受けることがある。
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】 AWS環境を操作できる担当者を限定し、必要最小限の権限を付与している。
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	利用者ごとに個別のアカウント（メールアドレス）を付与し、ログから調査可能。 ・管理サイトのログ：1年間保持 ・システムの処理ログ：3か月間保持 ・AWSの操作履歴（AWS CloudTrail）：90日間保持
47		ウイルススキャン	ウイルススキャンの頻度	頻度	【無】 サーバーレス構成のため、常時稼働するサーバーはなし。 アップロードされた音声ファイルは形式・サイズを制限し、評価後すぐに削除する。

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】 データは冗長化されたクラウドストレージに暗号化した状態で保管。 物理的な記憶媒体の管理・廃棄はAWSが実施。
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	把握している。 データはすべて日本国内で保管・処理している。
50	データセンター	データの所在地	サーバーおよびデータ保管先の所在地はどこか。	所在地	日本国内（AWS 東京リージョン） 生成AIによる処理は、日本国内のリージョン（東京・大阪）で実施。 海外での処理・保管はなし。
51		データの再委託	各顧客データ・顧客が入力したデータ取扱いの第三者委託はあるか。		【有】 利用規約に記載のとおり、クラウドサービス（AWS）の利用を含む再委託を実施。
52		データセンター入館管理	入退室管理されたコンピュータルームの施錠管理されたラック等、明示的に許可された者以外は触れない環境に設置されているか。	有無	【有】 AWSのデータセンターを利用（入退室管理・監視等の物理的なセキュリティはAWSが管理）。
53		データセンター監査	ユーザーによるデータセンター訪問、監査を受け付けるか。	可否	【否】 AWSの第三者監査報告書（AWS Artifact）で代替。必要に応じて書面で回答。
54	セキュリティ	脆弱性への対応	セキュリティパッチを適用する等、サーバの脆弱性対策を遅滞なくかつ定期的に実施しているか。	頻度	サーバーレス構成のため、サーバーのOS・実行環境へのパッチ適用はAWSが実施。 当社が用意する実行環境・ライブラリは定期的に更新し、緊急性の高い脆弱性は速やかに対応する。
55		アクセス経路の制限	ファイアウォール等のアクセス制御を行い、公開する必要のない通信ポートは閉じているか。	有無	【有】 ・外部に公開しているのは、管理サイトとYOMELからのデータ受信口（いずれもHTTPS）のみ ・保管データへのインターネットからのアクセスはすべて遮断 ・YOMELへの接続は固定IPアドレスからのみ実施
56		不正なアクセスに対する対策	侵入・改ざん・Dos攻撃を検知し制御する仕組みがあるか。	有無	【有】 ・Amazon GuardDutyによる不正アクセス・脅威の検知（重要度が中以上の場合は担当者へ自動通知） ・短時間の大量アクセスを制限（API Gateway） ・YOMELからのデータ受信時に署名（HMAC-SHA256）と送信時刻を検証 ・ログイン失敗が続いた場合は一時的にロック ・保管データの改ざん等の不正があった際の調査のためのログは確認できる

57		不要な表示の有無	公開する必要のないディレクトリ・ファイル・設定情報は外部から不可視とし、必要のない機能は、停止する等の措置がされているか。	有無	【有】 ディレクトリ一覧やエラーの詳細は外部に表示しない。 不要な接続口（AWSの既定のAPIエンドポイント等）は無効化している。
58		セキュリティ検査	公開前にセキュリティ検査を実施し、提供に適した状態であることを確認し報告を提出できるか。	有無	【有】 公開前に自動テストと動作確認を実施。第三者による Web アプリケーション脆弱性診断も実施済み（2026年10月）。必要に応じて書面で回答。
59		ログの保持	利用者の活動、セキュリティ事象と関連するログ期間はどのくらいか。	期間	管理サイトのログ：1年間、システムの処理ログ：3か月間、AWSの操作履歴：90日間保持
60	体制	内部不正についての対策1	人的な対策はどのようなものを行っているか。	対応状況	ISMSに基づき、入社時および定期的に情報セキュリティ教育を実施。
61		内部不正についての対策2	従業員が契約者のデータへ不必要に、許可なくアクセスすることへの抑止力はあるか。	対応状況	利用者のデータにアクセスできる担当者は限定しており、お問い合わせ対応・障害調査など業務上必要な場合に限りアクセスする。
62		内部事故についての対策	データの持ち出し・紛失への対策はあるか。	対応状況	ISMSの規程に基づき、情報の持ち出し・記憶媒体の利用を管理している。
63		ユーティリティ表示	現在のシステム稼働状況を視認できるページは準備されているか	有無	【無】 障害発生時は、お客様のご担当者様へメールまたは電話で通知。
64		セキュリティ領域の確保	オフィスの物理的セキュリティ領域を設け、出入りを管理しているか。	有無	【有】 ISMSに基づき、オフィスにセキュリティ区画を設け、入退室を管理している。
65		セキュリティに関する外部からの指導	契約者の指示による情報管理体制の改善等の指導を受け入れられるか。	可否	原則として受け入れていない。 必要に応じて書面で回答。
66		事故発生時の外部監査	セキュリティインシデント発生時、契約者による外部監査を受け入れられるか。	可否	監査については、基本的にチェックシート・書面での対応とする。
67	機能	パスワード定期変更	パスワードに有効期限を設け、再発行を強制する仕組みがあるか。	有無	【無】
68		パスワード強度	十分な強度のパスワード文字列が設定できるか。	有無	【有】 10文字以上、英小文字と数字を必須（英大文字・記号も使用可）。
69		多要素認証	ID/PW以外の本人認証の仕組みを設けているか。	有無	【有】 認証アプリ（TOTP）による二段階認証を用意。取引先ごとに必須化が可能。
70		アカウントロック	一定回数ログインに失敗した場合に、アカウントを無効化またはロックする機能が提供されているか。	有無	【有】 ログインの失敗が続くと、一時的にログインできなくなる（時間の経過で自動解除）。 管理者は利用者のアカウントを無効化できる。

71		アクセス制限	利用環境において、第三者がアクセス出来ない仕組みがあるか。	有無	【有】 ログインした利用者のみ閲覧可能。取引先ごとにデータを分離。 IP制限・端末単位でのアクセス制限の機能はなし。
72		アクセス権限管理	管理者毎のアクセス権限を制御する機能があるか。	有無	【有】 アカウントの種類は「管理者」「閲覧者（SV）」「オペレーター」の3種類。 オペレーターはご本人のレポートのみ閲覧可能、管理者は自社の利用者の追加・変更が可能。

改訂履歴	日付	改訂内容
初版（Ver1.0）	2026.10.19	Cynet Eva 版として作成
Ver1.1	2026.10.21	No.40・58 を更新（第三者による脆弱性診断を実施）
Ver1.2	2026.10.27	No.22・69 を更新（二段階認証を認証アプリに一本化）