GENFLUX Evaluation セキュリティチェックシート

株式会社Elith ｜ 第1.3版 ｜ 2026年9月10日

本書は標準のクラウド型サービスを基盤とする共通のセキュリティ・運用統制を記載します。顧客の要件に応じたカスタマイズの範囲・構成は、合意した仕様書・個別契約に従います。DBは評価データを保存するデータベースを指します。

1. サービス概要

No.	確認項目	確認内容	GENFLUX Evaluationの実施内容
1	提供者・サービス名	提供主体と対象サービス	株式会社Elithが提供する「GENFLUX Evaluation」を対象とする。
2	サービスの目的	提供する主な機能	生成AI、RAG、AIエージェントの品質、安全性、ポリシー適合性を評価・可視化する。
3	提供形態	SaaS / オンプレミス等	Webブラウザから利用するクラウド型SaaS。標準構成では、顧客環境へのサーバー設置は不要。
4	主要稼働地域	アプリケーション・DBの地域	・ アプリケーション：Google Cloud 東京リージョン ・ DB：Google Cloud 東京リージョン
5	第三者認証	ISMS・AIMSの取得状況	当社は、企業向けAI活用SaaSプラットフォーム「GENFLUX」の提供を対象とするISMS（ISO/IEC 27001:2022）およびAIMS（ISO/IEC 42001:2023）を2026年8月21日付で取得。適用範囲は認証書に従う。 AIガバナンス第三者認証「C認証」を2026年8月4日付で取得。C認証は当社の組織体制・運用を対象とする法人単位の認証。
6	責任分界	Elith・基盤事業者・利用者の役割	・ Elith：アプリケーションおよびサービス運用 ・ クラウド事業者：クラウド基盤 ・ 利用者：アカウント、入力データ、評価対象の管理

2. データ管理

No.	確認項目	確認内容	GENFLUX Evaluationの実施内容
7	主な取扱データ	保存・処理する情報	・アカウント情報、評価設定 ・テスト入力、AI出力、参照文脈、評価結果、レポート ・操作・認証ログ、任意で取り込んだ文書
8	データ最小化	個人情報・機密情報の取扱い	評価に必要なデータのみを取り扱う。個人情報・機密情報の投入可否と取扱条件は、利用契約および顧客の社内規程で定める。
9	外部AI処理	生成AI事業者へのデータ送信	評価方式により、テスト入力、AI出力、参照文脈を選択した生成AI事業者へ送信する。送信先と送信項目は、利用する生成AI事業者と評価設定で決まる。
10	モデル学習	入力・出力の学習利用	入力情報・評価結果を当社または外部事業者のAIモデルの学習・トレーニング目的で利用・提供しない。外部事業者についても同目的で利用されないよう措置を講じる。
11	データ所在地	保存・処理地域	・アプリケーション・評価データを保存するDB：東京リージョン ・認証基盤・外部AIサービスでのデータの取扱い：各事業者の提供条件に従う
12	テナント分離	他社データとの分離	顧客組織ごとのテナント識別子でデータを論理分離する。APIで認証情報と所属テナントを照合する。
13	通信時暗号化	インターネット・DB通信	・利用者との通信：HTTPS/TLS ・DB接続：暗号化接続
14	保存時暗号化	DB・クラウド保存領域	・Google Cloud上の保存データ：Google Cloudの標準暗号化 ・認証データ：Supabase管理基盤で保護
15	秘密情報管理	APIキー・DB資格情報	APIキーとDB資格情報をGoogle Cloud Secret Managerで管理する。実行主体ごとに必要な権限のみを付与する。
16	保持・消去	保持期間と契約終了時の取扱い	評価データ・監査イベントの保持期間は、個別契約で定めた条件がある場合はその条件を適用する。契約終了時は利用規約に基づきデータを消去できる。必要な結果は契約終了前に出力する。契約終了後の継続閲覧・保管は保証しない。
17	データ出力	レポート・データ返却	・評価結果：画面で閲覧 ・レポート：PDF出力 ・契約終了時の一括出力：個別契約

3. 認証・アクセス制御

No.	確認項目	確認内容	GENFLUX Evaluationの実施内容
18	利用者認証	標準のログイン方式	・ 認証基盤：Supabase Auth ・ API認証：JWTをサーバー側で検証 ・ 認証失敗時：API要求を拒否
19	APIアクセス制御	画面・API間の認証	Bearerトークンを検証し、ユーザー、所属テナント、アカウントの有効状態を確認する。
20	権限ロール	管理者・一般・閲覧者	・ ロール：admin / member / viewer ・ ユーザー管理・組織設定：adminのみ実行可能
21	アカウント管理	登録・変更・無効化	・ テナント管理者：同一テナント内のユーザー権限と有効状態を管理 ・ 無効なアカウント・テナント：アクセスを拒否
22	多要素認証	MFAの方式と適用	・ 方式：TOTP ・ 適用単位：テナント設定 ・ TOTPシークレット：暗号化して保存
23	企業ID連携	SSO / IdP連携	・ 標準構成：Supabase Auth ・ SSO / IdP連携：個別設計
24	接続元制御	IPアドレス等による制限	接続元IPアドレス制限は個別構成。
25	不正利用対策	総当たり・再設定悪用への対策	パスワード再設定に送信回数、再送間隔、試行回数の制限を適用する。

4. アプリケーションセキュリティ

No.	確認項目	確認内容	GENFLUX Evaluationの実施内容
26	ブラウザ保護	CSP・クリックジャッキング等	・ CSP：外部読込先を制限 ・ X-Frame-Options：埋込みを制限 ・ nosniff、Referrer-Policy、Permissions-Policy：ブラウザ機能を制限
27	入力検証	不正入力への対策	API入力をスキーマで検証し、想定外の形式・範囲を拒否する。
28	認可	越権アクセスの防止	ユーザー、テナント、ロールに基づいて認可する。顧客データへの処理にはテナント識別子を適用する。
29	外部URL制御	Web収集機能のアクセス範囲	Web収集先を許可されたオリジンに制限する。プライベートネットワークおよび予約済みネットワークへのアクセスを拒否する。
30	ブラウザセッション	Cookie・ログイン状態	Web収集で使用するログイン状態は、稼働中のブラウザコンテキスト内で処理する。ディスクへ保存しない。
31	ファイル取込み	文書アップロード時の制御	・ アクセス制御：認証およびテナント境界を適用 ・ 入力制御：ファイル形式・サイズを検証 ・ マルウェアスキャン：個別構成
32	開発・変更管理	テスト・レビュー・本番反映	・ 本番反映前：型検査、静的検査、テスト、DB migration、ビルド確認 ・ 本番運用：バージョン化したリビジョンを使用
33	脆弱性管理	検出・是正・第三者診断	・ 依存ライブラリと脆弱性情報を管理し、修正を反映 ・ 第三者診断・結果開示：個別契約

5. 基盤・可用性

No.	確認項目	確認内容	GENFLUX Evaluationの実施内容
34	実行基盤	冗長性・自動拡張	アプリケーションはGoogle Cloud Runで稼働する。負荷に合わせて複数インスタンスへ自動拡張する。
35	DBネットワーク	データベースの公開範囲	・公開IPv4：無効 ・接続経路：VPC経由のプライベート接続 ・通信：暗号化接続
36	高可用性	ゾーン障害への備え	DBは、同一リージョン内の複数ゾーンを使用するREGIONAL高可用性構成。
37	バックアップ・復元	世代管理・PITR	・自動バックアップ：有効、14世代保持 ・ポイントインタイムリカバリ：有効 ・トランザクションログ：7日保持
38	稼働監視	エラー・遅延・DB負荷等	・監視対象：サービスエラー、応答時間、稼働インスタンス、DB負荷、認証異常 ・異常検知：運用アラートを通知
39	境界防御	WAF・DDoS対策	・DDoS対策：Google Cloud基盤の標準保護 ・専用WAF：個別構成
40	BCP・災害対策	復旧方針・追加冗長化	・リージョン内対策：マルチゾーンDB、自動バックアップ、PITR ・リージョン間冗長化：個別設計
41	物理セキュリティ	入退室・設備・媒体管理	Google Cloudデータセンターの物理・環境統制を使用する。

6. 運用・サポート

No.	確認項目	確認内容	GENFLUX Evaluationの実施内容
42	本番アクセス	運用担当者のアクセス制御	・本番アクセス：Google Cloud IAMおよびサービスアカウントで制御 ・シークレット：対象リソース単位で権限を付与
43	監査ログ	操作・認証イベント	・対象：認証および重要なシステム操作 ・基本項目：テナント、実行者、操作、対象 ・追加項目：要求ID、接続元情報、ユーザーエージェント（一部イベント）
44	ログ保持	クラウド・監査ログの保持	・標準クラウドログ：30日保持 ・監査イベント：サービスDBに保存 ・評価データ・監査イベント：保持期間を個別契約で定めた場合はその条件を適用
45	インシデント対応	検知・封じ込め・復旧	監視・アラートを起点に、影響範囲の特定、封じ込め、復旧、原因分析、再発防止を実施する。
46	障害・事故通知	顧客への連絡	顧客影響のある障害・セキュリティ事象を対象顧客へ通知する。個別契約で通知条件・期限・方法を定めた場合はその条件に従う。
47	メンテナンス	計画変更・緊急変更	・計画メンテナンス：事前通知 ・緊急変更：安全性を優先し、事後通知となる場合あり
48	SLA・復旧目標	稼働率・RTO / RPO	稼働率保証、計画停止、RTO、RPOは個別契約で定める。
49	サポート	受付・連絡方法	契約時に案内する窓口への電子メール等で、本サービスの利用に関する問い合わせを受け付ける。カスタマイズの内容・費用・納期・保守対象は、合意した仕様書・個別契約に定める。
50	個人情報・法令対応	方針・公的要請	Elithのプライバシーポリシーおよび適用法令に従う。開示、訂正、削除、公的要請への対応手続を設ける。
51	文書の更新	仕様・契約変更時の扱い	本書は記載日現在の標準本番環境を対象とする。クラウド仕様、機能、契約条件の変更時に改定する。個別契約と異なる場合は個別契約を優先する。

改定履歴：第1.3版 / 2026年9月10日 / 正式ロゴに統一。回答内容の変更なし。
認証の公表情報：https://www.elith.ai/post/ismsaims ｜ https://www.jdla.org/news/20260804001/
本書とサービス仕様書は相互に参照してください。個別に合意した条件がある場合は、その合意に従います。