本チェックシートはアーニーＭＬＧ株式会社が提供する「YOMEL」のセキュリティ対策を表記したものです。
本チェックシートの項目は、それぞれ経済産業省が公開している内容を元に作成したものとなります。
「クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年版」を元に任意で項目修正を加えて作成したチェックシートです。
https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf

アーニーＭＬＧ株式会社は、JIS Q 27001:2014(ISO/IEC 27001:2013)の要件事項に適合し、認証登録番号IS767963を保有しています。

各種URLリスト
会社Webサイト： https://ernie.co.jp/
情報セキュリティポリシー： https://ernie.co.jp/policy

YOMEL(議事録利用)
利用規約： https://ai.yomel.co/gijiroku/terms
プライバシーポリシー： https://ai.yomel.co/gijiroku/privacy
サポートサイト： https://support.ai.yomel.co/

YOMEL for コールセンター
利用規約： https://ai.yomel.co/terms
プライバシーポリシー： https://ai.yomel.co/privacy
サポートサイト： https://support-cc.ai.yomel.co/

登録部門	アーニーＭＬＧ株式会社
認証基準	ISO/IEC 27001:2013/JIS Q 27001:2014
認証登録番号	IS 767963
認証登録範囲	音声認識、AIの研究・開発、Webサービスの開発・運用
初回登録日	2022年09月21日
認証登録機関	BSIグループジャパン株式会社

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）
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】 7日前までにWebサイト及びメールにて通知
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、サービス終了する場合は6ヶ月前にWebサイト/メールにて事前通知

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ません。 データについては、ダウンロードするためのツールを提供します。
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	稼働率（%）	サービス稼働率の実績値：99.9% （2023年実績）
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】 ・１回／年以上で訓練を実施
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ありません。 現在、遠隔地保管の仕組みを検討中です。
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	【無】 現時点で代替措置の準備予定はありません。
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	有無	【有】 ・システムアップデートは1ヶ月に1回のメンテナンスにて実施 ・重要なセキュリティパッチは3ヶ月に1回を目処に必要に応じて適用 ・緊急性の高い脆弱性情報への対応が必要と判断される際には緊急メンテナンスにてパッチ適用
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	公開しておりません。
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	公開しておりません。
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	2023年4月～2024年3月の１年間の実績は3回/0回でした。
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】 死活監視を行いながらオートスケーリングの仕組みを構築しています。同時に管理者への通知を行い、必要に応じて手動対応を実施します。
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】 webサイトでの障害情報掲示、指定連絡先へのメールでの連絡
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	当社への通知は通常数分以内に行われます。お客様への通知は、当社担当者から可能な限り速やかに実施します。 （目標通知時間） 営業時間内： 障害発生から1時間以内 営業時間外： 障害発生から8時間以内
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	24時間 必要に応じて、Webサイトへの掲示もしくはメールで報告を行います。
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】 監査ログとしてシステムへのアクセスログをシステムからダウンロードが可能です。
19	性能	応答時間	処理の応答時間	時間（秒）	公開しておりません。
20		遅延	処理の応答時間の遅延継続時間	時間（分）	公開しておりません。
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）	公開しておりません。

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	申請及びオプション機能があります。 ・オプトアウト申請 ・SSO認証（100,000円～）
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	【無】
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		ご契約のライセンス所有ユーザ数を上限とした同時接続を保障します。
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	同時接続数、月間利用時間数(ライセンスによる)
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）
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時～17時（メール）　※弊社の休業日を除く
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】 ・日次でバックアップを取得し、7世代保管します ・バックアップ先の提示、復旧方式については提示しておりません ・バックアップデータからのお客様データの抽出等は承っていません
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	担当者にお問い合わせください。
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、速やかに論理的にディスク内のデータを消去 ・削除したことの証明書は必要に応じて提供可能（別途、手数料がかかる場合があります）
32		バックアップ世代数	保証する世代数	世代数	7世代
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によって暗号化され、保管されています
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】 マルチテナントストレージは全顧で単一のキーを利用します。
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】
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】 サービス解約時のデータ破棄手順を含むフローを定めて運用しています。受託情報の返還/取り出しが必要な場合は、個別に申込みの上、別途契約が必要です。
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	【無】 ただし、保管データの改ざん等不正があった際の調査のためのログは確認できる仕組みがあります
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】 ユーザーから入力される情報は必要に応じてバリデーションを実施します。
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	JIS Q 27001:2014 (ISO/IEC 27001:2013)
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	1年に1回実施を目安に第三者によるアプリケーション脆弱性診断を実施。最終診断：2023年12月

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】 ・データセンター専用建物を利用しており関係者以外の立ち入りは不可 ・入退室管理・記録の実施 ・警備員の常駐、監視カメラの常時監視
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による暗号化を実施
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】
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	【無】 同一プラットフォーム内でマルチテナント管理しております。アカウント管理により、アクセス可能なテナントは限定されていますが、サイバー攻撃等により共通で影響が出ることがあります。
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】 データの取扱は最小権限の原則に則った付与を徹底するとともに、社内ネットワークのみのアクセス制限や多要素認証の導入等でアクセスを制限しています。
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	保管しているログから調査可能です。 Webアクセスログ、システム操作ログなどを最低1年間保持しています。
47		ウイルススキャン	ウイルススキャンの頻度	頻度	週次
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】 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を実施。USBポートを利用した記録デバイス利用は禁止しています。
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	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ます。
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	原則、国内。 要約オプションを利用される場合は国外（豪州、米国）へデータが送信され一定期間保持されます。
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】利用規約記載の通り、クラウドサービスの利用を含む、再委託を実施します。
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】 ・JDCCファシリティスタンダード ティア4相当 ・データセンター専用建物を利用しており、関係者以外の立ち入りは不可 ・入退室管理を実施 ・警備員の常駐、監視カメラの常時監視
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】 必要に応じて書面回答をベースとさせていただきます。
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	・重要なセキュリティパッチは3ヶ月に1回を目処に必要に応じて適用 ・緊急性の高い脆弱性情報への対応が必要と判断される際には緊急メンテナンスにてパッチ適用

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】 ・ファイヤーウォールポリシーによる通信制限、遮断及びWAFによる不正アクセスの遮断 ・公開する必要のない通信ポートは閉じています。
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】 ・AWS Security Hub/GuardDuty 導入 ・IPSの導入 ・保管データの改ざん等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】
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】 必要に応じて書面回答をベースとさせていただきます。
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	Webアクセスログ、システム操作ログなどを必要に応じて最低1年間保持しています。
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	入社時および定期的なe-ラーニング受講と周知を実施
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社員等はセキュリティ管理者の許可を得た者に限定
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	紙媒体及びUSB記憶機器の利用を禁止しており、預託データへのアクセスログは全て保存と監視を実施
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】 障害発生時にはサポートサイトにて掲示します。
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】 オフィスにおいて情報を取り扱う業務においてはセキュリティエリアを設け、該当領域へ立ち入りする人物は識別し入退室管理している
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	基本的には受け入れしていません。必要に応じて書面回答をベースとさせていただきます。
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ベースでの監査をお願いしております。
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】英/数/記号の3種必須、10文字以上32文字以下
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	【無】
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】 10回間違えるとアカウントがロックされ、管理者画面からロック解除が必要
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】 IP制限の設定が可能。端末単位でのアクセス制限はなし
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】 ユーザーアカウントの種類には管理者・マネージャー・スタッフの３つを準備しており、御社の体制に沿ったアクセス制御が可能

改訂履歴	日付	改訂内容
初版	2023.08.18	
Ver1.1	2023.12.07	No.50 データの所在地の変更
Ver1.2	2024.05.02	最新の情報に更新（No.5,6,7,12,22,40,46,68）
Ver1.3	2024.06.07	最新の情報に更新（No.59）