

ヘルプドッグ セキュリティチェックシート(IPA準拠)

noco株式会社
更新日: 2024年5月23日

本資料はIPA(独立行政法人情報処理推進機構)が公開している「安全なウェブサイトの作り方 改訂第7版」に基づき、noco株式会社から提供する「ヘルプドッグ」のセキュリティについて記載したものです。お客様フォーマットのチェックシートへの回答をご希望の場合は、別途有料オプションを提供しております。詳細は営業担当までお問い合わせください。

No	脆弱性の種類	対策の性質	チェック	実施項目	解説
1	SQLインジェクション	根本的解決	※ ■ 対応済 □ 未対策 □ 対応不要	■ 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
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	□ 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
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	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)
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	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)
2	OSコマンド・インジェクション	根本的解決	■ 対応済 □ 未対策 □ 対応不要	■ シェルを起動できる言語機能の利用を避ける。	2-(i)
		保険的対策	□ 対応済 □ 未対策 ■ 対応不要	□ 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)
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	※ ■ 対応済 □ 未対策 □ 対応不要	■ 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
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	□ 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
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	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)
4	セッション管理の不備	保険的対策	■ 対応済 □ 未対策 □ 対応不要	ファイル名のチェックを行う。	3-(iii)
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	セッションIDを推測が困難なものにする。	4-(i)
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	セッションIDをURLパラメータに格納しない。	4-(ii)
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	HTTPS通信で利用するCookieにはsecure属性を加える。	4-(iii)
5	クロスサイト・スクリプティング	根本的解決	※ ■ 対応済 □ 未対策 □ 対応不要	■ ログイン成功後に、新しくセッションを開始する。	4-(iv)-a
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	□ 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
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	セッションIDを固定値にしない。	4-(v)
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	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)
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	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)
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	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)
6	CSRF (クロスサイト・リクエスト・フォージェリ)	根本的解決	■ 対応済 □ 未対策 □ 対応不要	<script>...</script> 要素の内容を動的に生成しない。	5-(iii)
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	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)
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	入力値の内容チェックを行う。	5-(v)
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	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)
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	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)
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	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)
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	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)
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	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)
		根本的解決	※ ■ 対応済 □ 未対策 □ 対応不要	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
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	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
保険的対策	■ 対応済 □ 未対策 □ 対応不要	■ 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。 noco注: CORSの設定とOriginヘッダのチェックを使用。	6-(i)-c		
7	HTTPヘッダ・インジェクション	保険的対策	■ 対応済 □ 未対策 □ 対応不要	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)
		根本的解決	※ ■ 対応済 □ 未対策 □ 対応不要	■ 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APIを使用する。	7-(i)-a
8	メールヘッダ・インジェクション	根本的解決	■ 対応済 □ 未対策 □ 対応不要	□ 改行コードを適切に処理するヘッダ出力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
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	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)
		根本的解決	※ ■ 対応済 □ 未対策 □ 対応不要	■ 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
9	クリックジャッキング	根本的解決	■ 対応済 □ 未対策 □ 対応不要	■ 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
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	HTMLで優先を指定しない。	8-(ii)
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	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)
9	クリックジャッキング	根本的解決	※ ■ 対応済 □ 未対策 □ 対応不要	■ 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。 noco注: 後継の仕様であるContent-Security-Policy: frame-ancestorsヘッダを使用。	9-(i)-a
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	■ 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

			<input checked="" type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	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)
10	バッファオーバーフロー		<input checked="" type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	<input checked="" type="checkbox"/> 直接メモリにアクセスできない言語で記述する。 <input type="checkbox"/> 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)-a
			<input checked="" type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	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-(i)-b
			<input checked="" type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	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)
11	アクセス制御や認可制御の欠落		<input checked="" type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	アクセス制御機能による防衛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が必要とする認証機能を設ける。	11-(i)
			<input checked="" type="checkbox"/> 対応済 <input type="checkbox"/> 未対策 <input type="checkbox"/> 対応不要	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ましてアクセスできないようにする。	11-(ii)
※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。					

ヘルプドッグ セキュリティチェックシート(経済産業省準拠)

noco株式会社
更新日: 2024年5月23日

本資料は経済産業省が公開している「クラウドサービスレベルのチェックリスト(2010年8月発行)」に基づき、noco株式会社提供の「ヘルプドッグ」のセキュリティについて記載したものです。お客様フォーマットのチェックシートへの回答をご希望の場合は、別途有料オプションを提供しております。詳細は営業担当までお問い合わせください。

No.	種別	サービスレベル項目	規定内容	測定単位	設定
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	あり 1週間以上前にメール、ホームページで通知
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	あり 1ヶ月以上前にメール、ホームページで通知
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	なし
5		サービス稼働率	サービスを利用できる稼働率(計画サービス時間-停止時間)/計画サービス時間	稼働率(%)	非公開
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	あり システムは複数AZで稼働しています
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	有無	あり バックアップデータを利用して復元します
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(ファイル形式)	非公開
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	あり 機能追加・セキュリティパッチは随時対応しております
10		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	非公開
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	非公開	
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	0回	
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	あり システム外部からの死活監視、パフォーマンス監視	
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	あり 弊社担当者へ連絡(電話やメールなど)します。必要に応じて、お客様への連絡は可能な限り迅速に行われます。
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	時間	あり 弊社担当者への通知はリアルタイムに行われます。必要に応じて、お客様への連絡は可能な限り迅速に行われます。
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	時間(分)	1分間隔
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	非公開
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	アクセスログ(操作の種類の情報を含む)、エラーログ
19		応答時間	処理の応答時間	時間(秒)	非公開
20		遅延	処理の応答時間の遅延継続時間	時間(分)	非公開
21		パッチ処理時間	パッチ処理(一括処理)の応答時間	時間(分)	非公開
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	なし
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	あり サービス内の表記及びヘルプセンターにて掲載
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ー数	有無(制約条件)	非公開
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	非公開
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
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10:00~17:00
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	1日1回データベースのフルバックアップ
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	1日1回のバックアップ実行地点(時刻は非公開)
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	35日
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	解約後30日後(一部のログデータは60日後)オブジェクトストレージ、データベース上のレコード削除
32		バックアップ世代数	保証する世代数	世代数	35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	オブジェクトストレージ、データベースの暗号化(AES-256)
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	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	利用規約に記載
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	あり システムにより一定期間の後、自動削除
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	あり データベース保存時に整合性チェック
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	あり	
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	あり ISMS(ISO/IEC 27001:2022)
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	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	あり
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	あり TLS1.2/1.3
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	なし
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	なし
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	あり IaCによりコード管理されたシステム管理者のみアクセス可能、操作ログの保持
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	アクセスログから検索可能
47		ウイルススキャン	ウイルススキャンの頻度	頻度	リアルタイム(Amazon GuardDuty)
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	外部記憶媒体は利用していません
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	

ヘルブドッグ セキュリティチェックシート(総務省準拠)

noco株式会社
更新日: 2024年6月20日

本資料は総務省が公開している「クラウドサービスの安全・信頼性に係る情報開示指針」に基づき、noco株式会社が提供する「ヘルブドッグ」のセキュリティについて記載したものです。
本資料は一般社団法人日本クラウド産業協会(ASPIC)による「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。
一部の項目について、総務省が公開している「ASP・SaaSの安全・信頼性に係る情報開示指針(ASP・SaaS編) 第3版(ア)」と「AIを用いたクラウドサービスの安心・安全・信頼性に係る情報開示指針(ASP・SaaS編)」(イ)で重複することから「No.」に「ア」もしくは「イ」を併記しております。

No.	ア	イ	種別	サービスレベル項目	開示内容	内容
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)	2024年6月20日
事業所・事業						
2	2		事業所等の概要	事業者名	事業者の正式名称(商号)	noco株式会社
3	3			設立年月日	法人番号	5010001183598
4	4			事業所	事業者の本店所在地	東京都中央区日本橋小舟町8-13
5	5			事業所ホームページ	事業者ホームページ	https://nocoinc.co.jp/
5	5		事業の概要	主な事業の概要	事業者の主な事業概要	ヘルプデスク管理システム「ヘルブドッグ」の開発、運営 フォーム作成管理システム「ヘルブドッグ フォーム」の開発、運営 AIマニュアル作成ツール「トースターチーム」の開発、運営 AI・DX・SaaSコンサルティング事業
人材						
6	6		経営者	代表者	代表者氏名	堀辺 憲
7	7			役員	代表者経歴(生年月日、学歴、業務経歴、資格等)	非公開
8	8		従業員	従業員数	役員数	非公開
					正社員数(単独ベース)	非公開
財務状況						
9	9		財務データ	売上高	事業者の売上高(単独ベース)	非公開
10	10			経常利益	事業者の経常利益額(単独ベース)	非公開
11	11			資本金	事業者の資本金(単独ベース)	非公開
12	12			自己資本比率	事業者の自己資本の比率(単独ベース)	非公開
13	13			キャッシュフロー対有利子負債比率	事業者のキャッシュフロー対有利子負債比率(単独ベース)	非公開
14	14		インタレスト・カバレッジ・レシオ	事業者のインタレスト・カバレッジ・レシオ(単独ベース)	非公開	
15	15		財務信頼性	上場の有無	株式上場の有無と、「有り」の場合は市場名	非上場
16	16			財務監査・財務データの状況	該当する財務監査・財務データの状況を、以下より選択する。 (1)会計監査人による会計監査、(2)会計参与による計算書類の作成、(3)「中小会計要領」の適用に関するチェックリストの活用、(4)監査役による監査、(5)いずれでもない	非公開
17	17			決算公告	決算公告の実施の有無	非公開
資本関係・所属団体						
18	18		資本関係	株主構成	大株主の名称(上位5株主程度)、及び各々の株主保有比率	非公開
19	19		所属団体	所属団体	所属している業界団体、経済団体等の名称	なし
コンプライアンス						
20	20		組織体制	コンプライアンス担当役員	コンプライアンス担当役員の氏名	なし
21	21			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	なし
22	22			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責任者の有無と、「有り」の場合は責任者名・役職 情報セキュリティに関する組織体制の有無	あり
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	情報セキュリティに関する方針 https://nocoinc.co.jp/informationsecurity/privacy-policy/ https://nocoinc.co.jp/privacypolicy/
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 守秘義務違反があった場合のペナルティ条項の有無	あり
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	あり
26	26			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	あり
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 自社の個人情報保護指針に対する順守規定の有無	aaS: AWS, Cloudflare(CDNとして利用) aaSの契約内容による
28	28			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 委託先(再委託先)との守秘義務対応状況 委託先(再委託先)の管理方法	aaSの契約内容による aaSの契約内容による aaSとしての利用
29	29			情報セキュリティに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	情報セキュリティ基本方針、ISMSマニュアル、適用宣言書、情報セキュリティ管理規程、就業規則、情報資産、リスクアセスメント表、関連法規制一覧表、情報セキュリティ目的管理表、教育計画・実績表、事業継続計画・結果表、内部監査計画結果、是正処置報告書、内部監査チェックリスト、マネジメントレビュー議事録、機器管理台帳
30	30		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 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	事業継続計画 非公開	
31	31		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	リスク対応計画、リスクアセスメント規定	
32	32		文書類	勧誘・販売・係争に関する規定等の整備	勧誘・販売に関する基本方針・規定・マニュアル等の有無と、「有り」の場合は文書名 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	なし 利用規約に記載
33	33			ASP・SaaSの苦情対応に関する規定等の整備	ASP・SaaSの苦情処理に関する基本方針・規定・マニュアル等の有無と、「有り」の場合はそれらの文書名 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	苦情処理マニュアル 利用規約に記載

34	-	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」の場合は文書名方針等の文書の作成においては、「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」における対策項目を参照すると良い。	なし サービスマニュアルは、サービス内の表記及びヘルプセンターにて掲載
サービス基本特性				
35	34	サービス名称	本ASP・SaaSサービス名称	ヘルプドッグ
36	35	サービス開始時期	本ASP・SaaSのサービス開始年月日（西暦） 本サービス開始から申請時までの間の大規模な改変等の有無と、「有り」の場合は改変年月日（西暦）	2024年5月14日 なし
37	36	サービスの内容・範囲	本ASP・SaaSサービスの内容・特徴 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	カスタマーサポート業務に必要な機能を提供。 お客様の疑問を解決し、顧客満足度を高めるクラウドサービス。 あり サービス内のデータ連携
38	37	サービス提供時間	サービスの提供時間帯	24時間365日（計画停止を除く）
39	38	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）	なし
40	39	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）	なし
41	-	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	カスタマーサポートの一貫として対応可能性あり。 詳細は契約時にお尋ねください。
-	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	https://nocoinc.co.jp/ai-policy/
-	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 利用規約に記載
-	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 利用者が入力したデータは、構築済み学習モデルへの入力としてのみ利用し、モデルの学習には利用しません
-	43	権利関係	権利関係	利用者データに関する権利（所有権、使用权、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 利用規約に記載
42	44	サービスの更新・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） 告知方法 利用規約に記載
43	45	サービスの更新・終了後の対応・代替措置	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 なし
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 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 削除又は廃棄したことの証明書等の提供 なし（IaaS上のデータ削除を実施） なし
45	47	サービス料金	料金体系	初期費用額 月額利用額 最低利用契約期間 料金表に記載、もしくは契約時に提示 料金表に記載、もしくは契約時に提示
46	48	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	なし
47	49	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）	利用規約に記載
48	50	サービス稼働設定値	サービス稼働率の目標値 サービス稼働率の実績値 サービス停止の事故歴	非公開 非公開 なし
49	51	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 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	1分おきに検知 複数のサービス上のエンドポイントに対する外形監視、及びサーバの各種メトリクスの取得・通知 IaaSに準拠、またはオートスケール設定による
50	52	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	認証基準：ISO/IEC 27001:2022（JIS Q 27001:2023） 認証番号：GIJP-0320-1C
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 ソースコードの脆弱性チェック、WAFによるOWASP等のポリシー適用
52	-	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。	なし
53	-	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	営業担当、もしくはカスタマーサポートにご相談ください
54	54	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 世代バックアップ（何世代前までかを記述）	日々 35世代
55	55	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） DR（ディザスタリーカバリー）対策の有無と、「有り」の場合はその概要	高可用性ストレージ、複数AZによるサーバ稼働 なし
56	56	受賞・表彰歴	ASP・SaaSに関連する各種アワード等の受賞歴	なし
57	57	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	なし
58	58	契約者数	契約者数	本ASP・SaaSサービスの契約企業数等 非公開
アプリケーション等				

-	59		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	利用者の入力データの量・質に依存システム側で学習モデルや入力データの加工ロジックを定期的に更新（利用者のデータを再学習するわけではない）
-	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）	システムによって自動で実行
-	61		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）	ブラックボックス型
59	62		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	あり サービス内の表記及びヘルプセンターにて掲載
-	63	連携	AI関連の連携	API等による他社のAI機能の活用有無、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	あり OpenAI社のAPIを利用（OpenAI社のモデル学習には利用されない設定）
60	64		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	あり 複数のサービス上のエンドポイント
61	65		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	あり Amazon Time Sync Serviceを利用
62	66		ウイルス対策	ウイルス対策の有無	あり Amazon GuardDutyによるリアルタイムスキャン
63	67		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	あり IaCによるコードレビューを実施
64	68		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	事業者側によって利用者のID・PWを付与しません
65	69		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 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 ログの改ざん防止措置の有無	HTTPリクエストログを保持 保持期間は400日 利用者に提供はありません あり 無期限 あり
66	70		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	週1回以上の検出・対応
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	あり オブジェクトストレージ、データベースをAES-256によって暗号化
68	-		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	あり 1. IDとアクセス管理(IAM) : IaCによるコード管理、多要素認証あり、限定したメンバーのみの権限付与、本番/開発アカウントの分離、ゲストユーザーを利用せず 2. ロギングとモニタリング: クラウドの不正利用検知の仕組みを導入 3. オブジェクトストレージ: IaaS提供の暗号化キーを利用 4.1. 仮想マシン: コンテナ技術を利用しているため、VMは利用せず 4.2. ネットワーク: サーバはプライベートネットワークに配置、WAF(Cloudflare)、DDoS対策(Cloudflare)、IDS(Amazon GuardDuty)の利用 5. セキュリティ等の集中管理: 鍵管理システムの利用、 6.1. 鍵管理: IaaSの鍵管理システム(AWS Systems Manager Parameter Store)を利用、アクセスログの保持 6.2. PaaSが提供するアプリケーション: 利用せず 6.3. データベース: プライベートネットワークを利用、監査ログ取得、ストレージ暗号化 6.4. コンテナ: IaaS(Amazon ECS)を利用しているため、既定値のまま 7. その他の設定項目: 特利用せず
-	72		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	なし（モデルの再学習を行っていないため）
-	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	リアルタイム処理は数秒以内に応答開始、バッチ処理は非公開
ネットワーク					
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	インターネット回線
70	75		帯域	データ通信速度の範囲、帯域保証の有無	帯域保証なし
71	76		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	WAF(Cloudflare)を利用
72	77		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	IDS(Amazon GuardDuty)を利用
73	78		ネットワーク監視	事業者とエンドユーザー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	専用線の対応なし
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	メールアドレス/パスワード
75	80		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	なし
76	81		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	あり TLS1.2/1.3
77	82		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）	なし
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 ユーザ接続回線について、ASP・SaaS事業者が負う責任範囲	インターネット回線 （仮想OS環境、VPNなどのネットワーク制限下での動作は保証外） インターネット回線・ISP契約はご利用者の責任でご利用ください
79	84		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	あり 目安として、常時10Mbps以上の固定回線を推奨
端末					
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 利用するブラウザの種類	動作環境ページで公開 https://nocoinc.co.jp/environment/helpdog/ 動作環境ページで公開 https://nocoinc.co.jp/environment/helpdog/
ハウジング（サーバ設置場所）					
81	86		建物形態	データセンター専用建物か否か 国名、日本の場合は地域ブロック名（例：関東、東北）	IaaS利用のため記載せず AWS: 日本国内の東京リージョン Cloudflare: 利用者データを保持しておらず、CDNの特性のため世界各地
82	87	施設建築物	所在地	特筆すべき立地上的優位性があれば記述（例：標高、地盤等）	IaaS利用のため記載せず
83	88		耐震・免震構造	耐震数値 免震構造や制震構造の有無	IaaS利用のため記載せず IaaS利用のため記載せず
84	89		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	IaaS利用のため記載せず

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）	IaaS利用のため記載せず
86	91		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	IaaS利用のため記載せず
87	92	消火設備	サーバールーム内消火設備	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	IaaS利用のため記載せず
88	93		火災感知・報知システム	火災検知システムの有無	IaaS利用のため記載せず
89	94		直撃雷対策	直撃雷対策の有無	IaaS利用のため記載せず
90	95	避雷対策設備	誘導雷対策	誘導雷対策の有無	IaaS利用のため記載せず
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	IaaS利用のため記載せず
92	97		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	IaaS利用のため記載せず IaaS利用のため記載せず
93	98	セキュリティ	媒体の保管	個人認証システムの有無 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	IaaS利用のため記載せず IaaS利用のため記載せず
94	99		その他セキュリティ対策	保管管理手順書の有無 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）	IaaS利用のため記載せず IaaS利用のため記載せず
サービスサポート					
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 代理店連絡先の有無と、「有り」の場合は代理店名称、代理店の本店の所在地と連絡先	お問合せフォーム（ https://helpdog.ai/f/nocoinc/helpdog-support ） 電話またはメール（契約時ご確認ください） 代理店なし
96	101		営業日・時間	営業曜日、営業時間（受付時間）	平日10:00～17:00
97	102		サポート範囲・手段	サポート範囲 サポート手段（電話、電子メールの返信等）	サービス状態監視と障害対応を24時間365日実施 電話またはメール
98	103		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カ月前、3カ月前、6カ月前、12カ月前等の単位で記述） 告知方法	利用に影響がある場合、1週間以上前に告知（緊急対応時を除く） メール、ホームページ
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	全利用者に影響する場合やサービス停止を伴う場合、メール、ホームページで速やかに告知 それ以外の場合、該当利用者に通知
100	105		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）	全利用者に影響する場合やサービス停止を伴う場合、メール、ホームページで速やかに告知 それ以外の場合、該当利用者に通知
101	106		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）	なし