

Perplexity「Portable Computer for Windows」徹底調査：ローカルAIエージェントの実態、導入要件、セキュリティ、ライセンス、競合比較

エグゼクティブサマリ

Perplexityは**2026年9月14日**、ローカルファーストAIエージェント「Portable Computer」をWindows PCへ正式展開した。これは、同社が2026年8月25日にNVIDIA DGX Spark/Linux向けとして発表したPortable Computerを、既存のPerplexity Windowsアプリから利用可能にしたものだ。Windows版は**NVIDIA GeForce RTXまたはRTX PRO GPUでVRAM 24GB以上**を要求し、個人向けPro/MaxとEnterprise Pro/Maxの利用者に提供される。Portable Computer自体の製品バージョン番号、Windowsアプリの対応ビルド番号、最低Windowsビルド、最低RAM/CPU/ストレージ容量は、2026年9月15日時点の公開資料では**未特定**である。

1

最大の特徴は、「ローカルLLMを動かせる」というだけではない。Perplexity Computerの**オーケストレーター、ローカルモデル、ツールルーター、スケジューラ、永続タスクキュー、ローカル検索インデックス、ファイル操作ツール群**までPC側で動かし、ローカルで完結する作業についてはComputerクレジットを消費しない。必要なときだけ、ユーザーの承認を得てWeb検索、Perplexityクラウド、接続済みSaaS、15種類以上のフロンティアモデルへエスケーションする「local-first / hybrid」方式である。

2

ただし、「ローカル」＝「常時完全オフライン」「エアギャップ対応」ではない。Perplexityの研究資料ではWeb検索を完全に無効化してローカルワークフローを実行できると説明されている一方、Windows版の初回モデル取得、サインイン、契約確認、アップデート、ライセンス検証、テレメトリ等まで含めて完全にネットワークを切断できるという保証は公開されていない。したがって「処理内容をローカルに閉じること」と「製品全体をエアギャップ環境で運用できること」は分けて評価すべきである。

3

セキュリティ設計は競合する多くのOSSエージェントより強い。ツール実行はOSレベルのサンドボックス内で行われ、プロセス、ファイルシステムパス、ネットワークをポリシーで制約する。サンドボックスが利用できなければ非隔離モードにフォールバックせず、ツール呼び出し前に停止する**fail-closed**設計である。NVIDIAはWindows版についてPerplexity独自の「SPACE sandbox」を内蔵すると説明している。

4

一方、Portable Computerが「安全な自律エージェント」であることを意味するわけではない。Perplexity自身のEnterprise Agentic Specific Termsは、Computer等のエージェントが**プロンプトインジェクション等のセキュリティ攻撃を受け得る**ことを明記し、ユーザー側にアクセス権管理、監督、承認の責任を課している。したがって本番環境ではサンドボックスを理由に無監督のメール送信、ファイル更新、コード実行、SaaS書き込みを許可すべきではない。

5

ライセンス面では特に注意が必要である。一般消費者向けPerplexity利用規約は、サービス利用権を「**個人の非営利目的**」に限定し、営利目的での悪用を禁止している。対してEnterprise規約は明示的に「顧客の事業目的」の利用を許可する。そのため、会社の本番業務にPortable Computerを組み込むなら、個人Pro/Maxではなく**Enterprise Pro/Maxを基本線とするのが法務上安全**である。

6

2026年9月15日はWindows版公開の翌日であり、Windows固有の長期的な障害報告、脆弱性実績、GitHub Issues、Stack Overflow上の知見はまだほぼ形成されていない。したがって現時点では「成熟したWindows

エンタープライズ製品」と評価するより、強い技術設計を持つが、Windows実装の運用実績・公開仕様・SBOM・依存関係・モデル更新手順が不足している初期リリースとして扱うのが妥当である。 7

結論

評価軸	判断
ローカル性	高い。モデルだけでなくエージェント・ハーネス、検索索引、ツール実行までローカル
完全オフライン	タスク単位では可能。製品全体のエアギャップ保証は未確認
プライバシー	クラウド型Computerより有利。ただしクラウド・コネクタを許可すると送信が発生
セキュリティ	常時サンドボックス＋fail-closedは強み。ただしprompt injection等のエージェント固有リスクは残る
Windowsハードウェア	NVIDIA RTX / RTX PRO、VRAM 24GB以上
Windows OS要件	未特定
RAM/SSD最低要件	未特定
モデル	Qwen 3.8 27B、PPLX 27Bが公式発表済み。Windowsでの全モデル一覧・各版は未特定
CLI	Portable Computer専用のユーザー向け公開CLIは未確認
更新方式	Windowsアプリ経由とみられるが、モデル/ランタイム個別更新仕様は未特定
商用利用	個人版規約には非営利制限あり。企業利用はEnterprise推奨
本番導入判断	PoCは推奨可能。本番はネットワーク、権限、コネクタ、アップデートを管理した段階導入が必要

公式発表、製品定義、公開バージョン

発表の時系列

PerplexityによるPortable Computerの初回発表は2026年8月25日だった。当初はNVIDIA DGX Sparkと対応Linux/RTX環境が対象で、Windowsは「coming soon」とされていた。ローカルでComputerを動かし、必要に応じてユーザー承認付きでクラウドへエスケーションする構造、Qwen 3.8 27B / PPLX 27B、ローカルツール、サンドボックス等はこの時点で公表された。 8

続いて2026年9月1日、PerplexityはMac向けHybrid Computeと、デバイスからデータを外へ送る前にPIIを検出する研究「PII-TRACE」を公表した。これはWindows Portable Computerそのもののリリースではないが、Perplexityがローカル・クラウド間の境界をどう設計しているかを理解するうえで重要な一次資料である。 9

そして2026年9月14日、「Portable Computer for Windows is here」が公式ブログに掲載された。Perplexityブログのインデックスにも同日付で掲載され、「機密性の高い作業をローカルに保ち、定期タスクや長時間のワークフローをクレジットなしで実行する」と説明されている。NVIDIAも同日に、Perplexity Windowsアプリ上でGeForce RTX / RTX PRO搭載PCへ提供開始したことを発表した。 10

なお翌**2026年9月15日**には、Perplexity WindowsアプリのHP PCへのプリロード拡大も公式ブログに掲載されており、WindowsをPerplexityの主要クライアントプラットフォームにする動きが続いている。 ¹¹

公式資料一覧とバージョンの確認状況

資料	公開日	確認できる版・状態	主な内容
Introducing Portable Computer for local-first AI	2026-08-25	Portable Computer 初版。製品版番号は 未特定	DGX Spark/Linux、local-first、Qwen/PPLXモデル、クラウドエスケーレーション
A local-first agent for private and cost-effective knowledge work	2026-08-25	研究/アーキテクチャ資料	ハーネス、サンドボックス、コネクタ、ベンチマーク
PII-TRACE	2026-09-01	PII-Tracer 0.6B研究モデル	ローカルPII検出、13言語評価
Portable Computer for Windows is here	2026-09-14	Windows版正式公開。製品版番号は 未特定	既存Windowsアプリから利用、Pro/Max、RTX
NVIDIA Windows発表	2026-09-14	Windows対応	RTX/RTX PRO、24GB以上VRAM、SPACE sandbox
Perplexity Windowsアプリ	継続更新	対応ビルド番号未特定	Portable Computerのフロントエンド
Portable Computer固有FAQ	—	独立したFAQは確認できず	一般Help Center、ブログ、研究記事が主な仕様情報源
Portable Computer固有公開GitHub	—	確認できず	クローズドなPerplexity製品として配布

Windows版は**ProおよびMaxの個人・Enterpriseプラン双方**に提供されるとPerplexity公式検索結果に明記されている。 ¹²

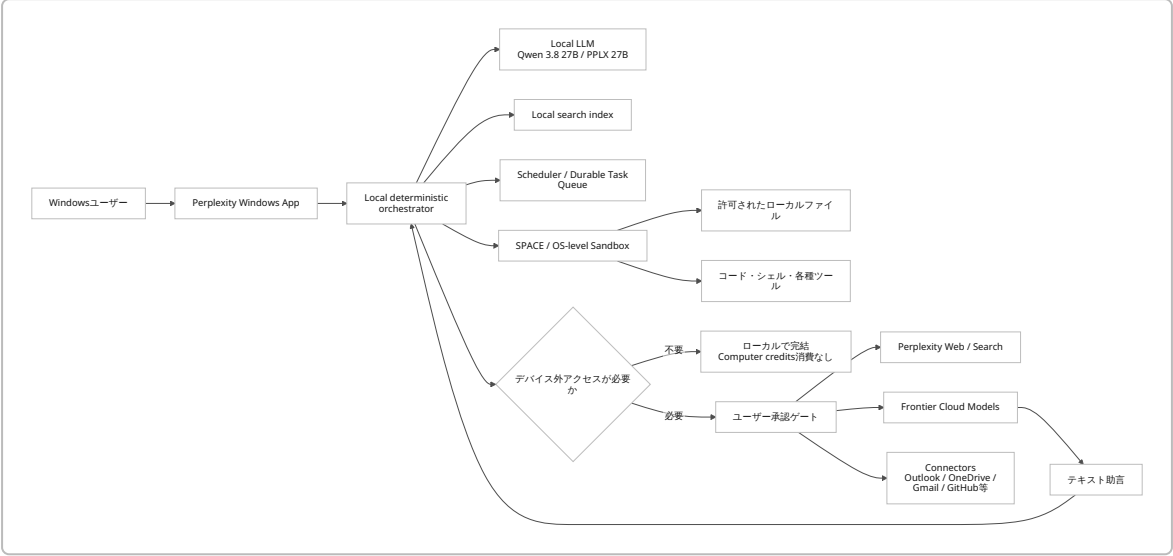
「ローカル」の正確な意味

Portable Computerにおける「local」は、単にLLMの重みだけをローカルに置くという意味ではない。Perplexityの説明では、少なくとも以下がPC内で動く。 ³

- ローカルLLM
- Computerのエージェント・ハーネス
- deterministic orchestrator
- planner / tool routing
- スケジューラ
- durable task queue
- ローカル検索インデックス
- ローカルファイル検索・読取・書込
- コード・シェル等のツール
- sandboxでのツール実行
- 長時間・定期タスク

ここで重要なのが**deterministic orchestrator**である。Perplexityの設計では、LLM自身がOS権限を直接保持するのではなく、決定論的なオーケストレーターがポリシーと権限を保持し、ローカルモデルが「次に何をしたいか」を提案し、承認されたツールだけがサンドボックスで実行される。これは、エージェントにそのままユーザー権限を与える構成との差が大きい。 13

概念的には次の構造になる。



クラウドの「advisor」へエスカレーションする場合でも、Perplexityの研究アーキテクチャではツール権限をローカルオーケストレーターが保持し、承認されたコンテキストだけをリモートモデルへ送り、リモートモデルはファイルやツールへ直接アクセスせずテキストによる助言を返す構造である。 14

モデルと依存ライブラリ

初回発表で確認できる主なモデルは**Qwen 3.8 27B**とPerplexityが事後学習した**PPLX 27B**である。NVIDIA Nemotron 3.5 Lightning 30Bについては8月25日時点で「model pickerに追加予定」とされたが、9月15日時点のWindows公開資料からはWindows環境での正式提供状態を再確認できなかったため、本レポートでは**Windows提供状況未特定**とする。 15

Perplexityの研究ではQwen 3.8 27Bの公称コンテキストウィンドウを260Kとしつつ、実際のエージェント軌跡では**100Kトークンを超えると性能が低下し始めると報告**しており、このためオンデマンド・スキルとコンテキスト圧縮を採用している。 16

NVIDIAはIFA 2026で、Perplexity Portable Computer、Hermes Agent、OpenClawなどの次世代ローカルエージェント群について、**llama.cppをベースとしNVIDIA推論最適化を組み込んでいる**と説明した。ただしPerplexityはWindows版について、llama.cppの正確なバージョン、CUDA/cuBLAS等の同梱バージョン、量子化形式を公開していない。したがって「llama.cpp系の統合ランタイム」と見ることはできるが、個別依存パッケージ一覧は**未特定**である。 17

次の情報も2026年9月15日時点では公開資料から特定できなかった。

項目	状況
モデルファイルのWindows上の保存パス	未特定

項目	状況
モデル量子化方式	未特定
モデルファイル容量	未特定
モデルSHA-256等の公式チェックサム	未特定
llama.cpp正確なバージョン	未特定
CUDA Runtime最低バージョン	未特定
NVIDIAドライバ最低バージョン	未特定
Portable Computer設定ファイルの公開スキーマ	未特定
Portable専用CLI	確認できず
Portable専用SDK/GitHubリポジトリ	確認できず

Perplexityの研究資料に出てくる「CLI tools」は、Gmail、GitHub、Outlook、Google Calendar等のMCPツール定義を圧縮するために**エージェント内部で利用されるコマンドラインツール**であり、ユーザー向けPortable Computer CLIが提供されているという意味ではない。¹⁶

Windows版の機能、要件、インストール

Windowsで確認されている機能

Windows版Portable Computerは、NVIDIAの発表ではPerplexity Windowsアプリに統合され、**GeForce RTX PCおよびRTX PRO Workstation**で利用できる。ローカルモデルによる文書分析、ファイル操作、長時間ワークフロー、スケジュール実行に加え、必要に応じてクラウド機能やコネクタを利用できる。¹⁸

Windows版のコネクタとしてNVIDIAが明示しているのは、**Microsoft Outlook、OneDrive、Word、Google Drive、Gmail、Slack、GitHub**である。接続したサービスへ書き込み操作を行う場合には、ローカル処理とは異なり当然ながらネットワーク通信と当該サービスへのデータ送信が発生する。¹⁹

音声について、初回Portable Computer発表ではNVIDIA Nemotron 3.5 ASRによるローカル音声認識を説明し、音声、文字起こし、ファイル上の操作をデバイス内に保持できるとしている。Windows版で利用可能な音声機能の完全な対応表・バージョンは公開資料では未特定である。²⁰

ハードウェア要件

Windows版で公式に確認できる決定的な要件は以下である。

要件	Windows Portable Computer
GPUベンダー	NVIDIA
GPU系列	GeForce RTX / RTX PRO
VRAM	24GB以上
AMD GPU	公式対応を確認できず
Intel GPU	公式対応を確認できず

要件	Windows Portable Computer
CPU	最低要件 未特定
システムRAM	最低要件 未特定
SSD空き容量	最低要件 未特定
Windows版	最低ビルド 未特定
NVIDIA Driver	最低版 未特定
CUDA Toolkit手動導入	公式手順では要求を確認できず
Python/Node.js	Portable Computer利用者向けの明示的要求なし

VRAM 24GB以上という条件はPerplexity/NVIDIA双方のWindows発表で確認されており、現時点で最大の導入障壁である。 ²¹

初回Linux版で使われたDGX SparkはGB10、20コアArm CPU、128GB統合メモリを持つが、これは**Windows PCの最低要件ではない**。Windows版に対して128GB RAMが必須と解釈してはいけない。 ²⁰

プラン要件と価格

Portable Computer for WindowsはPro/Maxの個人・Enterpriseプランで提供される。現行のPerplexity公式Help Centerによる料金は次の通りである。 ²²

プラン	現行公表価格	Portable Windows
Standard	\$0	対象として明記されず
Pro	\$20/月、\$200/年	○
Max	\$200/月、\$2,000/年	○
Enterprise Pro	\$40/月/seat、\$400/年/seat	○
Enterprise Max	\$325/月/seat、\$3,250/年/seat	○

ローカルで完結したPortable Computer処理はComputerクレジットを使わない。一方、クラウド機能にエスカレーションした処理は別であり、Perplexityの通常のComputerクレジット体系が関係する。2026年9月7日現在、Max個人プランは月10,000 credits、Enterprise Proは月500、Enterprise Maxは月15,000を基本割当としている。 ²³

推奨するインストール手順

公式資料で確認できるWindows版の基本導線は、**既存Perplexity WindowsアプリからPortable Computerをセットアップする「one-click」方式**である。Portable Computer用にPython環境を作成したりGitHubリポジトリをcloneしたりする手順は公開されていない。 ²⁴

実務では以下の順に導入するのが安全である。

事前確認。 まずNVIDIA GPUとVRAMを確認する。

```
# GPU、VRAM、ドライバの確認
nvidia-smi --query-gpu=name,memory.total,driver_version `
--format=csv,noheader

# Windows情報
Get-ComputerInfo |
    Select-Object WindowsProductName, WindowsVersion, OsBuildNumber

# RAM
Get-CimInstance Win32_ComputerSystem |
    Select-Object @{N="RAM_GB";E={[math]::Round($_.TotalPhysicalMemory / 1GB,1)}}

# ドライブ空き容量
Get-Volume |
    Where-Object DriveLetter |
    Select-Object DriveLetter,
        @{N="SizeGB";E={[math]::Round($_.Size/1GB,1)}},
        @{N="FreeGB";E={[math]::Round($_.SizeRemaining/1GB,1)}}
```

`memory.total` が24GB未満なら、現行のWindows Portable Computerの公式要件を満たさない。 19

次にPerplexity Pro/MaxまたはEnterprise Pro/Maxへ加入し、公式Windowsアプリをインストールする。企業の機密データを扱う場合は、後述する利用規約上の理由からEnterpriseアカウントを優先すべきである。

25

その後Windowsアプリにサインインし、Portable Computer / Computerのローカルセットアップを実行する。Perplexityはこのモデル・ランタイムの準備を「one-click setup」と表現しており、NVIDIAも複雑なローカル推論スタックをアプリ側で隠蔽する方式と説明している。 15

モデル取得後、まず**Web検索、クラウドadvisor、コネクタを使わないローカル限定のテストタスク**を実行する。その後に必要なコネクタだけを1個ずつ許可する運用が望ましい。Perplexityの設計上、Web検索は完全に無効化してローカルだけで作業させることが可能である。 26

オフライン性を自分で検証する方法

「ローカル」の実態を確認したい企業では、機密データ投入前にネットワーク接続を観測することを推奨する。

```
# 現在のEstablished TCP接続とPID
Get-NetTCPConnection -State Established |
    Sort-Object OwningProcess |
    Select-Object LocalAddress, LocalPort,
        RemoteAddress, RemotePort,
        OwningProcess

# PIDからプロセス確認
Get-Process |
```

```
Select-Object Id, ProcessName, Path |  
Sort-Object Id
```

完全ローカル検証では、ダミーファイルだけを使い、Web・Connectors・クラウドエスケーションを利用しない状態で通信有無を観測する。**Portable Computerがローカル処理を行うことと、Perplexity Windowsアプリ全体が通信ゼロであることは別問題**なので、アプリの更新チェック、認証、テレメトリ等も含めて確認する必要がある。Windows版に関するテレメトリの完全なフィールド一覧は公開資料では未特定である。 ²⁷

更新方法

Portable Computerは独立したGitHubバイナリではなくPerplexity Windowsアプリ内に組み込まれているため、少なくともアプリ本体はWindowsアプリの配布経路で更新される。ただし、**ローカルモデルの更新、ランタイム更新、モデルロールバック、モデル固定、チェックサム検証、LTSチャンネル**についてのPortable Computer固有の公開手順は確認できなかった。したがって企業運用では、自動更新前提とせず、アプリ更新の前後でモデル名、モデル容量、ネットワーク挙動、コネクタ権限を再検証すべきである。 ²⁸

セキュリティ、プライバシー、脅威分析

サンドボックス

Portable Computerの最も重要なセキュリティ上の差別化要素がツール隔離である。Perplexityの研究によればツールは**OSレベルのsandbox**内で実行され、プロセス、ファイルシステムパス、ネットワークアクセスをポリシーによって制限する。sandboxが利用できない場合はツールを直接ホストOS上で実行せず、ハーネス自体がツール呼び出し前に無効化される。 ¹⁶

Perplexityはこの分離を「常に有効」で「設定不要」とし、隔離なしではComputerがツールを実行できないと説明している。NVIDIAのWindows発表は、このWindows側の隔離機構をPerplexity独自の**SPACE sandbox**として説明している。 ⁴

これはOpenClawのように、デフォルトのmain sessionではホスト上で直接ツールを実行し、sandboxを必要に応じて設定する設計とは明確に異なる。OpenClaw自身の公式GitHubも「tools run on the host ... unless you configure sandboxing」と注意している。 ²⁹

クラウド送信境界

Portable Computerでは、ローカルモデルが高度な調査・推論等を必要と判断すると、Webやクラウドモデルを使うことができる。その際Perplexity/NVIDIAはいずれも**デバイス外へ情報を送る前にユーザー承認を求めると説明している**。 ¹⁵

主なデータ経路は次のように整理できる。

操作	データ送信	主な宛先
ローカルモデル推論	原則なし	PC内
ローカルファイル検索	原則なし	PC内
ローカルコード/ツール	sandboxのポリシー次第	PC内
Perplexity Web Search	あり	Perplexity/Web

操作	データ送信	主な宛先
Cloud Advisor	承認後あり	Perplexity経由のフロンティアモデル
Outlook/OneDrive/Word	あり	Microsoftサービス
Gmail/Google Drive	あり	Google
Slack	あり	Slack
GitHub Connector	あり	GitHub
更新/認証/テレメトリ	詳細未特定	Perplexity等

Cloud Advisorの研究設計では、クラウドモデルに直接ファイル操作権限やツール権限を与えず、承認されたコンテキストを送り、返ってきたテキスト助言をローカルモデルが利用する。この分離は、クラウドモデルをそのままPCのOSエージェントにする方式より攻撃面を小さくできる。 ¹⁴

PII保護は有用だが「絶対」ではない

Perplexityは9月1日のPII-TRACE研究で、デバイス外へデータを送る前にPIIをローカル検出し、ローカル処理、編集、ユーザー承認などにルーティングする設計を公開した。PII-TracerはQwen3系の0.6B双方向エンコーダで、最大4,096トークン、13言語、13,148件の合成会話、37,431件の識別子言及を使って評価されている。 ³⁰

しかし、公開された結果そのものが「PII検知＝漏洩防止保証」ではないことを示している。PII-Tracerのcharacter F1は0.629で、反復された識別子の全出現を捕捉できた割合は79.4%、ターンをまたぐ場合は77.6%だった。したがってPII検知を唯一のDLP層として扱うべきではない。 ³⁰

さらに、9月15日時点でWindows Portable ComputerにPII-Tracer 0.6BがMac Hybrid Computeと**全く同じ形で標準搭載されていることを示す詳細実装資料は確認できない**。Windows発表から確認できるのは、データがデバイス外へ出る前の承認制御である。したがって「PII-TRACE研究」から「Windows版が全PIIを自動遮断する」とまでは推定してはいけない。 ³¹

Perplexity側のデータ利用

一般消費者向けPerplexityでは、サービス提供、セキュリティ、製品改善等の目的で各種データを収集し、設定によっては検索・フィードバック等をモデル改善に利用する。Perplexityはデータを販売しないとしているが、Portable Computerの「ローカルタスク内容がPCに残る」という製品設計と、アカウント情報・利用情報等に適用される一般プライバシーポリシーは別レイヤーとして考える必要がある。 ³²

Enterpriseでは、Perplexityは**Enterpriseデータをモデル学習に使用しない**と明示し、SOC 2 Type II、GDPR/HIPAA関連の企業向け管理、SSO/SCIM、監査・保持管理などを提供する。機密業務でPortable Computerを利用する場合、この差は大きい。 ³³

Prompt injectionとエージェント権限

セキュリティ上もっとも重要な一次資料の一つがEnterprise Agentic Specific Termsである。Perplexityは、Computerを含む自律エージェントがWebや第三者システムとやり取りする以上、**prompt injectionを含むセキュリティ脅威に脆弱になり得る**と明記している。 ⁵

さらに同規約では、顧客に対し、

- エージェントが実行するアクション
- データ・アプリ・システムへのアクセス管理
- 適切な監督
- 必要なアクションの確認・承認

について責任を負わせ、エージェントの実行した操作を「権限を付与したユーザーによって実行されたもの」と扱う。⁵

つまり、Sandboxは「エージェントが許された領域から逸脱するリスク」を軽減するものであって、許可された領域内でAIが間違った操作をするリスクを消すものではない。

既知脆弱性

2026年9月15日時点で、本調査で確認できた公開情報からは、**Portable Computer for Windows固有のCVEや、公に再現可能な重大脆弱性は特定できなかった**。ただしWindows版は9月14日に公開されたばかりであるため、これは安全性の実証ではなく、単に公開後の観測期間が約1日しかないことを意味する。³⁴

したがって本番判断では「CVEがない」よりも、Perplexity自身がprompt injectionを明示的脅威として扱い、sandbox、ローカル権限制御、承認ゲートを設けている事実を重視すべきである。³⁵

ライセンス、商用利用、制限、ユーザー報告

個人向けPro/Maxをそのまま業務利用する際の注意

2026年1月23日最終更新の一般Perplexity利用規約では、Perplexityがユーザーへ付与する利用権は明確に「**お客様個人の非営利目的での利用に限り**」とされている。また営利目的でサービスを悪用することも禁止事項に含まれる。³⁶

一方、Enterprise Pro / Enterprise Maxの規約では「**顧客の事業目的のために本サービスを利用すること**」が明示的に認められ、入力的所有権を顧客が保持し、適用法の範囲で出力も顧客が所有すると定めている。³⁷

したがって、Portable Computerが技術的に個人Pro/Maxでも使えることと、その契約で企業の商用ワークフローに組み込んでよいことは同義ではない。

実務上の推奨は明確である。企業の業務処理、顧客データ、社内文書、ソフトウェア開発、本番自動化に使う場合はEnterprise契約を選ぶべきである。³⁸

また一般利用規約は、第三者LLMを利用する場合、そのモデル固有のライセンス・利用制限が出力に適用される可能性があると規定する。PPLX 27BのWindows配布物について独立したモデルライセンス、再配布権、重みの持ち出し可否は公開資料では**未特定**である。³⁶

Portable Computerはオープンソースではない

2026年9月15日時点で、Portable Computerのハース、Windowsクライアント、SPACE sandbox、PPLX 27B等を一式公開した公式GitHubリポジトリは確認できない。したがって、llama.cpp等のOSS技術を内部利用していても、Portable ComputerそのものをOSS製品として扱うことはできない。Perplexityの一般規約はソフトウェアの逆コンパイル、リバースエンジニアリング等も制限している。³⁹

性能上の制限

Perplexity自身のLocal Knowledge Work Benchでは、Qwen 3.8 27BをComputerハーネスで動かした場合のスコアは82.6%、PPLX 27Bは85.4%だった。一方、これはPerplexity自身が作成した53タスクのベンチマークであり、独立第三者評価ではない。 ¹⁶

特に高度なソフトウェアエンジニアリングではローカルモデルとフロンティアモデルの差が残る。Terminal Bench 2.1において、ローカルQwen 3.8 27Bは59.6%、Claude Opus 5へのadvisor escalationを許すと73.0%、Claude Opus 5単独では82.4%だった。エスカレーションの推定APIコストは1 rolloutあたり\$0.415、Claude単独は\$0.65と報告されている。 ¹⁴

これはPortable Computerの設計思想をよく示す。**プライバシーとコストを優先すれば完全ローカル、難題だけクラウドへ出せば精度を上げられる**が、完全ローカルと最先端クラウドを同一性能とは見せせない。

既知の問題・初期ユーザー報告

Windows版公開から約1日しか経過していないため、Reddit、GitHub、Stack Overflow等にWindows版固有の再現性の高い障害知見はまだ蓄積していない。Portable Computer自体に公開GitHub Issue trackerがないことも、OSS製品と比べて障害状況を外部から追跡しにくい要因である。 ³⁴

先行するDGX Spark版については、NVIDIA Developer Forumの初期利用者が、Perplexity ComputerがDGX Sparkを**専用推論サーバーのように扱う傾向**やメモリ管理面の注意を報告している。ただしこれは9月3日時点のDGX/Linux報告であり、Windows版にそのまま当てはまると判断してはいけない。 ⁴⁰

Perplexity公式Communityでも9月14日時点で、ComputerのコネクタがUI上選択済みでも実際のツール呼び出しへ渡らないというBug Report等が投稿されている。ただしこれもPortable Computer Windows固有の障害とは確認されていない。 ⁴¹

現時点で本番リスクとして重視すべき制限をまとめると以下になる。

制限	影響
24GB VRAM以上必須	多くの一般PC・ノートPCを除外
NVIDIA限定	AMD/Intel中心の環境には不向き
Windows版が公開直後	障害・互換性実績が少ない
OS/RAM/SSD最低仕様未公開	標準PCイメージの設計が難しい
モデル保存場所未公開	DLP、バックアップ、容量管理が難しい
SBOM/ライブラリ版未公開	脆弱性管理で不利
モデル更新ポリシー未公開	再現性・変更管理が難しい
完全エアギャップ保証なし	高度な閉域環境では事前検証必須
Prompt injectionリスク	Web/メール/外部文書処理は要監督
ローカルモデルの推論限界	難題ではクラウド利用が必要になり得る

競合・代替手段との比較

Portable Computerの直接競合は単なる「ローカルLLM GUI」ではなく、**ローカルでツール実行まで行うエージェント**である。その意味ではHermes AgentとOpenClawが最も近い。LM StudioのBionicはローカルAIワークステーション寄り、Ollamaはランタイムとして一段下のレイヤーに位置する。 ⁴²

製品	主用途	ローカルモデル	自律ツール/エージェント	Sandbox	Windows	UI / CLI	価格の目安
Perplexity Portable Computer	ナレッジワーク、ファイル、調査、長時間タスク	○	○	常時必須 / fail-closed	○、RTX 24GB+	Windows GUI	Pro \$20/月～
Hermes Agent	OSS汎用/self-improving agent	○、Ollama等	○	Perplexityほど強制的ではない	○	Desktop / terminal	無料OSS、MIT+モデル費
OpenClaw	パーソナルエージェント、メッセージング、自動化	○	○	設定しない場合host実行	○	Native/ UI/CLI/ TUI	本体無料+モデル費
LM Studio Bionic	ローカルLLM+文書/コード/PC作業	○	○	製品方式による	○	GUI中心	\$0から
Ollama	ローカルモデルランタイム/API	○	ランタイム中心	Agent側に依存	○	CLI/API	ローカル本体無料

Perplexityの最大の強みは、**セットアップ簡略化とsandboxを製品側で一体化**している点である。OSSエージェントでは、ユーザー自身がOllama、モデル、認証、ツール、権限、sandbox、アップデートを組み合わせる必要がある場合が多い。 ⁴³

Hermes AgentはNous ResearchによるMITライセンスの無料OSSで、Windows/macOSデスクトップおよびterminalから利用でき、Ollama等のセルフホスト推論にも接続できる。クラウドモデル費用は別途である。透明性、カスタマイズ性、再現性を重視する技術チームには強い選択肢である。 ⁴⁴

OpenClawは自PC上にstate、memory、credentialsを保持でき、Windowsを含む複数OS、CLI/TUI/Control UI、Slack・Teams・Telegram・WhatsApp等多数のチャンネルを扱える。2026年9月時点の公式GitHubは本体

の有料tierを設けていないと説明する。一方、main sessionのツールはsandboxを設定しなければホスト上で実行されるため、Portable Computerよりセキュアデフォルトの設計思想は弱い。 45

Windows向けOpenClaw CompanionはWindows 10 20H2以降またはWindows 11を要求し、ローカルGatewayをWSL内に構築できる。OpenClawは2026年9月3日にWindows RTX PC向けのローカルモデル設定も簡略化しているため、Portable Computerに最も近いOSS対抗馬の一つである。 46

ただしOpenClawの自由度には攻撃面も伴う。公式ドキュメント自体が外部入力をuntrustedとして扱うよう警告し、ClawHub拡張や高権限ツールをめぐって独立研究でもprompt injection、skill supply-chain、memory poisoning等が分析されている。Portable Computerが「閉じた統合製品」、OpenClawが「自由度の高い自己管理プラットフォーム」という違いがある。 47

LM StudioのBionicは無料tierでローカルLLM、llama.cpp/MLX、ローカル音声認識、文書編集、コーディング、オートメーション、computer controlまで提供する。Portable ComputerほどPerplexity Searchや企業コネクタに密接に統合されていない代わりに、ローカルモデル利用の自由度が高い。 48

OllamaはWindowsで利用可能なローカルモデルランタイムであり、単体ではPortable Computerと同等の企業向けエージェント統合製品ではない。ただしOpenClaw、Hermes等のバックエンドとして使えるため、「すべて自社管理したい」場合の構成要素として重要である。 49

どれを選ぶべきか

Portable Computerが向く組織は、Perplexity Computer/Searchをすでに利用し、24GB以上のNVIDIA RTXを配備でき、OSSエージェント基盤を自力で保守するより統合されたsandboxとUIを優先する組織である。 43

Hermes/OpenClawが向く組織は、モデル選択、設定、ログ、コード、バージョン固定、自己ホスティングを完全に管理したいチームである。特に監査上「どのコードが何を実行しているか」をソースで確認したい組織ではOSS側に優位性がある。 50

LM Studio/Ollamaが向くケースは、まずローカルLLM推論だけを導入し、OS自動操作やSaaS書き込みまでAIへ任せたくない場合である。エージェント能力を減らすこと自体がセキュリティ上のリスク削減になる。 51

本番導入手順、推奨運用、チェックリスト

段階的な導入手順

本番導入では、いきなりユーザーのOutlook、GitHub、OneDrive等を接続するべきではない。Perplexity自身がagentic機能にprompt injectionリスクがあると認めているため、**local-only → read-only → limited write → production**の順で権限を拡張するのが合理的である。 5

フェーズA：ハードウェア検査

```
$gpu = nvidia-smi `
--query-gpu=name,memory.total,driver_version `
--format=csv,noheader,nounits
```

\$gpu

VRAMが24,576MB前後以上あることを確認する。公式要件は「24GB以上」である。 19

フェーズB：Enterpriseアカウントと専用Windows端末

業務データを扱う場合はEnterprise Pro/Maxアカウントを使い、一般ユーザーのPCへ無制限に導入するより、まず専用ワークステーションまたは限定ユーザーグループで開始する。Enterprise規約は事業目的利用を許可し、Enterpriseデータをモデル学習に使わない方針も提供される。 52

フェーズC：ローカルモデルだけでPoC

ダミーデータを使い、

- PDF/Office ファイル要約
- ローカル検索
- 文書生成
- データ分析
- コード生成

等を実行する。ファイル操作、文書作成、データサイエンス、ソフトウェアエンジニアリングはPerplexityがPortable Computer向けスキルとして明示している。 16

フェーズD：ネットワーク観測

クラウド機能を使わない作業中に想定外の通信がないか、EDR、Windows Defender Firewall、プロキシ、DNSログ等で確認する。特に機密環境では、「モデル推論データ」と「認証・製品テレメトリ」を区別して記録する。

フェーズE：Read-only connector

Outlook、OneDrive、Google Drive、GitHub等を接続する際は、可能な範囲で読み取り権限から始める。Windows版ではこれらのコネクタがサポートされている。 19

フェーズF：書き込み操作を個別承認

メール送信、Git commit/push、ファイル上書き、文書共有など副作用のある操作はHuman-in-the-loopを残す。PerplexityのAgentic Termsも、必要な操作の確認・承認と能動的監督を顧客責任としている。 5

フェーズG：クラウドエスカレーションを限定解放

完全ローカルで品質不足となる業務だけadvisorを許可する。Perplexity自身のTerminal Benchでは、ローカルQwenからクラウドadvisorへエスカレーションすると59.6%から73.0%へ改善したため、性能面では有効だが、データ境界と費用が変わる。 14

設定ファイルについての重要な注意

2026年9月15日時点で、Portable Computer Windows版が直接読み込む公開設定ファイル形式は**確認できない**。したがって以下はPerplexity製品へ投入するファイルではなく、企業が導入要件を管理するための**内部ポリシー例**である。

```
# portable-computer-governance.yaml
# 注意: Perplexity公式設定ファイルではない。
# 組織内の導入・監査要件をコード化するための例。
```

```
portable_computer:
  deployment_tier: enterprise

local_processing:
  required_by_default: true
  web_search: deny_by_default
  cloud_advisor: approval_required

filesystem:
  allowed_roots:
    - "D:\\AI-Workspace"
  deny_roots:
    - "C:\\Users\\*\\Documents\\HR"
    - "C:\\Users\\*\\.ssh"

connectors:
  outlook:
    enabled: false
  onedrive:
    enabled: false
  github:
    enabled: true
    write_requires_human_approval: true

data_policy:
  pii: block_or_manual_review
  credentials: never_send_to_cloud
  customer_secrets: local_only

operations:
  auto_update: staged
  canary_group: "AI-Pilot"
  rollback_required: true
  network_logging: true
```

このように、「PerplexityのUI設定そのもの」ではなく、**どう設定されていなければならないかを組織側で宣言し、監査する**方式が、現段階では現実的である。

推奨運用・保守

Portable Computer本番環境では、次の三つを特に重視すべきである。

第一は**変更管理**である。アプリ、ローカルモデル、GPUドライバのいずれかが変わるだけでエージェントの挙動が変わる可能性がある。モデル更新ポリシーやPortable固有LTS版が公開されていない以上、本番端末の一部をcanary groupにし、更新後に定型テストを実施してから全社展開するのが望ましい。

第二は**権限の最小化**である。sandboxが強くても、sandboxに「全ホームディレクトリへの書き込み」「全GitHub orgへのwrite」「全メールボックスへの送信」を許してしまえば、誤操作時のblast radiusは大きい。Perplexity自身もアクセス制御を顧客責任としている。 35

第三は**クラウド送信の監査**である。Portable Computerの価値は、クラウド利用をゼロにすることより、「どの作業をローカルに残し、どの部分だけ外へ出すかを制御できる」点にある。したがって、クラウド承認を単なる確認ダイアログではなく情報分類ポリシーの一部として扱うべきである。 53

本番導入チェックリスト

契約・ガバナンス

- [] 業務利用ならEnterprise Pro/Maxの契約条件を法務確認した
- [] Enterprise Agentic Specific Termsをセキュリティ部門が確認した
- [] AIによる操作の責任主体とHuman-in-the-loopルールを定義した
- [] 個人Pro/Maxを商用本番用途に流用していない 6

端末

- [] NVIDIA GeForce RTX / RTX PROを搭載
- [] VRAM 24GB以上
- [] `nvidia-smi` でGPUとドライバを記録
- [] OS Build、RAM、SSD容量を資産管理DBへ記録
- [] モデル保存に伴う容量増加を監視する仕組みを用意 19

セキュリティ

- [] Portable Computerから利用可能なフォルダを限定
- [] `.ssh`、ブラウザプロフィール、資格情報保管場所等を対象外にした
- [] Connector権限を最小化
- [] メール送信・外部共有・Git write等を要承認化
- [] EDR/Firewall/DNS/Proxyでネットワーク挙動を観測
- [] Prompt injectionを前提に外部Web・メール・文書をuntrusted inputとして扱う
- [] sandboxが失敗した状態でツール実行できないことをPoCで確認 35

プライバシー

- [] ローカルだけで処理すべきデータ分類を定義
- [] Web Search / Cloud Advisorをdefault-denyまたは要承認にした
- [] PII検知だけをDLP代替にしている
- [] Enterpriseのtraining exclusionを確認
- [] Connector先のMicrosoft/Google/GitHub等の保持・監査ポリシーも確認 54

運用

- [] アプリ更新はcanary → 本番の段階展開
- [] GPUドライバ更新も同じ回帰テストを実施
- [] モデル名、バージョン、モデル容量を定期記録
- [] ローカル性能とクラウドadvisor使用率を測定
- [] 定期タスクの出力先と書込権限を監査
- [] 重大操作の監査ログを保持
- [] インシデント時にConnectorsのOAuthトークンを即時revoke可能にした
- [] Portable Computer固有CVE/セキュリティアドバイザリを継続監視

主要参考リンクと最終評価

以下は調査上重要度が高かった一次資料を、Perplexity公式、日本語ページ、NVIDIA、競合公式の順に整理したものである。

Perplexity公式

Portable Computer for Windows is here — 2026-09-14

<https://www.perplexity.ai/ja/hub/blog/portable-computer-for-windows-is-here>
Windows版の正式公開日、ローカル実行、クレジット非消費等の中心資料。 55

Introducing Portable Computer for local-first AI — 2026-08-25

<https://www.perplexity.ai/ja/hub/blog/introducing-portable-computer-for-local-first-ai>
Portable Computerそのものの初回製品発表。ローカルモデル、クラウドエスカレーション、Computer構成要素、sandbox等を説明。 20

A local-first agent for private and cost-effective knowledge work — 2026-08-25

<https://www.perplexity.ai/ja/hub/blog/a-local-first-agent-for-private-and-cost-effective-knowledge-work>
最も重要な技術資料。ハーネス、context management、MCP→CLI、sandbox、advisor、ベンチマークを説明。 13

PII-TRACE: Detecting Personal Data Before It Leaves the Device — 2026-09-01

<https://www.perplexity.ai/ja/hub/blog/pii-trace-detecting-personal-data-before-it-leaves-the-device>
PIIローカル検知の研究資料。 30

Introducing Hybrid Compute on Mac — 2026-09-01

<https://www.perplexity.ai/ja/hub/blog/introducing-hybrid-compute-on-mac>
Windowsそのものではないが、Perplexityのローカル/クラウド境界・承認設計を理解する一次資料。 56

Perplexity利用規約 — 最終更新2026-01-23

<https://www.perplexity.ai/ja/hub/legal/terms-of-service>
個人向けサービスの非営利利用制限等。 36

Enterprise Pro / Max利用規約

<https://www.perplexity.ai/ja/hub/legal/enterprise-terms-of-service>
事業目的利用、顧客コンテンツ所有権等。 37

Enterprise Agentic Specific Terms — 最終更新2026-08-03

<https://www.perplexity.ai/ja/hub/legal/enterprise-agentic-specific-terms>

Computer等の自律エージェントに対するprompt injection、監督責任、操作責任の最重要法務資料。 5

Enterprise料金・課金FAQ

<https://www.perplexity.ai/help-center/en/articles/10352986-enterprise-pricing-and-billing-frequently-asked-questions>

Enterprise Pro / Maxの現行価格。 57

Perplexity Subscription Plan比較

<https://www.perplexity.ai/help-center/en/articles/11187416-which-perplexity-subscription-plan-is-right-for-you>

個人・Enterpriseプランの現行機能。 58

NVIDIA公式

Local AI With Perplexity Comes to Windows RTX PCs — 2026-09-14

<https://blogs.nvidia.com/blog/local-ai-perplexity-windows-pcs/>

Windows版に関するもっとも具体的な補完資料。GeForce RTX/RTX PRO、**24GB以上VRAM**、Windows app、SPACE sandbox、Qwen、Outlook/OneDrive/Word等を確認できる。 19

Next-Generation Local AI Agents on RTX and DGX Spark — 2026-09

<https://blogs.nvidia.com/blog/local-ai-ifa-next-gen-agents-nv-pair-rtx-spark/>

llama.cppベースのローカルエージェント群や推論最適化を説明。 17

日本語の補助資料

GIGAZINEは2026年8月26日に初期Linux/DGX版Portable Computerを日本語で報道しており、初期発表内容を確認する補助資料として有用である。 59

ただし8月末時点の記事は「Windows近日公開」の状態を記述しているため、2026年9月14日のWindows正式公開後の現状確認にはPerplexity/NVIDIAの一次資料を優先すべきである。8月30日時点でWindows提供日は未発表だったことも日本語技術記事から確認できる。 60

競合公式

Hermes Agent — Nous Research

<https://hermes-agent.nousresearch.com/>

無料MIT OSS、Windows/macOS/Desktop/terminal、ローカル推論プロバイダー対応。 61

Hermes Agent GitHub

<https://github.com/NousResearch/hermes-agent>

ソースコードと開発状況。 62

OpenClaw GitHub

<https://github.com/openclaw/openclaw>

ローカル状態・モデル、Windows/Linux/macOS、CLI/TUI/UI、security model。 45

OpenClaw Windows Companion

<https://github.com/openclaw/openclaw-windows-node>

Windows 10 20H2以降/Windows 11、WSL Gateway等。 63

LM Studio / Bionic

<https://lmstudio.ai/>

無料ローカルLLM、Bionic agent、llama.cpp/MLX、ローカル音声等。 48

Ollama Windows

<https://ollama.com/download/windows>

Windowsローカルモデルランタイム。 64

総合評価

Portable Computer for Windowsは、2026年9月時点のローカルAIエージェント市場において、「高性能なローカルモデル」「長時間動作するエージェント」「ローカルファイル操作」「クラウドへの選択的エスケーション」「常時sandbox」を一つの商用Windows製品に統合した点で注目に値する。特に、ローカルLLMを起動しただけの製品と異なり、オーケストレーション層までデバイス側に置き、クラウドadvisorにOS権限を直接与えない設計は、企業の機密ナレッジワークに合理的なアーキテクチャである。 65

しかし、「ローカルだから即Enterprise-ready」と判断するのは早い。Windows版公開からまだ1日しか経っておらず、OS最低版、システムRAM、ストレージ、モデル格納場所、モデルチェックサム、依存ライブラリ版、更新/ロールバック方式、Portable固有の公開SBOM、完全エアギャップ要件、Windows固有の長期障害情報が公開資料から特定できない。これらは大規模導入では無視できない運用上の情報不足である。 66

したがって、2026年9月15日時点での最も妥当な企業導入方針は、Enterprise契約+24GB以上のRTX専用端末で、クラウドとコネクタをdefault-denyにした限定PoCから始め、ネットワーク挙動・sandbox・モデル更新・ファイルアクセス範囲を実測した後に段階的に権限を広げることである。これはPerplexity自身がエージェントに対するprompt injectionと監督責任を明示していることとも整合する。 67

現状を一言で評価すれば、Portable Computer for Windowsは「ローカルLLMアプリ」ではなく、クラウドAIとPC内エージェントの境界をユーザー管理下に戻そうとする本格的なlocal-first agent platformである。ただし、Windows版は極めて新しく、企業本番導入に必要な運用仕様の公開度はまだ技術アーキテクチャの完成度に追いついていない。この点を前提にPoCと権限設計を行うことが、現時点でもっとも低リスクな導入方法である。

1 7 10 12 22 25 28 34 38 55 66 Portable Computer for Windows is here

https://www.perplexity.ai/?utm_source=chatgpt.com

2 3 8 15 20 24 53 Introducing Portable Computer

https://www.perplexity.ai/en-GB/hub/blog/introducing-portable-computer-for-local-first-ai?utm_source=chatgpt.com

4 13 14 16 26 65 プライベートなナレッジワークのためのローカルファーストエージェント

<https://www.perplexity.ai/ja/hub/blog/a-local-first-agent-for-private-and-cost-effective-knowledge-work>

5 35 67 Perplexity Enterpriseエージェント固有条件

<https://www.perplexity.ai/ja/hub/legal/enterprise-agent-specific-terms>

6 36 39 Perplexity利用規約

<https://www.perplexity.ai/ja/hub/legal/terms-of-service>

- 9 56 Macでのハイブリッドコンピュートのご紹介
<https://www.perplexity.ai/ja/hub/blog/introducing-hybrid-compute-on-mac>
- 11 News | Perplexity blog
https://www.perplexity.ai/tr/hub/blog/category/news?utm_source=chatgpt.com
- 17 Sparks Fly: NVIDIA Accelerates Local AI at IFA 2026
https://blogs.nvidia.com/blog/local-ai-ifa-next-gen-agents-nv-pair-rtx-spark/?utm_source=chatgpt.com
- 18 19 21 31 43 Perplexity Portable Computer Is Now Available on Windows, Powered by NVIDIA RTX | NVIDIA Blog
<https://blogs.nvidia.com/blog/local-ai-perplexity-windows-pcs/>
- 23 How Credits Work on Perplexity - Perplexity Help Center
https://www.perplexity.ai/help-center/en/articles/13838041-how-credits-work-on-perplexity?utm_source=chatgpt.com
- 27 32 Data Collection at Perplexity - Perplexity Help Center
<https://www.perplexity.ai/help-center/en/articles/11564572-data-collection-at-perplexity>
- 29 47 GitHub - openclaw/openclaw at opentechhub.io · GitHub
https://github.com/openclaw/openclaw?ref=opentechhub.io&utm_source=chatgpt.com
- 30 54 PII-TRACE：デバイスから離れる前に個人データを検出する
<https://www.perplexity.ai/ja/hub/blog/pii-trace-detecting-personal-data-before-it-leaves-the-device>
- 33 Perplexity Enterprise
<https://www.perplexity.ai/enterprise>
- 37 52 Perplexity Enterprise ProおよびMax利用規約
<https://www.perplexity.ai/ja/hub/legal/enterprise-terms-of-service>
- 40 Perplexity Computer on DGX Spark — first impressions ...
https://forums.developer.nvidia.com/?utm_source=chatgpt.com
- 41 Feature Request: Bring Your Own Key (BYOK) — Let Users ...
https://community.perplexity.ai/?utm_source=chatgpt.com
- 42 50 61 LLM and Model Providers | Hermes Agent - NOUS RESEARCH
https://hermes-agent.nousresearch.com/?utm_source=chatgpt.com
- 44 62 NousResearch/hermes-agent: The agent that grows with you
https://github.com/?utm_source=chatgpt.com
- 45 OpenClaw — Your assistant, on your devices, in your chats - GitHub
https://github.com/openclaw/openclaw?utm_source=chatgpt.com
- 46 63 Windows companion suite for OpenClaw - GitHub
https://github.com/openclaw/openclaw-windows-node?utm_source=chatgpt.com
- 48 51 Bionic Pricing
https://lmstudio.ai/?utm_source=chatgpt.com
- 49 64 Download Ollama on Windows
https://ollama.com/?utm_source=chatgpt.com
- 57 Enterprise Pricing and Billing: Frequently Asked Questions - Perplexity
https://www.perplexity.ai/help-center/en/articles/10352986-enterprise-pricing-and-billing-frequently-asked-questions?utm_source=chatgpt.com

58 Which Perplexity Subscription Plan is right for you?

https://www.perplexity.ai/help-center/en/articles/11187416-which-perplexity-subscription-plan-is-right-for-you?utm_source=chatgpt.com

59 「Perplexity Computer」の完全ローカル版「Portable ...

https://gigazine.net/?utm_source=chatgpt.com

60 Perplexity Portable ComputerはWindowsでいつ使える？Linux ...

https://keieiax.jp/?utm_source=chatgpt.com