

ローカルで動くAIの今後の姿を試してみる MXCでOpenClaw保護・Aion Instructの用途

2026/7/21 須藤 (suusanex)

自己紹介

- ▶ ID:suusanex(connpass・Twitter・GitHub共通)
- ▶ 名前：須藤圭太
- ▶ サイエンスパーク株式会社という独立系ソフトウェアベンダーに所属
 - 自社製品開発・継続保守する製品開発を10年ほど・受託開発は5年ほど
- ▶ 小規模開発チームでPM・プログラマ・プラットフォームエンジニア・テックリード的な事まで何でもやっています
 - C#・Windows開発がメインでC++もいける
 - Windowsアプリ開発のネタが多い
- ▶ Developer Technologies .NETでMicrosoft MVPを受賞しました
- ▶ C# Tokyoコミュニティでイベント開催



今日の流れ

- ▶ Build 2026で見た「クラウドとエッジの使い分け」が面白かった
- ▶ その中で気になった2つを試した
 - ▶ MXC: ローカル高権限エージェントの安全境界
 - ▶ 軽量モデルAion Instruct: 小さな用途を手元で回すための選択

高機能AIとエッジAIの使い分けの流れが来る？

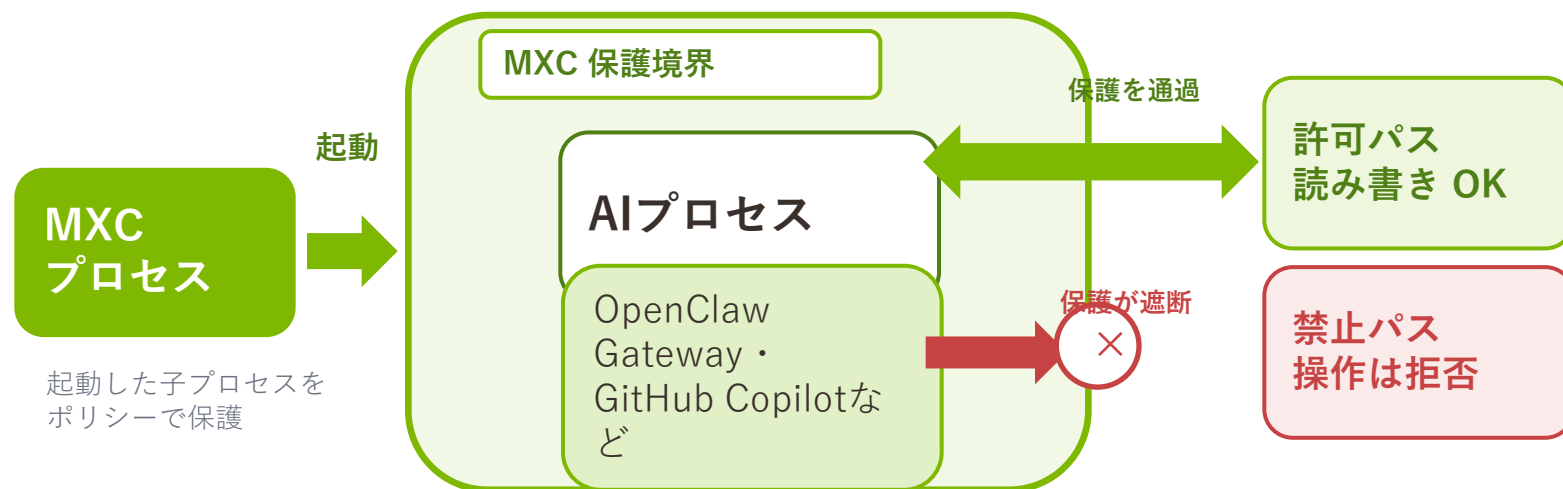
- ▶ GitHub Copilot や Claude Code などの高機能エージェントは便利だが、従量課金で「何でも任せる」には重くなってきた
- ▶ 一方で、ローカルで即答したい・手元のリソースも操作して色々やって欲しい用途は増えている
- ▶ これに対して Microsoft Build 2026 では「エッジAIとの使い分け」という提案が出ていた
- ▶ 単にローカルLLMを使うという話ではなく、手元のPC内でAIエージェントを動かす多面的な取り組み
- ▶ 特に気になったのはMXCと軽量モデルAion Instruct

MXCとは？

- ▶ 「AIに任せたら重要なファイルを消した」みたいな話は以前からずっと聞く、最近も見かけた
- ▶ かといってサンドボックスを付けると、必要な処理が出来ないことも多い
- ▶ もっと細かく、「ワークスペース外でもこのフォルダは使って良い、しかしUserProfileは書き込み・削除禁止」とか色々設定したい
- ▶ それをやってくれるのがMXC（まだプレビュー版）

汎用的に使えそうなプロセス単位制御を試す

- ▶ ここではWindowsにおいて最もシンプルで汎用性が高そうなプロセス単位制御
 - ▶ VM・コンテナ・プロセスなど色々な入れ方があるらしい
- ▶ MXCプロセスから起動した子プロセスに対して、制御できる
- ▶ そんな仕組みがWindowsに？
 - ▶ UWP・ストアアプリの方式っぽい



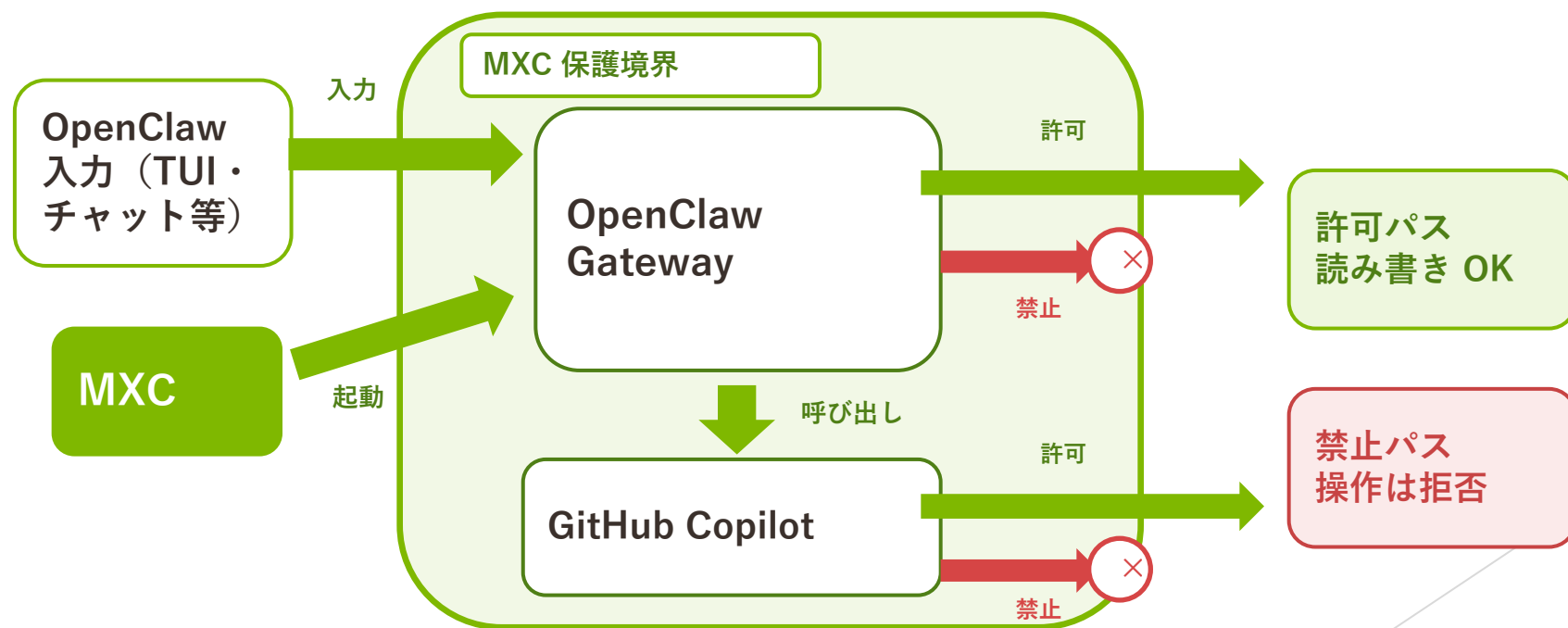
プロセス単位でどう使えるか

- ▶ AIエージェントには、親プロセスが1つ有ってそこからツールやサブエージェントを使うタイプが多い（知ってる範囲では）
 - ▶ Codex CLIとかGitHub Copilot CLIとかもそう
- ▶ なので汎用的に効く。たぶんGUI付きのタイプにも効く
- ▶ OpenClaw も、メインはGatewayプロセス部で動いてるので、そこに入れば効くはず
- ▶ JSONファイルでポリシーを与えて細かく制御できる
 - ▶ ファイルシステムはReadWrite,ReadOnly,Deny

```
readwritePaths?: string[];  
readonlyPaths?: string[];  
deniedPaths?: string[];
```
 - ▶ ネットワークやクリップボードなども

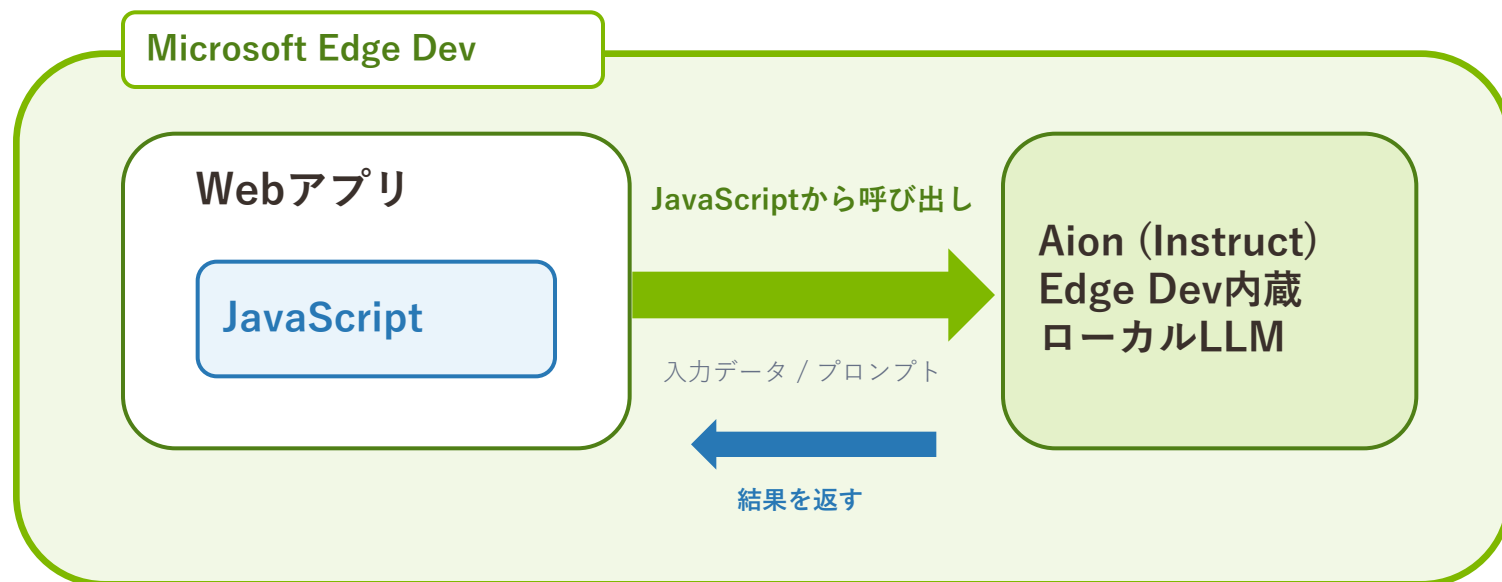
実際にOpenClawで使ってみた

- ▶ 効いた。Gatewayからの操作も、GitHub Copilotからの操作も、どちらも制御できた
- ▶ 許可パスのRead/Writeは成功していて、禁止パスの削除は禁止された



Aion(Instruct)とは

- ▶ MS製の、用途を限定したローカルLLM
- ▶ Plan と Instruct があり、Planは普通。Instructがだいぶ違って、尖っている
- ▶ Edge専用（初回使用時にモデルをDL）
 - ▶ 現在はStable未実装で、Devなどが必要
- ▶ Webブラウザ上の処理としてJavaScriptから呼べる
- ▶ 驚くほど、速い、軽い、能力は最小限



Aion Instructで何ができるか

- ▶ 試してみた結果・・・
- ▶ 短文の翻訳やカテゴリ分けなどはOK
- ▶ 長文の翻訳や、要約などの文章構造理解を要するものはかなりキツイ
- ▶ つまり・・・
- ▶ 高速軽量でどの環境でも動くことを優先し、用途は大胆に絞り込んでいる
- ▶ まさに、用途別にAIを使い分ける発想

まとめ

- ▶ 高性能AIになんでも投げる、は従量課金に耐えられる富豪向けになってきた
- ▶ 用途はむしろ増え、ローカルで高権限を与えて動かしたいケースも増えてきた
- ▶ そのため、今までとはちょっと違う機能が出てきている
 - ▶ ローカルAIの危険動作を制限
 - ▶ 超軽量モデルなどLLMの使い分け
- ▶ そういう技術も把握して、自分に使いやすいAIを構築していくのが良さそう