aiESG for CDP

セキュリティチェックシート（記入済み）

対象サービス	aiESG for CDP
提供者	株式会社aiESG
回答日	2026年10月16日
版数	1.0

本書について

本書は、株式会社aiESG（以下「当社」）が提供する「aiESG for CDP」（以下「本サービス」）のセキュリティ対策の概要を説明するものです。

本書は概要であり、当社による個別の保証を構成するものではありません。本サービスの利用条件は、利用規約および個別の合意（利用申込書の特記事項、覚書等）によります。

本書で引用する利用規約の条項は、aiESG for CDP 利用規約（2027年版）に基づきます。

本書の内容は、対策の見直し等により予告なく更新することがあります。最新版は当社ウェブサイトのセキュリティ情報ページでご確認ください。

記載の方針

対策の有無と方針の水準で記載しています。暗号方式・製品名の詳細・ネットワーク構成等の技術情報は記載していません。

「セキュリティ上の理由により非公開（個別のご依頼時にご案内）」と記載した項目は、個別のご依頼に応じてご案内します。

シート構成

IPA：IPA「安全なウェブサイトの作り方 改訂第7版」に基づく項目

経済産業省：経済産業省「クラウドサービスレベルのチェックリスト」（2010年8月）に基づく項目

総務省：総務省「ASP・SaaSの安全・信頼性に係る情報開示指針（ASP・SaaS編）第3版」および「AIを用いたクラウドサービスの安全・信頼性に係る情報開示指針（ASP・SaaS編）」に基づく項目

追加項目：上記の指針に含まれない項目（生成AI、多要素認証、クラウド設定、サプライチェーン、情報セキュリティマネジメント、AIマネジメント）

出典

本書は、一般社団法人日本クラウド産業協会（ASPIC）の「クラウドサービスの安全・信頼性に係る情報開示認定制度」の認定を受けたものではありません。

お問い合わせ

本書に関するお問い合わせ、および非公開項目のご案内のご依頼は、当社ウェブサイトのお問い合わせ窓口までご連絡ください。

© 2026 aiESG, Inc.

IPA「安全なウェブサイトの作り方」に基づく回答

株式会社aiESG　回答日：2026年10月16日　版数：1.0

IPA（独立行政法人情報処理推進機構）「安全なウェブサイトの作り方 改訂第7版」のチェックリストに基づき、本サービスの対策状況を記載しています。対応状況は「対応済」「未対策」「対応不要」のいずれかで示します。

No	脆弱性の種類	区分	対策の性質	実施項目	番号	対応状況	補足（脆弱性ごと）
1	SQLインジェクション		根本的解決	SQL文の組み立ては全てプレースホルダで実装する。	1-(i)-a	対応済	開発工程でセキュリティ要件のレビューとソースコードのレビューを行い、本脆弱性への対策を講じています。個別の実施項目ごとの状況はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
			根本的解決	SQL文の構成を文字列連結により行う場合は、アプリケーションの変数をSQL文のリテラルとして正しく構成する。	1-(i)-b	対応不要	
			根本的解決	ウェブアプリケーションに渡されるパラメータにSQL文を直接指定しない。	1-(ii)	対応済	
			保険的対策	エラーメッセージをそのままブラウザに表示しない。	1-(iii)	対応済	
			保険的対策	データベースアカウントに適切な権限を与える。	1-(iv)	未対策	
2	OSコマンド・インジェクション		根本的解決	シェルを起動できる言語機能の利用を避ける。	2-(i)	対応済	開発工程でセキュリティ要件のレビューとソースコードのレビューを行い、本脆弱性への対策を講じています。個別の実施項目ごとの状況はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
			保険的対策	シェルを起動できる言語機能を利用する場合は、その引数を構成する全ての変数に対してチェックを行い、あらかじめ許可した処理のみを実行する。	2-(ii)	対応不要	
3	パス名パラメータの未チェック／ディレクトリ・トラバーサル		根本的解決	外部からのパラメータでウェブサーバ内のファイル名を直接指定する実装を避ける。	3-(i)-a	対応済	開発工程でセキュリティ要件のレビューとソースコードのレビューを行い、本脆弱性への対策を講じています。個別の実施項目ごとの状況はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
			根本的解決	ファイルを開く際は、固定のディレクトリを指定し、かつファイル名にディレクトリ名が含まれないようにする。	3-(i)-b	対応済	
			保険的対策	ウェブサーバ内のファイルへのアクセス権限の設定を正しく管理する。	3-(ii)	対応済	
			保険的対策	ファイル名のチェックを行う。	3-(iii)	対応済	
4	セッション管理の不備		根本的解決	セッションIDを推測が困難なものにする。	4-(i)	対応済	開発工程でセキュリティ要件のレビューとソースコードのレビューを行い、本脆弱性への対策を講じています。個別の実施項目ごとの状況はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
			根本的解決	セッションIDをURLパラメータに格納しない。	4-(ii)	対応済	
			根本的解決	HTTPS通信で利用するCookieにはsecure属性を加える。	4-(iii)	対応済	
			根本的解決	ログイン成功後に、新しくセッションを開始する。	4-(iv)-a	対応済	
			根本的解決	ログイン成功後に、既存のセッションIDとは別に秘密情報を発行し、ページの遷移ごとにその値を確認する。	4-(iv)-b	対応不要	
			保険的対策	セッションIDを固定値にしない。	4-(v)	対応済	
			保険的対策	セッションIDをCookieにセットする場合、有効期限の設定に注意する。	4-(vi)	対応済	

© 2026 aiESG, Inc.

No	脆弱性の種類	区分	対策の性質	実施項目	番号	対応状況	補足（脆弱性ごと）
5	クロスサイト・スクリプティング	HTMLテキストの入力を許可しない場合の対策	根本的解決	ウェブページに出力する全ての要素に対して、エスケープ処理を施す。	5-(i)	対応済	開発工程でセキュリティ要件のレビューとソースコードのレビューを行い、本脆弱性への対策を講じています。個別の実施項目ごとの状況はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
		HTMLテキストの入力を許可しない場合の対策	根本的解決	URLを出力するときは、「http://」や「https://」で始まるURLのみを許可する。	5-(ii)	対応済	
		HTMLテキストの入力を許可しない場合の対策	根本的解決	<script>...</script> 要素の内容を動的に生成しない。	5-(iii)	対応済	
		HTMLテキストの入力を許可しない場合の対策	根本的解決	スタイルシートを任意のサイトから取り込めるようにしない。	5-(iv)	対応済	
		HTMLテキストの入力を許可しない場合の対策	保険的対策	入力値の内容チェックを行う。	5-(v)	対応済	
		HTMLテキストの入力を許可する場合の対策	根本的解決	入力されたHTMLテキストから構文解析木を作成し、スクリプトを含まない必要な要素のみを抽出する。	5-(vi)	対応不要	
		HTMLテキストの入力を許可する場合の対策	保険的対策	入力されたHTMLテキストから、スクリプトに該当する文字列を排除する。	5-(vii)	対応不要	
		全てのウェブアプリケーションに共通の対策	根本的解決	HTTPレスポンスヘッダのContent-Typeフィールドに文字コード（charset）の指定を行う。	5-(viii)	対応済	
		全てのウェブアプリケーションに共通の対策	保険的対策	Cookie情報の漏えい対策として、発行するCookieにHttpOnly属性を加え、TRACEメソッドを無効化する。	5-(ix)	対応済	
		全てのウェブアプリケーションに共通の対策	保険的対策	クロスサイト・スクリプティングの潜在的な脆弱性対策として有効なブラウザの機能を有効にするレスポンスヘッダを返す。	5-(x)	未対策	
6	CSRF（クロスサイト・リクエスト・フォージェリ）		根本的解決	処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行する。	6-(i)-a	対応不要	開発工程でセキュリティ要件のレビューとソースコードのレビューを行い、本脆弱性への対策を講じています。個別の実施項目ごとの状況はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
			根本的解決	処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。	6-(i)-b	対応不要	
			根本的解決	Refererが正しいリンク元かを確認し、正しい場合のみ処理を実行する。	6-(i)-c	対応済	
			保険的対策	重要な操作を行った際に、その旨を登録済みのメールアドレスに自動送信する。	6-(ii)	未対策	
7	HTTPヘッダ・インジェクション		根本的解決	ヘッダの出力を直接行わず、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用APIを使用する。	7-(i)-a	対応済	開発工程でセキュリティ要件のレビューとソースコードのレビューを行い、本脆弱性への対策を講じています。個別の実施項目ごとの状況はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
			根本的解決	改行コードを適切に処理するヘッダ出力用APIを利用できない場合は、改行を許可しないよう、開発者自身で適切な処理を実装する。	7-(i)-b	対応済	

© 2026 aiESG, Inc.

No	脆弱性の種類	区分	対策の性質	実施項目	番号	対応状況	補足（脆弱性ごと）
			保険的対策	外部からの入力の全てについて、改行コードを削除する。	7-(ii)	対応済	
8	メールヘッダ・インジェクション		根本的解決	メールヘッダを固定値にして、外部からの入力はすべてメール本文に出力する。	8-(i)-a	対応済	サービスから送信するメールは、送信元のドメインとアドレスを固定しており、利用者が変更できない仕様です。送信ドメインの詐称対策（SPF・DKIM・DMARC）を設定しています。個別の実施項目ごとの状況はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
			根本的解決	ウェブアプリケーションの実行環境や言語に用意されているメール送信用APIを使用する（8-(i) を採用できない場合）。	8-(i)-b	対応済	
			根本的解決	HTMLで宛先を指定しない。	8-(ii)	対応済	
			保険的対策	外部からの入力の全てについて、改行コードを削除する。	8-(iii)	対応済	
9	クリックジャッキング		根本的解決	HTTPレスポンスヘッダに、X-Frame-Optionsヘッダフィールドを出力し、他ドメインのサイトからのframe要素やiframe要素による読み込みを制限する。	9-(i)-a	対応済	開発工程でセキュリティ要件のレビューとソースコードのレビューを行い、本脆弱性への対策を講じています。個別の実施項目ごとの状況はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
			根本的解決	処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。	9-(i)-b	対応不要	
			保険的対策	重要な処理は、一連の操作をマウスのみで実行できないようにする。	9-(ii)	未対策	
10	バッファオーバーフロー		根本的解決	直接メモリにアクセスできない言語で記述する。	10-(i)-a	対応済	利用しているライブラリの既知の脆弱性を常時監視し、修正版への更新を行っています。個別の実施項目ごとの状況はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
			根本的解決	直接メモリにアクセスできる言語で記述する部分を最小限にする。	10-(i)-b	対応不要	
			根本的解決	脆弱性が修正されたバージョンのライブラリを使用する。	10-(ii)	対応済	
11	アクセス制御や認可制御の欠落		根本的解決	アクセス制御機能による防御措置が必要とされるウェブサイトには、パスワード等の秘密情報の入力を必要とする認証機能を設ける。	11-(i)	対応済	ID・パスワードによる認証機能を設け、利用企業ごとにデータをアプリケーション層で論理的に分離しています。利用企業内では、管理者権限を持つアカウントのみがアカウントの追加・削除・権限変更を行えます。
			根本的解決	認証機能に加えて認可制御の処理を実装し、ログイン中の利用者が他人になりすましてアクセスできないようにする。	11-(ii)	対応済	

© 2026 aiESG, Inc.

経済産業省「クラウドサービスレベルのチェックリスト」に基づく回答

株式会社aiESG　回答日：2026年10月16日　版数：1.0

経済産業省「クラウドサービスレベルのチェックリスト」（2010年8月）のサービスレベル項目ごとに、本サービスの状況を記載しています。

No.	種別	サービスレベル項目	規定内容	測定単位	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	原則として24時間365日提供しています。定期・緊急のメンテナンス、アクセスの集中、セキュリティ確保の必要等がある場合は、事前の通知なく一時的に中断することがあります（利用規約第10条第2項）。
2	可用性	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。可能な限り事前に、サービス画面への掲示または登録メールアドレス宛の電子メールでお知らせします。緊急の場合は事前の通知なく実施することがあります。
3	可用性	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。サービスを終了する場合は、1か月前までに利用者に通知します（利用規約第10条第1項）。
4	可用性	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	第三者へのプログラム・データの預託（エスクロー）は行っていません。利用者は、サービス上のデータをCSV形式（UTF-8）またはExcel形式でエクスポートできます。
5	可用性	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（%）	稼働率の保証（SLA）は設定していません。
6	可用性	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。国内リージョン内の複数のゾーンに冗長化した構成とし、単一ゾーンの障害時にもサービスを継続できるようにしています。別リージョンへの切替え構成はとっていません。
7	可用性	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	代替サービスの提供は定めていません。障害時は、速報と復旧の見通しを登録メールアドレス宛にお知らせします。
8	可用性	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）	代替措置としてのデータ提供は定めていません。データはCSV形式（UTF-8）またはExcel形式でエクスポートできます。
9	可用性	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。品質・セキュリティの向上のため随時更新しています。重要な機能の廃止など利用者に重大な不利益を及ぼす変更は、実施日の1か月前までに通知します（利用規約第13条第3項）。軽微な変更は、変更履歴の掲示等で内容を確認できるようにしています（同条第2項）。
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	数値は公開していません。
11	信頼性	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	定めていません。
12	信頼性	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	障害件数は公開していません。過去2年間に、対外的な公表や監督官庁等への報告を要するセキュリティインシデントは発生していません。
13	信頼性	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。性能と稼働状況（死活）を常時監視しています。監視基準の詳細はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
14	信頼性	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。社内のインシデント対応手順に基づき、登録メールアドレス宛に速報と復旧の見通しをお知らせします。
15	信頼性	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	障害は速報を随時お知らせします。セキュリティインシデントは、認識後速やかに通知します（社内規程で72時間以内と定めています）。
16	信頼性	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）	稼働状況（死活）を1分間隔で自動監視しています。

© 2026 aiESG, Inc.

No.	種別	サービスレベル項目	規定内容	測定単位	回答
17	信頼性	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	定期報告は行っていません。障害・メンテナンスの際に随時お知らせします。
18	信頼性	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。利用者がログを閲覧する機能はありませんが、ご要請に応じてログイン記録・操作記録を提供できます。
19	性能	応答時間	処理の応答時間	時間（秒）	目標値は定めていません。
20	性能	遅延	処理の応答時間の遅延継続時間	時間（分）	目標値は定めていません。
21	性能	バッチ処理時間	バッチ処理（一括処理）の応答時間	時間（分）	目標値は定めていません。
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	有無	利用企業ごとのカスタマイズは提供していません。
23	拡張性	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	利用者向けのAPIは提供していません。利用者が設定した場合に、CDPが提供するAPI（CDP連携）を通じて、CDPに登録された利用者のCDP回答を取得する機能があります。現在提供しているのは取得（読み取り）のみで、CDPへの送信（書き込み）は行いません。送信機能を提供する場合は、利用者が設定した場合に限って行い、事前にお知らせします。設定はいつでも解除できます（利用規約第17条）。
24	拡張性	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）	利用担当者の登録数に上限は設けていません。
25	拡張性	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	上限は公開していません。
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	当社の営業日の営業時間内に対応します（利用規約第13条第7項）。連絡方法と受付時間は、ご契約時にご案内します。
27	サポート	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	当社の営業日の営業時間内に対応します。対象は操作方法と不具合に関するお問い合わせです（利用規約第13条第7項・第8項）。連絡方法と受付時間は、ご契約時にご案内します。
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。日次で自動バックアップを取得し、暗号化したうえで、日本国内（Google Cloud 東京リージョン）に保存しています。当社従業員による利用者データへのアクセスは原則禁止とし、事前に承認を得た場合に限っています。
29	データ管理	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	日次のバックアップに加え、直近7日以内の任意の時点に復旧できる機能を有効にしています。
30	データ管理	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	セキュリティ上の理由により非公開（個別のご依頼時にご案内）
31	データ管理	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	「本契約終了後、当社は、３０日間、利用者に対し入力データのダウンロード機会を提供するものとします。当該期間経過後、当社は、入力データを削除することができるものとします。」（利用規約第21条第3項）削除のご依頼があった場合は、当社で削除します。削除後も、バックアップ等に最大7日間残ります。利用規約第18条第5項に基づき匿名化または統計的に処理した情報は対象外です。保管媒体の廃棄は、利用するクラウド事業者の基準により復元できない状態で行われます。
32	データ管理	バックアップ世代数	保証する世代数	世代数	セキュリティ上の理由により非公開（個別のご依頼時にご案内）
33	データ管理	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。保存データとバックアップを、安全な暗号方式と十分な鍵長で暗号化しています。通信も暗号化しています。

© 2026 aiESG, Inc.

No.	種別	サービスレベル項目	規定内容	測定単位	回答
34	データ管理	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	暗号鍵は、クラウド基盤事業者の鍵管理機能により管理しています。利用企業ごとのデータは、アプリケーション層で論理的に分離しています。
35	データ管理	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	損害賠償は、当社が利用者から実際に支払いを受けた料金の合計金額を上限とします。ただし、当社の故意または重大な過失による場合は除きます（利用規約第16条）。
36	データ管理	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。「本契約終了後、当社は、３０日間、利用者に対し入力データのダウンロード機会を提供するものとします。当該期間経過後、当社は、入力データを削除することができるものとします。」（利用規約第21条第3項）エクスポート形式はCSV（UTF-8）またはExcelです。
37	データ管理	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	整合性検証の報告書は提供していません。バックアップが取得できていることを定期的に確認しています。
38	データ管理	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。設問ごとの定義に基づき、文字数の上限・選択肢・数値や日付の範囲をサーバー側で検査しています。添付ファイルは種類とサイズを検査しています。
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	無。ISMS、プライバシーマーク等の認証は取得していません。利用するクラウド基盤（Google Cloud）は、ISO/IEC 27001等の第三者認証を取得しています。
40	セキュリティ	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	クラウドサービスのセキュリティ評価サービス「Assured」の評価を受けています。
41	セキュリティ	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。業務用端末には、マルウェア対策ソフトの導入とセキュリティ更新の適用を行っています。外部記憶媒体の利用は原則禁止しています。
42	セキュリティ	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。安全なプロトコルのバージョンと、安全な暗号方式・十分な鍵長の組み合わせのみを使用しています。サーバー証明書は信頼できる認証局が発行した有効なものを使用しています。詳細はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
43	セキュリティ	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	当社としての保証報告書（SOC報告書等）はありません。利用するクラウド基盤（Google Cloud）は、SOC 2等の第三者保証報告書を取得しています。
44	セキュリティ	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。利用企業ごとのデータをアプリケーション層で論理的に分離し、利用企業間でデータが混在しないようにしています。
45	セキュリティ	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。当社従業員による利用者データへのアクセスは原則禁止とし、事前に承認を得た場合に限っています。システムへのアクセス権限は、業務上必要な担当者に必要最小限で付与しています。利用企業内では、管理者権限を持つアカウントがアカウントの追加・削除・権限変更を行えます。
46	セキュリティ	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は利用者（利用担当者）ごとに発行します。ログは365日間保存し、管理者の特権操作の記録は400日間、改ざんできない形式で保存しています。必要時に追跡でき、ご要請に応じて提供します。
47	セキュリティ	ウイルススキャン	ウイルススキャンの頻度	頻度	本番環境はクラウド事業者のマネージドサービスを利用し、提供事業者の対策を適用しています。業務用端末にはマルウェア対策ソフトを導入し、常時検査しています。
48	セキュリティ	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。バックアップは暗号化して保存しています。USBメモリ等の外部記憶媒体の利用は社内規程で原則禁止しています。情報資産を廃棄する際は、復元できない状態にする手順を定めています。

© 2026 aiESG, Inc.

No.	種別	サービスレベル項目	規定内容	測定単位	回答
49	セキュリティ	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	預託データとバックアップは日本国内（Google Cloud 東京リージョン）に保管しています。次の処理は日本国外で行われる場合があります：生成AI機能の処理、アプリケーションのログの保存、メール送信（SendGrid、米国）、社内への問い合わせ通知（Slack、米国）、エラー情報の収集（Sentry、米国。メールアドレス等は除いて送信）。

© 2026 aiESG, Inc.

総務省「クラウドサービスの安全・信頼性に係る情報開示指針」に基づく回答

株式会社aiESG　回答日：2026年10月16日　版数：1.0

総務省「ASP・SaaSの安全・信頼性に係る情報開示指針（ASP・SaaS編）第3版」(*1) と「AIを用いたクラウドサービスの安全・信頼性に係る情報開示指針（ASP・SaaS編）」(*2) の開示項目のうち、本サービスのセキュリティと利用条件に関する項目を記載しています。会社の財務・資本・人員等の情報は記載していません。

「No.」は本書の通し番号です。指針の項目番号は「指針No.」欄に併記しています。

No.	指針No.(*1)	指針No.(*2)	種別	サービスレベル項目	規程内容	回答
S-1	1	1	開示情報の時点	開示情報の日付	開示情報の年月日（西暦）	2026年10月16日
事業所・事業						
S-2	2	2	事業所等の概要	事業者名	事業者の正式名称（商号）	株式会社aiESG
S-3	4	4	事業所等の概要	事業所	事業者の本店所在地	福岡県福岡市博多区博多駅前1丁目15番20号 NMF博多駅前ビル2階
S-4	4	4	事業所等の概要	事業所	事業者ホームページ	https://aiesg.co.jp/
S-5	5	5	事業の概要	主な事業の概要	事業者の主な事業概要	製品・サービス単位のESG分析・評価、ESGコンサルティング、CDP回答支援サービス「aiESG for CDP」等の提供
S-6	6	6	経営者	代表者	代表者氏名	代表取締役 馬奈木 俊介
コンプライアンス						
S-7	21	21	組織体制	専担の部署・会議体	コンプライアンスを担当する社内の部署・会議体の有無と、「有り」の場合は社内の部署名・会議体	有（管理部）
S-8	22	22	組織体制	情報セキュリティに関する組織体制の状況	情報セキュリティに関する組織体制の有無	有。セキュリティ管理の責任者と関係部署の職務・権限・責任を定め、平常時に加えて有事を想定した役割も定めています。セキュリティリスクへの対応計画は経営層が承認し、進捗・結果を経営層に報告しています。
S-9	23	23	個人情報	個人情報の取り扱い	個人情報の取り扱いに関する規定等の有無と、「有り」の場合は記載箇所	有。プライバシーポリシー（https://aiesg.co.jp/privacy-policy/）
S-10	24	24	守秘義務	守秘義務契約	守秘義務契約に関わる契約又は条項の有無	有（利用規約第18条）。入力データ・出力データは、秘密である旨の明示の有無を問わず秘密情報として扱います。
S-11	24	24	守秘義務	守秘義務契約	守秘義務違反があった場合のペナルティ条項の有無	守秘義務違反に限った違約金等の条項は設けていません。損害賠償は利用規約第16条によります。
S-12	25	25	従業員教育等	従業員に対するセキュリティ教育の実施状況	従業員に対するセキュリティ教育実施に関する取組状況	入社時と社内規程の改定時に、セキュリティと重要情報の取扱いに関する教育を行っています（社内規程、AIツールの利用ガイドライン、権限付与時のセキュリティテスト等）。
S-13	26	26	従業員教育等	従業員に対する守秘義務等の状況	従業員に対する守秘義務対応の取組状況	従業員と、秘密保持契約または誓約書を締結しています。契約終了・変更時は、アクセス権の変更・削除と貸与資産の返却を文書化した手順に基づき行っています。
S-14	27	27	委託	委託情報に関する開示	サービス提供に関わる委託先（再委託先）の情報開示の可否と、可能な場合の条件等	Google Cloud（サーバー・データベース・生成AI）、SendGrid（メール送信）、Slack（問い合わせの社内通知）、Sentry（エラー情報の収集）、Backlog（問い合わせの管理）を利用しています。
S-15	28	28	委託	委託先に対する管理状況	自社の個人情報保護指針に対する順守規定の有無	有。委託先の選定・管理の基準を定め、定期的に見直しています。
S-16	28	28	委託	委託先に対する管理状況	委託先（再委託先）の個人情報保護等の状況に関する情報提供の可否と、可能な場合の条件等	個別のご依頼時にご案内します。

© 2026 aiESG, Inc.

No.	指針No.(*1)	指針No.(*2)	種別	サービスレベル項目	規程内容	回答
S-17	28	28	委託	委託先に対する管理状況	委託先（再委託先）との守秘義務対応状況	委託先とは、秘密保持、情報の消去、関連法令の遵守、セキュリティインシデント発生時の報告・対処を契約で定めています。委託先には、利用規約に基づき当社が負う義務と同等の義務を課しています（利用規約第14条）。
S-18	28	28	委託	委託先に対する管理状況	委託先（再委託先）の管理方法	契約更新時に、合意内容の履行状況と業務・セキュリティ対応を確認しています。クラウド事業者は、第三者認証の取得状況を随時確認しています。
文書類						
S-19	29	29	文書類	情報セキュリティ関する規定等の整備	情報セキュリティに関する基本方針・規定・マニュアル、リスクアセスメント結果等の状況と文書名	有。情報セキュリティに関する社内規程（情報セキュリティガイドブック）と、クラウド運用手順を整備し、定期的に見直しています。
S-20	30	30	文書類	事業継続に関する規定の整備	事業継続に関する基本方針・規定・マニュアル等の有無と、「有り」の場合は文書名	有。サービスの障害・停止・データ消失をインシデントとして定義し、復旧とエスカレーションの手順を社内規程とクラウド運用手順に定めています。
S-21	30	30	文書類	事業継続に関する規定の整備	BCP対応計画及び運用手順等の開示の可否と、可能な場合の条件等	個別のご依頼時にご案内します。
S-22	31	31	文書類	リスク管理に関する規定等の整備	リスク管理に関する基本方針・規定・マニュアル等の有無と、「有り」の場合の文書名	有。セキュリティリスクへの対応計画を策定し、経営層の承認を得ています。
S-23	32	32	文書類	勧誘・販売・係争に関する規定等の整備	係争に関する規定・管轄裁判所等、係争が生じた際の対応に関する情報を含む文書類の有無と、「有り」の場合の文書名	有（利用規約第26条）。準拠法は日本法、東京地方裁判所または東京簡易裁判所を第一審の専属的合意管轄裁判所とします。
S-24	33	33	文書類	ASP・SaaSの苦情対応に関する規定等の整備	ASP・SaaS事業者の事故責任の範囲と保証範囲が記述された文書の有無と、「有り」の場合は文書名	有（利用規約第16条「免責事項」）
S-25	34		文書類	利用者による設定不備の抑止・防止に係る規程等の整備	サービス提供の際の利用者による設定不備を起こさせないための基本方針・規程・マニュアル等の有無と「有り」の場合は文書名	利用者が設定できる項目は、アカウントと権限の管理に限られます。権限の変更は、利用企業の管理者権限を持つアカウントのみが行えます。操作方法は本サービスの案内・マニュアルで提供しています。
サービス基本特性						
S-26	35	34	サービス内容	サービス名称	本ASP・SaaSサービス名称	aiESG for CDP
S-27	37	36	サービス内容	サービスの内容・範囲	本ASP・SaaSサービスの内容・特徴	CDP質問票への回答作成を支援する分析支援サービスです。生成AIによる回答案の作成支援、スコアの分析、改善提案等の機能を提供します。
S-28	37	36	サービス内容	サービスの内容・範囲	他の事業者との間で行っているサービス連携の有無と、「有り」の場合はその内容	生成AI機能の提供に、Google Cloud（Vertex AI）を利用しています。また、利用者が設定した場合に、CDPが提供するAPI（CDP連携）を通じて、利用者のCDP回答を取得します。現在提供しているのは取得（読み取り）のみで、CDPへの送信（書き込み）は行いません。送信機能を提供する場合は、利用者が設定した場合に限って行い、事前にお知らせします。（利用規約第17条）。
S-29	38	37	サービス内容	サービス提供時間	サービスの提供時間帯	原則として24時間365日（メンテナンス等による一時的な中断を除く）
S-30	39	38	サービス内容	サービスのカスタマイズ範囲	アプリケーションのカスタマイズの範囲（契約内容に依存する場合はその旨記述）	利用企業ごとのカスタマイズは提供していません。
S-31	40	39	サービス内容	移行支援	本サービスを利用する際における既存システムからの移行支援の有無（解約内容に依存する場合はその旨記述）	無

© 2026 aiESG, Inc.

No.	指針No.(*1)	指針No.(*2)	種別	サービスレベル項目	規程内容	回答
S-32	41		サービス内容	マネージド・サービスやコンサルティング・サービスの提供	本サービスのシステム動作環境の設定や運用支援などをマネージド・サービスやコンサルティング・サービスとして提供しているか、または第3者の当該サービスを紹介しているかの有無。「有り」の場合はその概要	有。利用者との別途の合意に基づき、ESG専門家によるコンサルティング等のフォローアップサービスを有償で提供することがあります（利用規約第5条第2項）。
S-33		40	ＡＩサービス基本事項	（ＡＩポリシー）	ＡＩサービスに対する基本的な考え方。透明性、公平性、安全、セキュリティ、プライバシー保護、倫理など	AIの利用に関する社内ガイドラインを定めています。本サービスにおけるデータの扱いは「追加項目」シートの生成AIの項をご参照ください。
S-34		41	責任分担	ＡＩ機能に関連する責任分担	人間の判断の有無、ＡＩによる判断に基づく損害賠償責任など責任分担にかかわる事項	生成AIによる文章は誤りや不完全な内容を含む可能性があり、利用者が正確性・適法性・適切性を確認したうえで利用するものとしています（利用規約第16条）。最終的なCDP回答の作成と提出は利用者が行います。
S-35		42	データ及び学習済みモデルの権利	利用	利用者が入力したデータの利用の有無、内容同意の取得方法など	「追加項目」シートの生成AIの項をご参照ください。
S-36		43	データ及び学習済みモデルの権利	権利関係	利用者データに関する権利（所有権、使用権、著作権、肖像権など） 利用者データを使った追加学習後の学習済みモデルの権利	入力データの知的財産権は利用者に留保されます（利用規約第15条第2項）。利用者が自らのCDP回答・開示資料等に取り込んだ回答案等（回答成果物）は、契約終了後も期間の制限なく自由に利用できます（同条第5項）。利用者データによる追加学習は行わないため、追加学習後のモデルの権利は生じません。
S-37	42	44	サービスの変更・終了	サービス（事業）変更・終了時等の事前告知	利用者への告知時期（事前の告知時期を1ヶ月前、3ヶ月前、6ヶ月前、12ヶ月前等の単位で記述）	サービス終了：1か月前まで（利用規約第10条第1項）／重大な変更：実施日の1か月前まで（同第13条第3項）／規約の変更：効力発生日の1か月前まで（同第6条第2項）
S-38	42	44	サービスの変更・終了	サービス（事業）変更・終了時等の事前告知	告知方法	サービス画面または当社ウェブサイトへの掲示、または登録メールアドレス宛の電子メール（利用規約第20条）
S-39	43	45	サービスの変更・終了	サービス（事業）変更・終了後の対応・代替措置	対応・代替措置の基本方針の有無と、「有り」の場合はその概要	有。利用者の責めによらず有効期間満了前に契約が終了する場合、前払いの料金を日割りで返金します（利用規約第5条第5項）。契約終了後30日間は入力データのダウンロード機会を提供します（同第21条第3項）。
S-40	44	46	契約の終了等	情報の返却・削除・廃棄	契約終了時の情報資産（利用者のデータ等）の返却責任の有無と、受託情報の変換方法・ファイル形式・費用等	「本契約終了後、当社は、３０日間、利用者に対し入力データのダウンロード機会を提供するものとします。当該期間経過後、当社は、入力データを削除することができるものとします。」（利用規約第21条第3項）形式はCSV（UTF-8）またはExcelです。
S-41	44	46	契約の終了等	情報の返却・削除・廃棄	情報の削除又は廃棄方法の開示の可否と、可能な場合の条件等	データの削除は、利用するクラウド事業者の削除基準に従い、復元できない状態で行われます。
S-42	44	46	契約の終了等	情報の返却・削除・廃棄	削除又は廃棄したことの証明書等の提供	消去証明書の発行は行っていません。削除は記録媒体の廃棄ではなく、データベース上で対象データを消去する処理で行うためです。削除したデータは、バックアップの保持期間（最大7日間）を過ぎると復元できない状態になります。
S-43	45	47	サービス料金	料金体系	初期費用額	利用申込書に記載します。
S-44	45	47	サービス料金	料金体系	月額利用額	利用申込書に記載します。
S-45	45	47	サービス料金	料金体系	最低利用契約期間	利用期間は料金プランごとに定め、利用申込書に記載します。自動更新はしません（利用規約第21条第1項）。

© 2026 aiESG, Inc.

No.	指針No.(*1)	指針No.(*2)	種別	サービスレベル項目	規程内容	回答
S-46	46	48	サービス料金	解約時違約金支払いの有無	解約時違約金（利用者側）の有無と、「有り」の場合はその額	違約金は定めていません。支払済みの料金は、利用規約第5条第5項に定める場合を除き返金しません。
S-47	47	49	サービス料金	利用者からの契約事前受付期限	利用者からのサービス解約の受付時期の有無と、「有り」の場合はその期限（何日・何ヶ月前かを記述）	当社所定の手続により退会できます（利用規約第12条）。
サービス品質						
S-48	48	50	サービス品質	サービス稼働設定値	サービス稼働率の目標値	稼働率の保証（SLA）は設定していません。
S-49	48	50	サービス品質	サービス稼働設定値	サービス稼働率の実績値	公開していません。
S-50	48	50	サービス品質	サービス稼働設定値	サービス停止の事故歴	過去2年間に、対外的な公表や監督官庁等への報告を要するセキュリティインシデントは発生していません。
S-51	49	51	サービス品質	サービスパフォーマンスの管理	システムリソース不足等による応答速度の低下の検知の有無と、「有り」の場合は、検知の場所、検知のインターバル、画面の表示チェック等の検知方法	有。性能と稼働状況を常時監視しています。検知方法の詳細はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
S-52	49	51	サービス品質	サービスパフォーマンスの管理	ネットワーク・機器等の増強判断基準又は計画の有無、「有り」の場合は増強の技術的措置（負荷分散対策、ネットワークルーティング、圧縮等）の概要	有。将来必要となるリソースも考慮してキャパシティ計画を行っています。
S-53	50	52	サービス品質	認証取得・監査実施	プライバシーマーク（JIS Q 15001）等、ISMS（JIS Q 27001等）、ITSMS（JIS Q 20000-1 等）の取得、監査基準委員会報告書第18号（米国監査基準SSAE16、国際監査基準 ISAE3402）の作成の有無と、「有り」の場合は認証名又は監査の名称	無
S-54	51	53	サービス品質	脆弱性診断	脆弱性診断の有無と、「有り」の場合は、診断の対象（アプリケーション、OS、ハードウェア等）と、対策の概要	有。依存ライブラリの脆弱性情報を継続的に監視し、重大な脆弱性は優先的に修正しています。
S-55	52		サービス品質	システム動作環境の設定・診断に係る支援ツール等の提供	システム動作環境の設定や設定値の診断に係る支援ツール等提供の有無。「有り」の場合は、ツールの概要。	無
S-56	53		サービス品質	学習コンテンツや学習機会の提供	システム動作環境そのものや設定に係る学習コンテンツもしくは講習会等の学習機会の提供有無。「有り」の場合はその概要	操作方法の案内・マニュアルを提供しています。
S-57	54	54	サービス品質	バックアップ対策	利用者データのバックアップ実施インターバル	日次
S-58	54	54	サービス品質	バックアップ対策	世代バックアップ（何世代前までかを記述）	セキュリティ上の理由により非公開（個別のご依頼時にご案内）
S-59	55	55	サービス品質	サービス継続	サービスが停止しない仕組み（冗長化、負荷分散等）	データベースは東京リージョン内の2つのゾーンに冗長化し、7日以内の任意の時点に復旧できるようにしています。
S-60	55	55	サービス品質	サービス継続	DR（ディザスターリカバリー）対策の有無と、「有り」の場合はその概要	有。単一ゾーンの障害時にもサービスを継続できる構成としています。別リージョンへの切替え構成はとっていません。
S-61	57	57	サービス品質	SLA（サービスレベル・アグリーメント）	本サービスに係るSLAが契約書に添付されるか否か	添付しません。

No.	指針No.(*1)	指針No.(*2)	種別	サービスレベル項目	規程内容	回答
S-62		59	品質	ＡＩの精度	高い精度は実現するための環境条件など、ＡＩの精度に関わる情報	スコア、分析結果等はAIまたはルールベースの分析に基づく参考情報であり、CDPによる公式の評価結果との一致を保証するものではありません（利用規約第16条）。
S-63		60	品質	ＡＩの精度向上策	追加学習の有無（有りの場合は時期、頻度、役割分担、料金など）	利用者のデータを使った追加学習は行いません。
S-64		61	品質	説明可能性のレベル	ＡＩの出力結果の根拠の説明可能性のレベル（ホワイトボックス型／ブラックボックス型）	大規模言語モデル（ブラックボックス型）を利用しています。出力は参考情報として、利用者が確認したうえで利用する前提です。
S-65	59	62	連携	他のサービス・事業との連携状況に関する情報提供	他のサービスや事業との連携の有無と、「有り」の場合は情報提供の条件等	生成AI機能にGoogle Cloud（Vertex AI）を、通知メールの送信に外部のメール配信サービスを利用しています。利用者が設定した場合は、CDPが提供するAPI（CDP連携）と連携します。
S-66		63	連携	ＡＩ関連の連携	ＡＰＩ等による他社のＡＩ機能の活用の有無、フレームワークやライブラリなどオープンソースの利用有無	有。Google Cloud（Vertex AI）経由でAnthropic社のClaudeを利用しています。オープンソースソフトウェアは、利用しているものを把握し、既知の脆弱性を常時監視しています。
アプリケーション、プラットフォーム、サーバ・ストレージ等						
S-67	60	64	セキュリティ	死活監視	死活監視の有無と、「有り」の場合は死活監視の対象	有。サービスの稼働状況を常時監視しています。
S-68	61	65	セキュリティ	時刻同期	時刻同期への対応の有無と、「有り」の場合は時刻同期方法	有。各構成要素の時刻を統一して管理し、同期しています。
S-69	62	66	セキュリティ	ウイルス対策	ウイルス対策の有無	有
S-70	63	67	セキュリティ	管理者権限の運用管理	システム運用部門の管理者権限の登録・登録削除の手順の有無	有。特権アカウントの付与は承認制とし、必要最小限に限定しています。手順を文書化し、定期的に見直しています。不要になったアカウントは無効化・削除しています。
S-71	64	68	セキュリティ	ID・パスワードの運用管理	事業者側にて、利用者のID・PWを付与する場合におけるIDやパスワードの運用管理方法の規程の状況	IDとパスワードは、契約の開始日に登録メールアドレス宛に通知して発行します（利用規約第7条第1項）。IDは利用担当者ごとに発行でき、共有は禁止しています。パスワードの要件は「追加項目」シートの多要素認証の項をご参照ください。
S-72	65	69	セキュリティ	記録（ログ等）	利用者の利用状況の記録（ログ等）取得の状況と、その保存期間及び利用者への提供可否	取得しています。保存期間は365日です。ご要請に応じて提供できます。
S-73	65	69	セキュリティ	記録（ログ等）	システム運用に関するログの取得の有無と、「有り」の場合は保存期間	有。アプリケーションのログは365日間、管理者の特権操作の記録は400日間保存しています。AIアシスタントのやりとりの記録は365日で自動削除しています。
S-74	65	69	セキュリティ	記録（ログ等）	ログの改ざん防止措置の有無	有。アクセス制御等によりログを保護しています。管理者の特権操作の記録は改ざんできない形式で保存しています。
S-75	66	70	セキュリティ	セキュリティパッチ管理	パッチ管理の状況とパッチ更新間隔等、パッチ適用方針	データベースなどのマネージドサービスはGoogle Cloudが更新を適用し、アプリの実行環境はリリースのたびに最新のものに更新しています。依存ライブラリの脆弱性情報を継続的に監視し、重大な脆弱性は優先的に修正しています。
S-76	67	71	セキュリティ	暗号化対策	暗号化措置（データベース）への対応の有無と、「有り」の場合はその概要	有。データベースとバックアップを、安全な暗号方式と十分な鍵長で暗号化しています。

© 2026 aiESG, Inc.

No.	指針No.(*1)	指針No.(*2)	種別	サービスレベル項目	規程内容	回答
S-77	68		セキュリティ	設定不備防止対策	申請したサービスが該当する「クラウドサービス利用・提供における適切な設定のためのガイドライン」における「【評価項目】 a. クラウドにおけるセキュリティ設定項目の類型と対策」それぞれに対する設定不備防止対策の有無。「有り」の場合は、該当項目と設定不備防止対策の概要	有。クラウド環境の構成は、変更管理のもとでバージョン管理しています。詳細はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
S-78		72	セキュリティ	ＡＩ関連セキュリティ対策	ＡＩに特化したセキュリティ対策の有無	有。AIに対する攻撃手法や動向について情報を収集し、対応しています。
S-79		73	性能	ＡＩ性能	推論時間等（利用者の操作に係わるもの）、（利用者が学習を行う場合は）学習時間	目標値は定めていません。
ネットワーク						
S-80	69	74	センター側ネットワーク	回線	専用線（VPNを含む）、インターネット等の回線の種類	インターネット（暗号化通信）
S-81	70	75	センター側ネットワーク	帯域	データ通信速度の範囲、帯域保証の有無	帯域保証はありません。
S-82	71	76	セキュリティ	ファイアウォール	ファイアウォール設置等の不正アクセスを防止する措置の有無	有。外部からの通信は既定ですべて遮断し、アプリケーションにはロードバランサ経由でのみ到達できるよう設定しています。設定はコードで管理し、変更はレビューを経て履歴を残しています。
S-83	72	77	セキュリティ	不正侵入検知	不正パケット、非権限者による不正なサーバ侵入に対する検知等の有無と、「有り」の場合は対応方法	侵入検知・防御システム（IDS/IPS）は導入していません。
S-84	73	78	セキュリティ	ネットワーク監視	事業者とエンドユーザとの間のネットワーク（専用線等）において障害が発生した際の通報時間	専用線は提供していないため、該当しません。
S-85	74	79	セキュリティ	ユーザ認証	ユーザ（利用者）のアクセスを管理するための認証方法、特定の場所及び装置からの接続を認証する方法等	ID・パスワードによる認証に加え、認証アプリによる二要素認証をご利用いただけます（組織単位で必須化も可能）。接続元の場所・端末を限定する機能は提供していません。
S-86	75	80	セキュリティ	なりすまし対策（事業者サイド）	第三者によるなりすましサイトに関する対策の実施の有無と、「有り」の場合は認証の方法	有。信頼できる認証局が発行したサーバー証明書を使用しています。サービスから送信するメールには、送信ドメインの詐称対策（SPF・DKIM・DMARC）を設定しています。
S-87	76	81	セキュリティ	暗号化対策	暗号化措置（ネットワーク）への対応の有無と、「有り」の場合はその概要	有。サービスへのアクセス時の通信を暗号化しています。
S-88	77	82	セキュリティ	その他セキュリティ対策	その他特筆すべきセキュリティ対策を記述（情報漏洩対策等）	外部からの通信はGoogle Cloudの外部ロードバランサを経由しており、Google Cloudの基盤が標準で提供するネットワーク層のDDoS防御を受けています。アプリケーション層の防御（WAF）は導入していません。データベースは外部から直接アクセスできないようにしています。
S-89	78	83	ＰＣ側ネットワーク	推奨回線	専用線（VPNを含む）、インターネット等の回線の種類	インターネット
S-90	78	83	ＰＣ側ネットワーク	推奨回線	ユーザ接続回線について、ASP・SaaS事業者が負う責任範囲	利用に必要な通信機器と通信費用は、利用者の負担となります（利用規約第5条第3項）。
S-91	79	84	ＰＣ側ネットワーク	推奨帯域	推奨帯域の有無と、「有り」の場合はそのデータ通信速度の範囲	特に定めていません。

© 2026 aiESG, Inc.

No.	指針No.(*1)	指針No.(*2)	種別	サービスレベル項目	規程内容	回答
S-92	80	85	ＰＣ等（操作端末）	推奨端末	パソコン、携帯電話等の端末の種類、OS等	パソコン（Windows・Mac）。スマートフォン・タブレットは推奨環境外です。
S-93	80	85	ＰＣ等（操作端末）	推奨端末	利用するブラウザの種類	最新版のGoogle Chrome、Microsoft Edge、Safari
ハウジング（サーバ設置場所）						
S-94	81	86	施設建築物	建物形態	データセンター専用建物か否か	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-95	82	87	施設建築物	所在地	国名、日本の場合は地域ブロック名（例：関東、東北）	日本（関東）。Google Cloud 東京リージョンに保管しています。
S-96	82	87	施設建築物	所在地	バックアップデータの保管場所	日本（関東）。Google Cloud 東京リージョンに保管しています。
S-97	82	87	施設建築物	所在地	特筆すべき立地上の優位性があれば記述（例：標高、地盤等）	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-98	83	88	施設建築物	耐震・免震構造	耐震数値	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-99	83	88	施設建築物	耐震・免震構造	免震構造や制震構造の有無	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-100	84	89	非常用電源設備	無停電電源	無停電電源装置（UPS）の有無と、「有り」の場合は電力供給時間	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-101	85	90	非常用電源設備	給電ルート	異なる変電所を経由した給電ルート（系統）で２ルート以上が確保されているか否か（自家発電機、UPSを除く）	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-102	86	91	非常用電源設備	非常用電源	非常用電源（自家発電機）の有無と、「有り」の場合は連続稼働時間の数値	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-103	87	92	消火設備	サーバルーム内消火設備	自動消火設備の有無と、「有り」の場合はガス系消火設備か否か	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-104	88	93	消火設備	火災感知・報知システム	火災検知システムの有無	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-105	89	94	避雷対策設備	直撃雷対策	直撃雷対策の有無	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-106	90	95	避雷対策設備	誘導雷対策	誘導雷対策の有無	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。

© 2026 aiESG, Inc.

No.	指針No.(*1)	指針No.(*2)	種別	サービスレベル項目	規程内容	回答
S-107	91	96	空調設備	空調設備	空調設備（床吹き上げ空調、コンピュータ専用個別空調等）の内容	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-108	92	97	セキュリティ	入退室管理等	入退室記録の有無と、「有り」の場合はその保存期間／監視カメラの有無／個人認証システムの有無	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-109	93	98	セキュリティ	媒体の保管	紙、磁気テープ、光メディア等の媒体の保管のための鍵付きキャビネットの有無／保管管理手順書の有無	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
S-110	94	99	セキュリティ	その他セキュリティ対策	その他特筆すべきセキュリティ対策を記述（破壊侵入防止対策、防犯監視対策等）	利用するクラウド基盤（Google Cloud）のデータセンターの基準によります。当社は、クラウド事業者の選定時に、入退室管理や自然災害への対策等の物理的セキュリティ対策を第三者認証等により確認しています。
サポート						
S-111	95	100	サービス窓口（苦情受付・問合せ）	連絡先	電話／FAX、Web、電子メール等の連絡先	お問い合わせの連絡方法は、ご契約時にご案内します。
S-112	96	101	サービス窓口（苦情受付・問合せ）	営業日・時間	営業曜日、営業時間（受付時間）	受付時間は、ご契約時にご案内します。
S-113	97	102	サービス窓口（苦情受付・問合せ）	サポート範囲・手段	サポート範囲	本サービスの操作方法に関するお問い合わせと、不具合の報告です。CDP回答の内容に関する助言、スコア等の解釈の個別説明は含みません（利用規約第13条第7項・第8項）。
S-114	97	102	サービス窓口（苦情受付・問合せ）	サポート範囲・手段	サポート手段（電話、電子メールの返信等）	ご契約時にご案内します。
S-115	98	103	サービス通知・報告・インシデント対応	メンテナンス等の一時的サービス停止時の事前告知	利用者への告知時期（1ヵ月前、3ヵ月前、6ヵ月前、12ヵ月前等の単位で記述）	可能な限り事前にお知らせします。緊急の場合は事前の通知なく実施することがあります（利用規約第10条第2項）。
S-116	98	103	サービス通知・報告・インシデント対応	メンテナンス等の一時的サービス停止時の事前告知	告知方法	サービス画面への掲示または登録メールアドレス宛の電子メール
S-117	99	104	サービス通知・報告・インシデント対応	障害・災害発生時の通知	障害発生時通知の有無と、「有り」の場合は通知方法及び利用者への通知時間	有。登録メールアドレス宛に、速報と復旧の見通しをお知らせします。
S-118	100	105	サービス通知・報告・インシデント対応	セキュリティ・インシデント対応	セキュリティに関するインシデントが発生した場合の対応（通知、被害の拡大防止、暫定対処、本格対処など）	入力データ・出力データ・利用者情報の漏えい等のインシデントを認識した場合は、速やかに利用者に通知し、必要な調査、被害の拡大防止、復旧および再発防止の措置を講じます（利用規約第18条第7項）。社内規程では、認識後72時間以内の通知を定めています。対応後は教訓を対応手順の改善に反映しています。
S-119	101	106	サービス通知・報告・インシデント対応	定期報告	利用者への定期報告の有無（アプリケーション、サーバ、プラットフォーム、その他機器の監視結果、サービス稼働率、SLAの実施結果等）	定期報告は行っていません。利用者の合理的な求めがある場合は、1年に1回を限度に、安全管理措置とインシデント対応措置の実施状況に関する情報を提供します（利用規約第18条第8項）。

© 2026 aiESG, Inc.

追加項目（生成AI・認証・クラウド設定・サプライチェーン・マネジメント）

株式会社aiESG　回答日：2026年10月16日　版数：1.0

IPA・経済産業省・総務省の指針に含まれない項目のうち、利用企業のセキュリティ審査でよく確認される項目を記載しています。ISMS観点・AIMS観点の項目は各規格の観点で整理したものであり、当社はこれらの認証を取得していません。

ID	区分	項目	回答
生成AI			
AI-1	生成AI	利用しているAIモデルと提供経路	Google Cloud（Vertex AI）経由で、Anthropic社の大規模言語モデル「Claude」を利用しています。他の生成AIサービスは利用していません。
AI-2	生成AI	AIモデル提供元による入力データの学習利用	LLMの提供元（Google Cloud Vertex AI経由のAnthropic Claude）は、本サービスから送信された入力データをモデルの学習に利用しません。
AI-3	生成AI	当社による入力データ・出力データの利用	当社は、利用者の入力データ・出力データ等を、特定の個人および利用者を識別できないように匿名化または統計的に処理したうえで、利用規約第18条第5項に定める目的の範囲に限り利用します。同項は「当社は、入力データ及び出力データを、分析モデルの開発若しくは改善又はＡＩの学習のために利用せず、又は第三者に利用させないものとします。」と定めています。統計情報を第三者に提供・公表する場合は、特定の利用者を識別できない形式で行います。
AI-4	生成AI	入力データを学習に利用させない設定の可否	当社は利用者のデータをAIの学習に利用しないため、設定は設けていません。
AI-5	生成AI	生成AI処理の所在地	生成AI機能の処理は、日本国外のリージョンで行われる場合があります。預託データの保管場所（日本国内）とは異なります。
AI-6	生成AI	他の利用企業への出力の混入	入力データが他の利用企業に対して出力されることはありません。利用企業ごとのデータはアプリケーション層で論理的に分離しています。
AI-7	生成AI	出力の正確性と利用者の確認	生成AIによる文章は、事実と異なる内容や不完全な内容を含む可能性があります。利用者が正確性・適法性・適切性を確認したうえで利用するものとしています（利用規約第16条）。
AI-8	生成AI	AI固有の攻撃への対策	AIに対する攻撃手法（プロンプトインジェクション等）や動向について情報を収集し、対応しています。詳細はセキュリティ上の理由により非公開（個別のご依頼時にご案内）。
AI-9	生成AI	AIに関する社内ルール	従業員向けにAIツールの利用ガイドラインを定め、教育を行っています。学習データの収集・利用について、個人情報と知的財産権に関するルールを定めています。
多要素認証（MFA）・認証			
MFA-1	多要素認証・認証	利用者のログイン方式	IDとパスワードによる認証です。二要素認証も利用できます（MFA-4参照）。
MFA-2	多要素認証・認証	利用者パスワードの要件	12文字以上とし、英大文字・英小文字・数字・記号をそれぞれ含めることを必須にしています。パスワードは安全な方式でハッシュ化して保管しています。
MFA-3	多要素認証・認証	パスワード再発行時の本人確認	登録メールアドレス宛に、有効期限付き（1時間）のワンタイムのリセット用リンクを送信します。
MFA-4	多要素認証・認証	利用者向け多要素認証	認証アプリ（TOTP）による二要素認証をご利用いただけます。各利用者が設定でき、組織の管理者が組織全体で必須にすることもできます。

© 2026 aiESG, Inc.

ID	区分	項目	回答
MFA-5	多要素認証・認証	当社の管理画面・管理ツールの認証	管理画面・管理ツールのすべてのアカウントに多要素認証（パスワード＋ワンタイムパスワード）を適用しています。
MFA-6	多要素認証・認証	開発・運用基盤の認証	緊急用アカウント等の例外を除き、開発・運用に携わる要員のすべてのアカウントに多要素認証を適用しています。
MFA-7	多要素認証・認証	セッション管理	一定時間操作がない場合、セッションをタイムアウトさせています。
MFA-8	多要素認証・認証	利用企業によるアカウント管理	利用企業の管理者権限を持つアカウントが、アカウントの追加・削除・利用停止・権限変更、一覧の表示・出力を行えます。
クラウド設定			
CL-1	クラウド設定	利用しているクラウド基盤	Google Cloudのみを利用しています。
CL-2	クラウド設定	責任の分担	データセンターの物理的対策と基盤の運用はクラウド事業者が、アプリケーション・クラウド環境の設定・当社アカウントの管理は当社が、利用企業内のアカウント・権限の管理は利用者が担います。
CL-3	クラウド設定	設定の管理と監視	クラウド環境の構成はコードで管理し、変更はレビューを経て履歴を残しています。
CL-4	クラウド設定	管理アクセスの制限	クラウド環境の管理権限は、承認を得た限られた担当者に必要最小限で付与し、多要素認証を適用しています。
CL-5	クラウド設定	預託データの保管場所	日本（Google Cloud 東京リージョン、複数ゾーンに冗長化した構成）
CL-6	クラウド設定	バックアップデータの保管場所	日本（Google Cloud 東京リージョン）
CL-6b	クラウド設定	ログの保管場所	アプリケーションのログの保存場所は、日本国内に限定していません。
CL-7	クラウド設定	ログの保存	アプリケーションのログは365日間保存しています。管理者の特権操作の記録は400日間、改ざんできない形式で保存しています。
サプライチェーン			
SC-1	サプライチェーン	主な委託先・外部サービス	Google Cloud（サーバー・データベース・生成AI。データは日本、生成AIの処理は国外の場合あり）、SendGrid（メール送信、米国）、Slack（問い合わせの社内通知、米国）、Sentry（エラー情報の収集、米国。メールアドレス等は除いて送信）、Backlog（問い合わせの管理、日本）を利用しています。
SC-2	サプライチェーン	委託先の選定・管理基準	委託先の選定・管理の基準を定め、定期的に見直しています。外部サービスやツールを利用する際は、セキュリティ水準を確認しています。
SC-3	サプライチェーン	委託先との契約上の要求事項	秘密保持、セキュリティ対策、情報の消去、関連法令の遵守、セキュリティインシデント発生時の報告・対処を契約で定めています。委託先には、利用規約に基づき当社が負う義務と同等の義務を課しています（利用規約第14条）。
SC-4	サプライチェーン	委託先の履行確認・評価	契約更新時に、合意内容の履行状況と業務・セキュリティ対応を確認しています。クラウド事業者は、第三者認証（ISO/IEC 27001、SOC 2等）の取得状況を随時確認しています。
SC-5	サプライチェーン	オープンソースソフトウェアの管理	利用しているオープンソースソフトウェアを把握し、依存ライブラリの脆弱性を常時検知しています。重大な脆弱性は優先的に修正しています。
SC-7	サプライチェーン	APIの認証情報の管理	外部サービスのAPIを利用する際の認証情報は、業務上必要な担当者のみがアクセスできるよう制限しています。
情報セキュリティマネジメント（ISO/IEC 27001の観点）			

© 2026 aiESG, Inc.

ID	区分	項目	回答
IS-1	ISMS観点	情報セキュリティ方針	経営層の承認を得て、情報セキュリティに関する社内規程（情報セキュリティガイドブック）を定め、全従業員に周知しています。規程の改定時に内容を見直しています。
IS-2	ISMS観点	経営層の関与	セキュリティリスクへの対応計画は経営層が承認し、進捗と結果を経営層に報告しています。
IS-3	ISMS観点	第三者認証	ISMS（ISO/IEC 27001）等の第三者認証は取得していません。
IS-4	ISMS観点	内部監査・評価	独立した部門による定期的な評価は行っていません。社内規程の改定時等に、管理部門が対策の整備・運用状況を確認しています。
IS-5	ISMS観点	情報資産の管理	情報資産の管理手順と重要度の基準を文書化し、情報資産の一覧を作成しています。手順は定期的に見直しています。
IS-6	ISMS観点	採用時の確認	採用時は、書類審査や面接等による選考を行い、入社時に所定の書類の提出を求めています。
IS-7	ISMS観点	教育・意識向上	入社時と社内規程の改定時に、セキュリティと重要情報の取扱いに関する教育を行っています。
IS-8	ISMS観点	違反時の懲戒	就業規則に、会社や取引先の秘密・情報の漏えい、社内規程への違反等を懲戒事由として定めています。
IS-9	ISMS観点	秘密保持	従業員と、秘密保持契約または誓約書を締結しています。
IS-10	ISMS観点	退職・契約終了時の手続	アクセス権の変更・削除と貸与資産の返却を、文書化した手順に基づき行っています。
IS-11	ISMS観点	業務端末とリモートワーク	業務用端末には、マルウェア対策ソフトの導入とセキュリティ更新の適用を行っています。禁止するソフトウェアを規程で定め、利用されないよう制限・確認しています。外部記憶媒体の利用は原則禁止しています。
IS-12	ISMS観点	共有アカウント	開発・運用での共有アカウントの利用は原則禁止しています。例外的に利用する場合は事前の承認を必要とし、管理簿や利用ログで確認しています。
IS-13	ISMS観点	インシデント対応体制	インシデント対応の役割・責任と手順を定め、定期的に見直しています。対応や他社事例から得た教訓を、手順の改善に反映しています。
IS-14	ISMS観点	法令・契約上の要求事項	サービス提供にあたって遵守すべき法令・規制・契約上の要求事項を整理し、対応しています。個人情報は個人情報保護法に従って取り扱っています。
IS-15	ISMS観点	セキュアな開発	開発時のセキュリティ要件を明確にし、定期的に見直しています。要件のレビュー、ソースコードのレビュー、各工程の承認を行っています。開発環境と本番環境を分離しています。不具合調査等でお客様のデータを本番以外の環境で扱う場合は、必要な範囲に限り、当社の担当者のみがアクセスできる環境で扱い、目的の終了後に削除します。変更は、本番環境と同等の環境で事前にテストしています。認証情報（シークレット）の混入は、コミット前に検出して防いでいます。
IS-16	ISMS観点	構成管理・変更管理	システム構成とネットワーク構成、その変更状況を構成管理・変更管理により把握しています。
IS-17	ISMS観点	事業継続	サービスの障害・停止・データ消失をインシデントとして定義し、復旧とエスカレーションの手順を定めています。システムは国内リージョン内の複数のゾーンに冗長化しています。
AIマネジメント（ISO/IEC 42001・AI事業者ガイドラインの観点）			
AM-1	AIMS観点	AIに関する方針・ルール	従業員向けにAIツールの利用ガイドラインを定めています。学習データの収集・利用について、個人情報と知的財産権に関するルールを定めています。
AM-2	AIMS観点	AIの利用目的と範囲	AIは、CDP回答案の作成支援やスコア分析等に利用しています。最終的なCDP回答の作成と提出は、利用者が行います。

© 2026 aiESG, Inc.

ID	区分	項目	回答
AM-3	AIMS観点	人による確認	生成AIによる文章は、利用者が正確性・適法性・適切性を確認したうえで利用するものとしています（利用規約第16条）。
AM-4	AIMS観点	利用者への説明	AI機能に関する利用条件（データの扱い、出力の正確性、責任分担）を利用規約で明示しています。
AM-5	AIMS観点	画面上でのAI生成の表示	AIアシスタントは専用のパネルに表示し、入力欄の下に注意書きを表示しています。ガイダンスのうちAIで補った説明には「AI補足」と表示しています。
AM-6	AIMS観点	AIのリスク評価・影響評価	AI機能の導入・変更ごとに影響評価を行う手順は定めていません。生成AIの用途を回答案の作成支援等に限り、最終的な判断は利用者が行う設計としたうえで、モデル提供元が入力データを学習に利用しないことの確認（AM-7）、モデル切り替え前の出力確認（AM-8）、利用者による確認（AM-3）によってリスクを抑えています。
AM-7	AIMS観点	AIモデルの提供者の管理	外部のサービスやツールを利用する際は、セキュリティ水準を確認しています。AIモデルの提供元が入力データを学習に利用しないことを確認しています（AI-2参照）。
AM-8	AIMS観点	AIモデルの変更時の対応	利用モデルを切り替える前に、社内で出力を確認してからリリースしています。切り替えはサービス内のお知らせでご案内します。
AM-9	AIMS観点	出力品質の監視・改善	利用者からのご意見をお問い合わせで受け付け、担当者が内容を確認したうえで、プロンプトや参照資料の改善に随時反映しています。変更は社内で出力を確認してからリリースしています。
AM-10	AIMS観点	入力内容・出力のログの保存	AIアシスタントのやりとり（入力・出力・会話の履歴）は当社のデータベースに保存し、365日で自動削除しています。閲覧できるのは当社のみです。プロンプトや出力のキャッシュ（使い回し）は行っていません。
AM-11	AIMS観点	AIに関する問い合わせ窓口	サービス内のお問い合わせフォームで受け付けています。

© 2026 aiESG, Inc.