

日本の政府AI基盤「源内」とフランスの政府AI基盤「Albert API」詳細比較

エグゼクティブサマリー

調査基準日：2026年10月10日。本報告では、デジタル庁、内閣府、個人情報保護委員会、国家サイバー統括室、フランスDINUM、beta.gouv.fr、Albert API公式技術文書、EU・ANSSIの原典を優先した。なお、以下で「**未指定**」とする項目は、調査時点の公開された政府・公式技術資料から具体値または仕様を確認できなかったものを意味し、「機能が存在しない」と断定するものではない。

最も重要な結論は、「源内」と「Albert API」は同じレイヤーの製品ではないという点である。源内は、政府職員がブラウザから直接使う**職員向けAIワークスペース／AIアプリ基盤**を中核とし、チャット、翻訳、文書分析、RAG、行政専用AIアプリを一つの利用環境に集約している。一方Albert APIは、行政システムや開発チームが生成AIを組み込むための**共通モデル・ゲートウェイ／推論API基盤**が中心である。したがって、源内のフランス側の完全な対応物はAlbert API単体ではなく、その上のチャットUI等まで含む「Albert系サービス」であり、逆にAlbert APIの日本側の直接対応物は「源内Webそのもの」より、源内内部のモデルゲートウェイ／AIアプリ連携層に近い。¹

政策思想にも鮮明な差がある。日本は、人口減少・行政人材制約を背景に、政府自身がAIを「普段使い」して行政生産性を高め、同時に国産LLMの政府調達需要を形成することを強く意識している。2026年度には全府省庁約18万人が利用可能となる大規模実証を進めている。フランスは、各行政機関が外部AI APIや独自GPU基盤を個別調達することによる**情報漏えい、外国ベンダー依存、重複投資**を避け、DINUMが主権的な共通APIとしてモデル・GPU・RAGを集約することを明示的な目的としている。²

技術面では、**Albert APIの方が公開APIとしては標準化・可観測性・データ保持方針が明確**である。OpenAPI 3.1、OpenAI互換の `/v1/chat/completions`、Bearer認証、embeddings、rerank、search/RAG、OCR、音声認識等が公開され、推論内容を永続保存しない「zero-retention」に近い設計と、24か月保存する運用メタデータの境界まで技術文書に明記している。³

源内では、外部の行政特化AIアプリを接続する「源内AIアプリAPI仕様」が公開され、同期／非同期処理、`x-api-key`、ファイル転送等が定義されているが、これは**Albertのような汎用モデル推論APIそのものではない**。一般チャットから基盤モデルへ至る内部推論API、プロンプト／応答の保持期間、モデル事業者へのデータ伝達境界、数値SLAなどは公開資料では**未指定**である。⁴

一方、ソフトウェア供給網のセキュリティについては源内の公開情報が非常に具体的である。GitHub Advanced Security、secret scanning、Dependabot、GitHub Actionsのcommit SHA固定、依存パッケージのminimum release age、スクリプト実行抑止、内部セキュリティ技術者による脆弱性評価などが明示されている。Albertでは推論経路と運用アクセス制御の透明性が優れているが、SBOM、依存関係固定、パッチSLA等について同程度の詳細は公開資料から確認できず、**未指定**である。⁵

主要比較表

項目	日本「源内」	フランス「Albert API」	評価
基本性格	政府職員向けAIインターフェース＋行政AIアプリ実行基盤	行政システム向け共通AI API／モデルゲートウェイ	レイヤーが異なる 。単純な製品比較は不適切。 6
主体	デジタル庁。AI政策上は内閣府・AI戦略本部とも連動	DINUM、ALLiance	両者とも政府横断型。 7
政策目標	政府AI普及、行政効率・質向上、国産AI活用・政府需要形成	主権性、外部API依存・情報漏えい・重複GPU投資の削減	日本は「利用普及＋産業政策」、仏は「共通インフラ＋デジタル主権」がより強い。 8
主な利用者	2026年度に全府省庁約18万人を対象	国家公務員・行政デジタルサービス。70超の公共プロジェクト	源内は人間利用、Albertはアプリ/API利用を強く想定。 9
UI	Web UIが中核	APIが中核	源内優位。 10
公開API	行政特化AIアプリ連携用REST API	OpenAPI 3.1、OpenAI互換AI API	Albertが開発者向け標準化で優位。 11
認証	本番はGSSポータルSSO。OSSはCognito/SAML複数IdP。AIアプリAPIは <code>x-api-key</code>	ProConnectによる利用開始、APIはBearerトークン	目的に応じた方式。 12
ホスティング	本番はガバメントクラウド。公開記事はAWS構成を例示	Outscale SecNumCloud環境＋DGFIPのNubo	Albertは主権ホスティングをより明文化。 13
オンプレミス	未指定 。OSSは政府クラウド外の通常クラウドへの展開が可能	OpenGateLLMは自己環境へ展開可能、Ollama/vLLM等へ接続可能	Albert側の移植性が高い。 14
モデル	2026年5月資料ではNova Lite、Claude Haiku 4.5、Claude Sonnet 4.5/4.6。国産5モデルも試用	GPT-OSS-120B、Mistral/Ministral、Qwen Coder、Whisper、BGE、LightOn OCR等	源内は商用＋国産調達、Albertはopen-weight自前ホスト中心。 15
RAG	行政文書・マニュアル・政府共通データセットを利用する多数のRAGアプリ	<code>/v1/search</code> 等によるRAG、ベクトルストア	双方対応。ただしAlbertはAPIとして一般化。 16
学習/ Fine-tuning API	未指定 ／公開APIとして確認できず	公開サービスとして確認できず	基本的に両者とも「推論・RAG」が中心。
推論内容の保存	保持範囲・期間は 未指定 。ログ転送機能自体は公開	推論本文は永続化しない。RAGアップロード文書は別途永続化	Albertの方がデータライフサイクルを明確化。 17

項目	日本「源内」	フランス「Albert API」	評価
運用メタデータ	チャット、AIアプリ、呼出履歴、ユーザー関連ログ等を転送可能。保持期間は 未指定	時刻、APIキーID、モデル、tokens、HTTPコード、latency、IP等を24か月保存	Albertは監査境界が具体的。 ¹⁷
SLA	数値SLA 未指定	実験枠は保証なし。共同出資パートナーにはSLAあり。ただし数値は 未指定	Albertの契約階層が明確。 ¹⁸
課金	利用単価・課金体系 未指定 。2027年度以降、利用省庁が予算措置	国家公務員の実験利用は無料。高枠は限定本番・共同出資。共同出資額は 未指定	Albertの方が公開度が高い。 ¹⁹
OSS	源内Webの一部をMIT等で公開	OpenGateLLMをMITで公開	双方OSSだが、コミュニティ運営はAlbertの方が開放的。 ²⁰

目的・成立背景・政策的位置付け

日本・源内。 デジタル庁は2025年5月に源内を内製して庁内利用を開始した。背景には、人口減少・労働力不足下で行政サービスの質を維持・向上させる必要性と、各省庁が個別に生成AIを導入するのではなく、政府共通の安全なAI利用基盤を整える必要がある。2025年6月のデジタル社会重点計画では政府内AI開発・政府データ整備が位置付けられ、その後、2025年成立のAI法とAI基本計画により「政府自らAI利用を先導する」という政策が強化された。源内はその具体的実装の一つである。 ²¹

AI法は「人工知能関連技術の研究開発及び活用の推進に関する法律」（令和7年法律第53号）で、2025年6月4日に公布され、同年9月1日に全面施行された。AI戦略本部を置き、AI基本計画に基づいて政府横断の施策を進める枠組みである。最初の基本計画は2025年12月23日に閣議決定され、**現行の公開ページでは2026年7月14日閣議決定版が最新版**となっている。したがって、源内を「2025年12月計画だけにに基づく施策」と捉えるのではなく、現在は2026年版AI基本計画の下で評価する必要がある。 ²²

デジタル庁は2026年度、全府省庁約18万人を対象に大規模実証を行い、国産基盤モデル、政府共通データセット、高度行政AIアプリ、エージェントAIへ段階的に広げる計画を進めている。2025年度にはデジタル庁内約1,200人以上が利用し、2026年1月には19省庁で試験利用、5月から全府省庁規模へ拡大した。2027年度以降は各省庁による予算措置を伴う本格利用が想定されている。 ²³

国産AI政策との結び付きも強い。2026年にデジタル庁が源内で試用対象とした国産モデルには、NTTデータ「tsuzumi 2」、ソフトバンク「Sarashina3 mini」、NEC「cotomi v3」、富士通「Takane 32B」、Preferred Networks「PLaMo 2.0 Prime」が含まれる。行政現場からモデル提供企業へフィードバックし、政府調達によって安定需要を形成することまで政策目的に含まれており、これは単なる行政SaaS導入を超えた**産業政策的性格**を持つ。 ²⁴

フランス・Albert API。 beta.gouv.frが示す公式プロダクト履歴では、Albert APIは2024年6月1日に「construction」、2025年9月に「accélération」、2026年9月に「consolidation」へ移行している。開発・スポンサー主体はフランス政府のDINUM（Direction interministérielle du numérique）で、ALLiaNCEが担っている。 ²⁵

Albert APIの問題設定は非常に明示的である。フランス政府は、行政機関がChatGPTや外部AI APIを個別利用すると、機微情報漏えい、民間・国外事業者への技術依存が生じ、各行政サービスがGPU、モデル管理、ス

ケーリング機能を重複して構築すれば公共コストも膨らむと整理している。そこでDINUMが「主権的、安全、相互利用可能な共通生成AIインフラ」としてモデル推論、RAG、OCR等を集約するのがAlbert APIである。 25

現在、公式サイトはAlbert APIをDINUMの「interministerial reference API」と位置付け、70以上の公共プロジェクトで利用され、週10万件超のリクエストを処理しているとしている。これは日本の「18万人の利用可能職員」という指標とは母集団も単位も異なるため直接比較はできないが、Albertが既に単なる実験用APIから共有インフラへ進みつつあることを示す。 26

したがって政策的には、

源内 = 「政府全体のAI利用を日常業務まで浸透させる」ことを起点に、国産AI・政府データ・行政AIアプリへ拡張する政策基盤、

Albert API = 「政府共通の主権的AIバックエンドを持つ」ことで、行政サービスごとの外部ベンダー依存と重複投資を抑える共通インフラ

と整理するのが最も正確である。 27

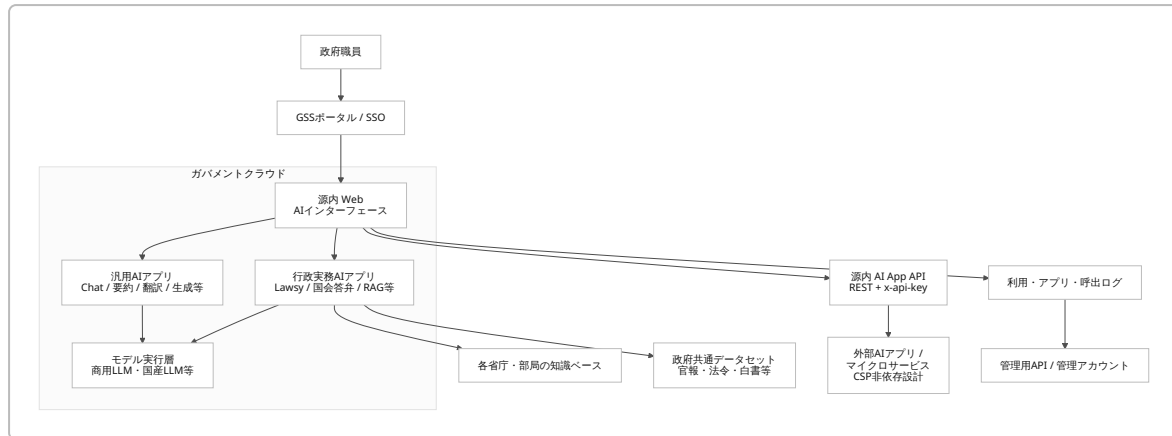
アーキテクチャと技術仕様

源内WebはAWSのOSS「Generative AI Use Cases (GenU)」を出発点としているが、チーム管理、AIアプリ管理、外部マイクロサービス型AIアプリ実行、デジタル庁デザインシステム、アクセシビリティ試験、監視・運用機能等を大幅追加しており、現在のコードはGenUとは独立して開発されていると説明される。本番の源内はガバメントクラウド上で稼働し、デジタル庁の技術記事ではAWS構成を例に、IAM利用制約、国内リージョン中心の利用、管理アカウントへのログ集約等を説明している。 28

一方、源内の「AIアプリAPI」は、外部マイクロサービスとして実装した行政特化AIアプリを源内Webから呼び出すための仕様である。JSONでtext、number、textarea、file、select、checkbox、radio、hidden等の入力を定義し、ファイルはBase64で渡せる。非同期処理ではPOST /requestsでrequest_idとstatus_urlを取得し、GET /status/{request_id}でPENDING、IN_PROGRESS、COMPLETED、ERRORを確認する。認証にはx-api-keyが用いられる。仕様書自体は2026年3月時点で「experimental」であり、変更され得ると明記されている。 4

重要なのは、このAPIをAlbert APIの/v1/chat/completionsと同一視しないことである。源内AIアプリAPIは「業務アプリを源内にプラグインするインターフェース」であり、任意の行政システムが共通LLMをOpenAI互換形式で直接呼び出すモデルゲートウェイ仕様ではない。公開資料上、源内内部の一般チャット用モデル推論APIの標準仕様は**未指定**である。 11

公開情報から再構成すると、源内の論理構成は次のようになる。下図は公開された構成図・技術文書を抽象化したものであり、非公開のネットワーク境界や内部モデルルーティングは推定していない。 29



認証は、本番環境ではGSSポータルからのSSOが基本であり、公開OSSはAmazon Cognitoを介した複数 SAML IdPをサポートし、Entra ID等との構成例も示されている。したがって、人間ユーザーにはフェデレーション認証、AIアプリ間接続にはAPIキーという二層構造である。RBAC／チーム権限に関する文書も公開されている。 30

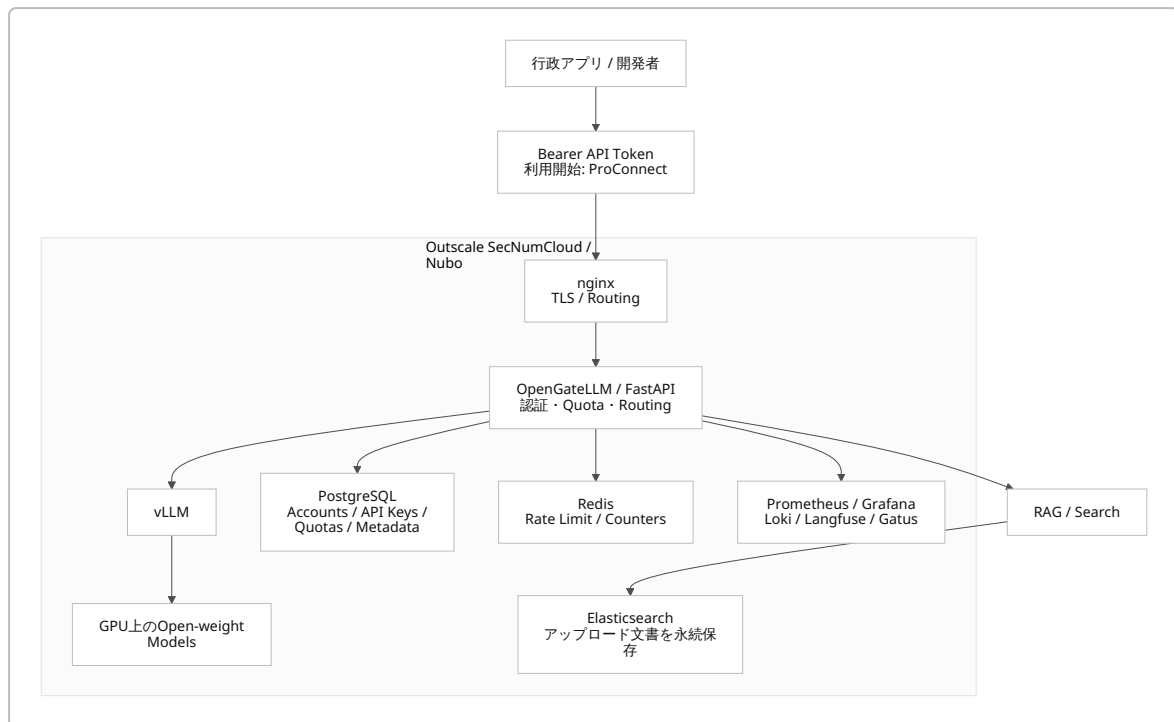
対応LLMについて、公開資料で具体名を確認できる基準日は注意が必要である。2026年5月29日付資料では通常チャットにAWS「Nova Lite」、Anthropic「Claude Haiku 4.5」「Claude Sonnet 4.5」「Claude Sonnet 4.6」が利用可能とされる。その後もモデル追加・更新予定とされているため、**2026年10月10日時点の全モデル一覧は未指定**と扱うのが厳密である。 31

また、Preferred NetworksのPLaMoを使う日英翻訳については、処理がガバメントクラウド内で完結し入力情報を外部送信しないことが個別に明記されている。しかし、この記述をClaudeやNovaを含む全源内アプリに一般化できる公開根拠は確認できないため、**一般チャット全体について「モデル事業者にデータが一切送られない」とは評価できない**。この点はAlbertとの重要な透明性差である。 24

Albert APIはより典型的なAPIゲートウェイ構成である。APIのベースは `albert.api.etalab.gouv.fr`、OpenAPI 3.1を採用し、OpenAI SDK等からbase URLとAPIキーを変更して利用できる。代表的なエンドポイントは `POST /v1/chat/completions`、`POST /v1/embeddings`、`/v1/rerank`、`/v1/search` 等で、テキスト生成、embeddings、分類／rerank、音声認識、OCR、RAGを提供する。API呼び出し時はHTTP `Authorization: Bearer ...` を使用し、国家公務員の利用開始にはProConnectが使われる。 32

2026年9月の変更履歴では、`/v1/chat/completions` 内部で直接使う旧 `search` toolを非推奨とし、明示的に `/v1/search` とchat completionを組み合わせる方式へ移行する方針が示されている。これはRAGの検索過程をアプリ側で制御しやすくする一方、Albert API/OpenGateLLMが依然活発に仕様進化していることを意味する。 33

中央サービスはOutscaleのSecNumCloud環境と、フランス財政総局DGFIPのNubo上で運用される。推論層はnginx、OpenGateLLM/FastAPI、vLLM等で構成され、PostgreSQLがアカウント・APIキー・quota・counter、Redisがセッション／rate limit counter、Prometheus/Grafanaが数値メトリクス、Lokiが本文を含まないアプリ／システムログを担う。RAGだけはElasticsearchに文書を永続保存する。 34



Albertで現在公開されているモデルには、`openai/gpt-oss-120b`、`mistralai/Mistral-Small-3.2-24B-Instruct-2506`、`mistralai/Ministral-3-8B-Instruct-2512`、`Qwen/Qwen3-Coder-30B-A3B-Instruct`、`openai/whisper-large-v3`、`BAAI/bge-m3`、`BAAI/bge-reranker-v2-m3`、`lightonai/LightOnOCR-2-1B` などがある。共同出資省庁にはMistral Medium 3.1やMistral OCR 3等のプロプライエタリモデルも提供される。これらopen-weightモデルはAlbert側のサーバーでホストされ、モデル供給元へ利用者データを送らないと明記されている。³⁵

さらにAlbertの基盤ソフトウェアOpenGateLLMは中央DINUMサービスとは別に自己環境へ展開でき、ローカルOllama/vLLMや、用途によってはOpenAI/Anthropic等の商用APIにも接続可能である。したがって、**中央Albert APIは主権的ローカル推論を重視する一方、OpenGateLLMというソフトウェア自体はマルチプロバイダー型**である。この二つを混同すべきではない。³⁶

機能・運用・エコシステム・性能

機能レイヤーでは源内の方が「完成した職員向け業務体験」の範囲が広い。2026年5月時点の公開資料には、チャット、文章生成、日英翻訳、一般多言語翻訳、画像生成、ダイアグラム生成、音声文字起こし、Excel関数提案、表データ分析、最大10万行のExcel処理、文書校正、複数ファイル横断分析、ALTテキスト作成などが並ぶ。行政特化領域では、法制度調査「Lawtsy」、国会答弁検索・分析、jGrants補助金調査、EASY・SEABIS等のRAG質問応答、行政文書用例検索などを提供または開発している。²⁴

Albert APIはより低レイヤーで、主力機能はテキスト推論、embeddings、rerank、OCR、音声認識、RAG/search、モデル選択、quota・project managementである。つまり源内は「何を仕事として完成させるか」までアプリ化するのに対し、Albertは「行政サービス開発者がその機能を組み合わせて仕事を実装する」構造になっている。³⁷

機能	源内	Albert API
汎用チャット	○、Web UI	○、API

機能	源内	Albert API
文書生成・要約・翻訳	○、完成アプリとして提供	○、LLM APIを通じて構築
画像生成	○	公開されたAlbert標準サービスでは 未指定
OCR	文書分析機能に含まれるが基盤API仕様は 未指定	○ 専用サービス
音声文字起こし	○	○ Whisper系モデル
Embeddings	内部利用は想定されるが公開汎用APIは 未指定	○ <code>/v1/embeddings</code>
Rerank	未指定	○
RAG	○ 多数の行政特化アプリ	○ <code>/v1/search</code> 等
行政業務専用アプリ	◎ 源内の中心的差別化要素	API上に各行政サービスが実装
モデルfine-tuning API	未指定	未指定／標準サービスで確認できず
モデル学習基盤	源内の構成図では基盤モデル学習は外側のモデル開発工程	提供対象外
チーム／利用者管理	○	○ APIキー・権限・quota
メタデータ／利用量管理	○ ダッシュボード・ログ	○ token/latency/status/IP等
非同期ジョブ	AI App APIで○	エンドポイントにより異なる／包括仕様は 未指定

出典：源内の機能はデジタル庁公開資料・OSS仕様、Albertは公式サービス/API文書による。 38

源内のログ機構では、一般AIログ、行政AIアプリログ、Use Case Builderログ、アプリ定義、呼出履歴、Cognitoユーザー情報等を日次収集し、IAM SigV4認証された任意のAPIエンドポイントへ転送する機能が公開されている。これは省庁横断運用の可視化には有用だが、ログ本文のデータ分類、保存年限、削除規則、法的保全処理等の統一仕様は公開文書では**未指定**である。 39

源内は複数省庁向け展開を「silo model」のマルチテナント方式で管理するテナント管理システムを採用していると説明されるが、テナント間隔離の詳細や暗号鍵分離、データベース分離レベル等は今後の公開事項とされており、現時点では**未指定**である。 40

Albertではメタデータ境界がかなり明確で、推論時のプロンプト、completion、embedding対象テキスト、ファイル等を永続ストレージに書き込まず、監視、セキュリティ、学習、guardrail等の目的にも本文を保存しない。一方、リクエスト時刻、APIキー／アカウントID、モデル、endpoint、input/output token数、HTTP status、latency、生成時間、送信元IP等は24か月保持され、quota、capacity planning、内部コスト配賦、rate limiting、セキュリティ等に利用される。 34

ここには重要なトレードオフがある。Albertの本文非保持はプライバシーと漏えい面で強いが、**中央DINUMが事後に「どのプロンプトが問題を起こしたか」を内容ベースで再現することはできない**。公式文書も、ア

アプリケーション単位のコンテンツ監査、abuse detection、moderation、必要な業務ログは呼出元アプリ／管理者の責任であると明記している。したがって、高リスク行政用途では、zero-retentionをそのまま採用するのではなく、目的制限された安全なアプリ側監査ログが別途必要になる。 41

エコシステムについて、源内は2026年4月から一部を商用利用可能なOSSとして公開し、8月にはOSS Ver.2.0を行政・産業界によるエコシステム形成の基盤とする説明会を開催した。リポジトリはMITライセンスを主体とするが、一部AWS由来コードにはAmazon Software Licenseが適用される。もっとも、公開リポジトリでは一般利用者のPR受付を限定し、Issueも重大問題中心としており、典型的なコミュニティ主導OSSというより「政府開発コードの公開」に近い運営である。 42

AlbertのOpenGateLLMもMITライセンスで公開されるが、公式リポジトリはcommunity contributionを明示的に呼び掛けている。OpenAI互換性によりLangChainやLlamaIndex等の既存ツールから移行しやすく、モデル提供者のAPI独自仕様を行政システムから隠蔽できる点はエコシステム上の大きな利点である。ただしOpenGateLLM自体は2026年時点でもBETA表示があり、breaking changeの可能性を明示している。 43

利用状況とスケール。 源内のデジタル庁内ダッシュボードでは2026年5月11日時点で、登録1,363人、利用1,280人、累計利用回数331,014回、登録アプリ43件が表示されている。これはデジタル庁内の値であり、18万人規模実証全体の利用統計ではない。 44

Albertは公式に70超の公共プロジェクト、週10万リクエスト超と公表している。ただし源内の「利用回数」とAlbertのHTTP「request」は定義が異なるので、331,014対100,000という数値を性能比較や普及率比較に用いることは不適切である。 26

SLA・性能・価格。 源内について、P50/P95 latency、tokens/sec、同時接続、数値SLA、RTO/RPO、ユーザー単価、token単価は公開資料ではすべて**未指定**である。2027年度以降、利用省庁が予算措置する方針は明示されている。 24

Albertの実験枠は国家公務員に無料で、低quotaかつ可用性保証なし、高需要時には制限され得る。「production limitée」はより大きなquotaを申請でき、共同出資パートナー省庁には全モデル、高quota、個別支援、可用性SLAが提供される。ただし**SLAの具体的な99.x%値と共同出資額は未指定**である。 18

例えばGPT-OSS-120Bについて、公開料金表では実験枠が10 requests/minute、1,000 requests/day、128k tokens/minute、1.28M tokens/day、限定本番枠が50 requests/minute、5,000 requests/day、246k tokens/minute等と明示されている。少なくとも容量計画の透明性ではAlbertが源内を上回る。 18

なお両プラットフォームとも、公開された共通ベンチマークによる**同条件のレイテンシ、スループット、行政タスク精度、hallucination率、RAG recall、コスト/正答率比較は確認できない**。したがって「どちらが性能上優れる」と数値的に断定する根拠は現時点ではない。

ガバナンス・法令順守・セキュリティ

日本では、源内そのもののガバナンスにAI法だけを当てはめれば足りるわけではない。AI法・AI基本計画は政府全体のAI推進と適正性確保の政策枠組みを与える一方、政府職員が個人情報を処理する場合は個人情報保護法と行政機関等向けガイドライン、情報システムとしては政府機関等のサイバーセキュリティ対策統一基準群等が引き続き適用される。個人情報保護委員会の行政機関等向けガイドラインは、行政機関、地方公共団体、独立行政法人等における個人情報の適正取扱いを法に基づく具体的指針として定めている。 45

デジタル庁は源内について、政府統一基準に適合させ、デジタル庁では**機密性2情報を入力可能**としている。GSSからのSSO、庁内専用アクセス、チーム権限等と組み合わせることで、一般向け生成AIサービスへ行政情報を直接投入するより管理された環境を構築する狙いがある。 46

2026年度の全省庁実証では各省庁にAI統括責任者、すなわちChief AI Officerの役割を明確化し、組織的な利用方針や普及を推進する構造が示されている。ただし、個々のAI回答に対する説明責任、モデルカード、データ来歴、プロンプトversion、モデルversionを一体管理する政府横断のAI監査台帳については、公開資料では**未指定**である。 24

フランスでは、Albert APIの個人データ処理はGDPRの枠組みと明示的に結び付けられている。DINUMの技術文書は推論サービスについてDINUMをGDPR第28条上の**processor (sous-traitant)**、利用する行政機関を**controller (responsable de traitement)**と整理する。モデル推論内容はDINUMによる再学習・fine-tuning・評価に再利用されない。 41

さらにEU AI Actはリスクベース規制を採用し、2026年8月2日からAI Officeと各国当局による主要な執行段階に入っている。ただし、Albert APIという汎用基盤を使うだけで全てのアプリが一律「high-risk AI system」になるわけではなく、**採用する行政用途・意思決定内容ごとにAI Act上の分類と義務を判断する必要がある**。 47

Albertのホスティングで特に重要なのがSecNumCloudである。ANSSIはSecNumCloudを、機微データ保護のための技術・運用・法的要件を持つ「trusted cloud」資格としている。一方ANSSI自身が、**SecNumCloud認定クラウド上で動くアプリケーションが自動的にSecNumCloud認定サービスになるわけではない**と注意している。このため「Albert APIはSecNumCloud認定済み」と単純表現するより、「AlbertはSecNumCloud適格クラウドであるOutscale上にホストされる」と表現する方が正確である。 48

セキュリティを要素別に見ると差はさらに明確になる。

脅威・統制	源内	Albert API
ID不正利用	GSS SSO、SAML/Cognito、チーム/RBAC。外部AIアプリはAPI key。 49	Bearer token、API key、quota。運用管理者アクセスは専用経路。 50
管理者侵害	ガバメントクラウドの権限管理。詳細privileged-access方式は 未指定	記名・追跡可能な管理者アクセスをbastion/暗号化tunnel経由、専用強化端末「Securix」から実施。 41
入力データ漏えい	機密性2まで利用可能。一般推論データの全保持・転送境界は 未指定	推論本文は永続保存せず、open-weightモデルは自前ホスト、外部モデル提供者へ本文を送らない。 51
RAGデータ	省庁KB・政府共通データセットを利用。保存年限等は 未指定	RAG文書はElasticsearchへ永続化するため、zero-retention対象外。 52
Rate limit/DDoS	数値rate limitは 未指定	Redis+quota、RPM/RPD/TPM/TPDを設定。 53
脆弱性検出	GitHub Advanced Security、secret scanning、Dependabot、内部脆弱性評価。 54	セキュリティ分析・homologation資料あり。ただしpatch SLA等は 未指定

脅威・統制	源内	Albert API
OSS supply chain	Actionsをcommit SHA固定、minimum release age、 <code>ignore-scripts</code> 等を導入。 ⁵⁴	OpenGateLLM/vLLM等OSS依存。SBOM・dependency pinningの公開統一要件は 未指定
Prompt injection	プラットフォーム共通の具体的防御仕様は 未指定	中央での本文moderationを原則行わず、呼出アプリ側の責任。 ⁴¹
監査	多種ログ・呼出履歴を外部管理基盤へ転送可能。保持年限は 未指定 。 ³⁹	本文以外の詳細メタデータを24か月保持。本文事後監査は呼出側で設計。 ⁴¹

源内のソフトウェア供給網対策は特筆に値する。GitHub Actionsの第三者Actionをタグではなく完全commit SHAで固定し、依存パッケージ公開直後の悪性バージョン取り込みを避けるminimum-release-age、インストールスクリプト抑止、Dependabot、secret scanning等を組み合わせている。生成AIコーディングツールを開発工程に利用しつつ、コードレビューや内部セキュリティレビューを残している点は、行政OSSのDevSecOpsとして比較的详细な公開例である。⁵⁴

Albertの強みは逆に**推論ランタイムの情報流通を細部まで公開していること**である。nginxはrequest bodyをログしない、OpenGateLLMは本文をメモリ上だけで扱う、vLLMのrequest loggingは無効、KV/prefix cacheはGPUメモリのみで永続化しない、Promtail/LokiやLangfuseもbusiness contentを保存しない、とコンポーネント単位で説明している。これはDPIAや監査を行う行政機関にとって大きな利点である。⁵⁵

ただしzero-retentionは万能な安全策ではない。プロンプトインジェクション、モデル出力による誤判断、有害なtool call、RAG poisoning、盗まれたAPI keyによる不正利用などは、本文を保存しないことでは防止できない。Albert側がコンテンツmoderationを呼出アプリへ委ねている以上、**中央基盤の安全性と行政業務アプリの安全性は別々に評価する必要がある**。これは源内でも同様で、行政RAG・エージェント化が進むほどアプリレイヤーの認可、tool permission、出力検証が重要になる。Albertについての前半はDINUM文書に基づき、後半はその構成からのリスク推論である。⁵⁶

利点・課題・リスク評価

両者を政策・技術の二軸で評価すると、源内の最大の強みは「**利用者にAIを使わせる最後の1マイル**」まで政府が共通化している点にある。ブラウザを開けばチャットだけでなく行政実務アプリが並び、GSS SSOと政府共通データを組み合わせるため、各省庁がAIエンジニアリング能力を持っていなくても利用を始められる。18万人規模に広げる政策は、モデル性能より組織変革を重視したアプローチである。⁵⁷

さらに源内を「インターフェース」「プラットフォーム」「メディア」と位置付け、政府共通アプリやアプリエコシステムを形成しようとしている点は、AI技術そのものより**再利用可能な行政業務部品**を蓄積する政策として評価できる。パブリックコメント分類のように、約8,000件規模の回答分析を従来約2か月から約3日に短縮した事例もあり、定型的な大量文章処理では具体的な効果が見え始めている。⁵⁸

一方、源内の主要な弱点は**基盤API・データライフサイクル・サービスレベルの対外透明性**である。公開OSSは充実してきたものの、一般LLM推論の内部API、各モデルへのルーティング、プロンプト・completionの保持条件、保存年限、モデルプロバイダー別データ境界、P95 latency、RTO/RPO、SLA、token原価等が公開されていない。このため、第三者がプラットフォーム全体を技術監査する際、Webアプリ層のコード透明性に比べて推論・運用層の透明性が弱い。⁵⁹

また、Claude等の外国商用モデルに依存しつつ、国産LLMを政府調達で育成する二重戦略は合理的である反面、**モデルの性能・コスト・主権性のどれを調達評価で優先するか**という難しい問題を生む。国産であること自体は安全性・品質を保証せず、逆に外国モデルであること自体も不適格を意味しない。行政タスク精

度、セキュリティ、総保有コスト、障害時代替性を同一ベンチマークで評価しなければ、産業政策が技術選定を歪めるリスクがある。源内が国産5モデルを行政実務で比較評価していることは、このリスクを緩和する方向の施策と評価できる。²⁴

Albertの最大の技術的強みは、**モデルと行政アプリの疎結合化**である。OpenAI互換APIの背後でモデルを差し替えれば、各行政システムはモデル企業ごとのAPIへ直接依存しなくてよい。OpenGateLLMを自己ホストできるため、中央DINUMサービス、各省庁独自インフラ、将来の別モデル間の移植性も高い。これは長期的な vendor lock-inの抑制に有効である。⁶⁰

もう一つの強みは、「**保存しないもの**」と「**保存するもの**」を明示したガバナンスである。推論本文を永続化せず、利用量・モデル・IP・latency等は24か月保存し、RAG文書は別扱いとする分離は、privacy by designと運用監査を両立させる明快な設計である。³⁴

ただしAlbertは源内ほど「一般職員がすぐ業務成果を出す」ための完成アプリを共通基盤自体には持たない。APIを導入する各行政チームに、prompt/RAG設計、UI、業務権限、出力検証、法的影響評価、コンテンツ監査を実装する能力が必要となる。このため技術人材の少ない行政組織では、Albert APIが存在するだけではAI普及につながらない可能性がある。DINUMが共通APIによって技術負担を下げているとはいえ、アプリ層の責任は依然利用側に残る。⁶¹

AlbertにはAPI安定性のリスクもある。OpenGateLLMがBETAでbreaking changeの可能性を明記し、2026年9月にもRAGの旧 `search` toolが非推奨化されている。政府共通基盤として利用範囲が広がるほど、versioning policy、long-term support、deprecation期間を民間クラウド並みに明示する必要性が高まる。⁶²

総合すると、評価は次のようになる。

評価軸	源内	Albert API	優位
一般職員がすぐ使えること	非常に強い	API単体では弱い	源内
行政特化アプリ	非常に強い	各アプリ側で実装	源内
標準API・開発者体験	中程度	非常に強い	Albert
モデル交換可能性	中～強	非常に強い	Albert
データ保持透明性	中程度／未指定項目あり	非常に強い	Albert
DevSecOps供給網対策の公開度	非常に強い	中程度	源内
主権ホスティングの明確さ	強化中	非常に強い	Albert
国産AI産業政策との連動	非常に強い	欧州・仏モデル活用はあるが目的は共通基盤寄り	源内
OSSコミュニティ参加性	コード公開中心	contribution型	Albert
全府省庁への利用普及設計	非常に強い	API普及中心	源内

評価軸	源内	Albert API	優位
数値SLA・性能透明性	弱い／未指定	中程度。quota公開、SLA数値は未指定	Albert
高リスク業務の本文監査	設計詳細未指定	中央は意図的に保持せずアプリ側責任	用途依存

したがって「どちらが優れているか」という問いへの最も妥当な答えは、**源内は上位のGovernment AI Workplaceとして優れ、Albertは下位のGovernment AI Infrastructure/APIとして優れている**、である。理想的な政府AI基盤は、この二つを競合モデルではなく、**Albert型の主権的・標準化されたAI gatewayの上**に、**源内型の職員UX・行政アプリ・共通データ基盤**を載せる多層構造にすることである。

推奨事項・結論・主要参照元

日本側への最優先提案は、「**源内WebのOSS化**」の次に「**政府共通AI Gateway仕様の公開**」を進めることである。Albert型のOpenAI互換APIを必ずコピーする必要はないが、モデル名、capability、context window、quota、version、deprecation policy、token使用量、推論latency、データ保持区分を共通スキーマで返す政府AI gatewayを設けるべきである。現在のAI App APIは行政アプリ連携には有効だが、モデル抽象化レイヤーとしては機能目的が異なる。¹¹

第二に、源内は**データライフサイクルをAlbert並みに機械可読・コンポーネント単位で公開**すべきである。「入力可能な情報は機密性2」という利用規則だけでなく、プロンプト、completion、添付ファイル、embedding、RAG文書、IP、利用者IDについて、どこを通り、誰がprocessor/subprocessorとなり、何日保存し、モデル改善に利用されるか否かをモデルごとに表形式で公表するとよい。Albertの「本文非保持／メタデータ24か月／RAGは別」という記述は有用なベンチマークとなる。⁵¹

第三に、**国産・外国モデルを同じ行政ベンチマークで継続評価**すべきである。法令調査、国会答弁、パブコメ分類、公用文、表処理等について、正確性、citation fidelity、hallucination、latency、単位コスト、消費GPU/電力、機密性条件を共通評価し、「国産だから採る」「最高性能だから採る」ではなく用途別routeを行うのが望ましい。源内には既に多数の行政特化タスクと国産5モデル実証があるため、評価データを蓄積する条件は整っている。²⁴

第四に、**AI監査台帳を標準装備**すべきである。モデルversion、system prompt version、参照データセットversion、tool permission、実行AIアプリversion、生成日時、利用者、重要な設定値を、本文そのものとは分離して監査メタデータとして保存すれば、個人情報最小化と説明責任を両立しやすい。現在のログ転送・呼出履歴基盤は、その実装母体になり得る。³⁹

第五に、エージェントAI導入に先立ち、**tool-level authorization、実行前承認、transaction limit、kill switch、prompt-injection評価**を政府共通要件にする必要がある。検索・要約のみのLLMと、行政システムに書き込みを行うagentではリスクが質的に異なる。源内が2026年度以降エージェントAI環境を検討している以上、UIの「便利さ」より先に権限境界を標準化すべきである。²³

フランス側への第一の提案は、Albert APIの上に「政府共通AI Workplace」をより強く標準化することである。Albertのgateway設計は優れているが、一般職員に対するAI普及では源内のような共通UI、行政特化アプリカタログ、利用研修、共通ワークフローが有効である。API基盤だけでは、AI能力の高い省庁と低い省庁の格差が残りやすい。これは両国の設計差から導かれる政策上の推論である。⁸

第二に、zero-retentionを維持しつつ、**高リスク用途向けの「privacy-preserving audit mode」**をオプション化することを推奨する。例えば暗号化された短期本文ログ、厳格な目的制限、アプリcontrollerだけが復号可能な方式などにより、AI Act対象となり得る重要行政判断でのincident reconstructionを可能にする余地が

ある。現行設計では本文の事後分析責任が呼出アプリ側に完全に移るため、小規模行政チームが監査設計を誤るリスクがある。 63

第三に、**SLAを数値化して公開**すべきである。共同出資パートナーには可用性保証があるものの、公開ページでは具体的なavailability percentage、P95 latency、support response time、RTO/RPOが確認できない。政府共通インフラとして基幹業務へ進むには、モデル別quotaだけでなくサービス品質指標が必要である。 18

第四に、OpenGateLLMについて、**SemVer、LTS release、deprecation最短期間、SBOM、CVE対応SLA**を公式化することが望ましい。2026年9月のAPI変更やBETA表示は急速な改善の裏返しだが、70以上の公共プロジェクトが依存する段階では「破壊的変更を許容するスタートアップ型開発」と「政府共通インフラの安定性」のバランスを変える必要がある。 64

第五に、SecNumCloudホスティングとアプリケーション自体の安全性を混同しないよう、**Albert自身のhomologation、脆弱性管理、penetration test、software supply chainの公開レベルを引き上げることが望ましい**。ANSSI自身が「SecNumCloud上で動くサービスが自動的にSecNumCloud認定になるわけではない」と明示している以上、インフラ資格の強さをアプリ層の保証へ読み替えない説明が重要である。 65

最終的には、両国が互いから学べる部分はかなり明確である。

日本がフランスから学ぶべきものは、OpenAI互換共通gateway、open-weightモデルの主権ホスティング、本文非保持を含む詳細なデータフロー公開、quota/API仕様の透明性である。

フランスが日本から学ぶべきものは、一般職員の業務画面まで含む導入設計、行政特化アプリの中央再利用、研修と組織変革、国全体を一齐に実証へ巻き込む普及戦略である。これらを統合した「**主権的AI gateway → 共通データ/RAG → 行政AIアプリ → 職員向けWorkplace**」の四層構造が、両者の長所を最も合理的に統合する将来像と考えられる。 66

主要参照元URL（原典中心）

資料	URL
デジタル庁「ガバメントAI『源内』」	https://www.digital.go.jp/policies/genai
デジタル庁「源内 Web 開発概要」	https://digital-gov.note.jp/n/n3ef31ec45995
源内Web OSS	https://github.com/digital-go-jp/genai-web
源内AIアプリAPI仕様	https://github.com/digital-go-jp/genai-web/blob/main/docs/AIアプリAPI仕様.md
デジタル庁「ガバメントAI源内の展開状況」	https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/fc155eba-e83d-4ecf-9c6a-a3c855e2e7b3/d0d53b25/20260528_news_genai_outline_01.pdf
内閣府「AI法」	https://www8.cao.go.jp/cstp/ai/ai_act/ai_act.html
e-Gov「人工知能関連技術の研究開発及び活用の推進に関する法律」	https://laws.e-gov.jp/law/507AC0000000053
内閣府「人工知能基本計画」	https://www8.cao.go.jp/cstp/ai/ai_plan/ai_plan.html

資料	URL
個人情報保護委員会 行政機関等向けガイドライン	https://www.ppc.go.jp/personalinfo/legal/guidelines_administrative/
政府機関等のサイバーセキュリティ統一基準群	https://www.cyber.go.jp/policy/group/general/kijun.html
DINUM Albert API	https://ia.numerique.gouv.fr/outils-ia/albert-api/
Albert API モデル	https://ia.numerique.gouv.fr/outils-ia/albert-api/modèles/
Albert API 料金・上限	https://ia.numerique.gouv.fr/outils-ia/albert-api/tarifs-et-limites/
Albert API サービス一覧	https://ia.numerique.gouv.fr/outils-ia/albert-api/offre-de-services/
Albert API セキュアインフラ	https://ia.numerique.gouv.fr/outils-ia/albert-api/infrastructure-sécurisée/
Albert API 展開／自己ホスト	https://ia.numerique.gouv.fr/outils-ia/albert-api/déploiement/
Albert API 開発者ガイド	https://guides.ia.numerique.gouv.fr/albert-api
beta.gouv.fr Albert API	https://beta.gouv.fr/startups/albert-api.html
OpenGateLLM	https://github.com/etalab-ia/OpenGateLLM
Albert「推論経路における業務データ非保持」技術文書	https://github.com/betagouv/doc.albert-api/blob/main/ressources/absence-de-retention-des-donnees-metier-sur-le-chemin-dinference.md
EU AI Act / EUR-Lex	https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32024R1689
欧州委員会 AI Act実施情報	https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
ANSSI SecNumCloud解説	https://cyber.sites.beta.gouv.fr/enjeux-technologiques/cloud/

公開資料から見る限り、源内は「行政職員のAI利用基盤」として世界的にも野心的な大規模展開である一方、Albert APIは「政府共通AIバックエンド」としてデータフロー・API・主権性の設計公開が一段成熟している。両者の次の競争軸は、単なるモデル性能ではなく、監査可能性、データ境界、API安定性、エージェント権限管理、行政タスク単位の費用対効果をどこまで公開し、政府横断の共通標準にできるかに移っている。

1 7 9 27 57 66 ガバメントAI「源内」

https://www.digital.go.jp/policies/genai?utm_source=chatgpt.com

2 12 21 30 46 49 51 58 ガバメントAI「源内」 | デジタル庁

<https://www.digital.go.jp/policies/genai>

- 3 32 50 guides.ia.numerique.gouv.fr
<https://guides.ia.numerique.gouv.fr/albert-api>
- 4 11 genai-web/docs/AIアプリAPI仕様.md at main · digital-go-jp/genai-web · GitHub
<https://github.com/digital-go-jp/genai-web/blob/main/docs/AI%E3%82%A2%E3%83%97%E3%83%AA%E4%BB%95%E6%A7%98.md>
- 5 10 13 14 28 40 54 源内 Web 開発概要 | デジタル庁
<https://digital-gov.note.jp/n/n3ef31ec45995>
- 6 digital-go-jp/genai-web: 源内Web (AIインターフェース)
https://github.com/digital-go-jp/genai-web?utm_source=chatgpt.com
- 8 15 16 19 23 24 29 31 38 44 52 (参考資料) ガバメントAI源内の展開状況
https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/fc155eba-e83d-4ecf-9c6a-a3c855e2e7b3/d0d53b25/20260528_news_genai_outline_01.pdf
- 17 39 genai-web/docs/ログ設定.md at main · digital-go-jp/genai-web · GitHub
<https://github.com/digital-go-jp/genai-web/blob/main/docs/%E3%83%AD%E3%82%B0%E8%A8%AD%E5%AE%9A.md>
- 18 Tarifs et limites — IA dans l'État
<https://ia.numerique.gouv.fr/outils-ia/albert-api/tarifs-et-limites/>
- 20 59 GitHub - digital-go-jp/genai-web: 源内Web (AIインターフェース) · GitHub
<https://github.com/digital-go-jp/genai-web>
- 22 人工知能基本計画 - 科学技術・イノベーション
https://www8.cao.go.jp/cstp/ai/ai_plan/ai_plan.html?utm_source=chatgpt.com
- 25 61 Albert API — beta.gouv.fr
<https://beta.gouv.fr/startups/albert-api.html>
- 26 43 60 Albert API — IA dans l'État
<https://ia.numerique.gouv.fr/outils-ia/albert-api/>
- 33 Changelog | Documentation Albert API
https://guides.ia.numerique.gouv.fr/albert-api/ressources/changelog?utm_source=chatgpt.com
- 34 41 53 55 56 63 doc.albert-api/ressources/absence-de-retention-des-donnees-metier-sur-le-chemin-dinference.md at main · betagouv/doc.albert-api · GitHub
<https://github.com/betagouv/doc.albert-api/blob/main/ressources/absence-de-retention-des-donnees-metier-sur-le-chemin-dinference.md>
- 35 Modèles — IA dans l'État
<https://ia.numerique.gouv.fr/outils-ia/albert-api/mod%C3%A8les/>
- 36 Déploiement — IA dans l'État
<https://ia.numerique.gouv.fr/outils-ia/albert-api/d%C3%A9ploiement/>
- 37 Offre de services — IA dans l'État
<https://ia.numerique.gouv.fr/outils-ia/albert-api/offre-de-services/>
- 42 【終了】「ガバメントAI 源内OSS Ver 2.0の計画に関する ...
https://www.digital.go.jp/news/b6d94913-60d0-450d-ab46-8e89659f1fc6?utm_source=chatgpt.com
- 45 人工知能関連技術の研究開発及び活用の推進に関する法律 ...
https://www8.cao.go.jp/cstp/ai/ai_act/ai_act.html?utm_source=chatgpt.com

47 **European approach to artificial intelligence**

https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence?utm_source=chatgpt.com

48 **Cloud**

https://cyber.sites.beta.gouv.fr/enjeux-technologiques/cloud/?utm_source=chatgpt.com

62 64 **GitHub - etalab-ia/OpenGateLLM: An open-source, unified interface for running and managing self-hosted LLMs. · GitHub**

<https://github.com/etalab-ia/OpenGateLLM>

65 **FAQ avant de se lancer dans la qualification SecNumCloud**

https://cyber.sites.beta.gouv.fr/enjeux-technologiques/cloud/faq-qualification-secnumcloud/?utm_source=chatgpt.com