

第45回　「MCP: Advanced Topics」
Anthropic 公式 Claude Academy

Claude Code

触っていい場所を決める

公式の教材を、順番に

原石工房
隠れた才能に気づき、花開く

この資料について

原石工房

Anthropic とは関係のない、非公式の資料です

公式の学習サイト Claude Academy の日本語訳です

原文（英語）MCP: Advanced Topics ／ Roots

原文は、決まりごとの2026年7月28日の改訂より前の MCP を教えています

出どころ＝ Anthropic 公式 Claude Academy「MCP: Advanced Topics」／
https://academy.claude.com/courses/model-context-protocol-advanced-topics/roots ／ 非公式の日本語訳

全51回の、今日はここ

原石工房

Claude Code 101 — 第1回〜第12回

1 2 3 4 5 6 7 8 9 10 11 12

Claude Code in Action — 第13回〜第21回

13 14 15 16 17 18 19 20 21

スキル — 第22回〜第27回

22 23 24 25 26 27

手分け（subagents） — 第28回〜第31回

28 29 30 31

MCP 入門 — 第32回〜第40回

32 33 34 35 36 37 38 39 40

MCP 応用 — 第41回〜第51回

41 42 43 44 **45** 46 47 48 49 50 51

今日はここ　第45回

出どころ＝ Anthropic 公式 Claude Academy「MCP: Advanced Topics」／
https://academy.claude.com/courses/model-context-protocol-advanced-topics/roots ／ 非公式の日本語訳

今日のレッスン

原石工房

MCP: Advanced Topics の第5回

原題　Roots

訳　触っていい場所を決める

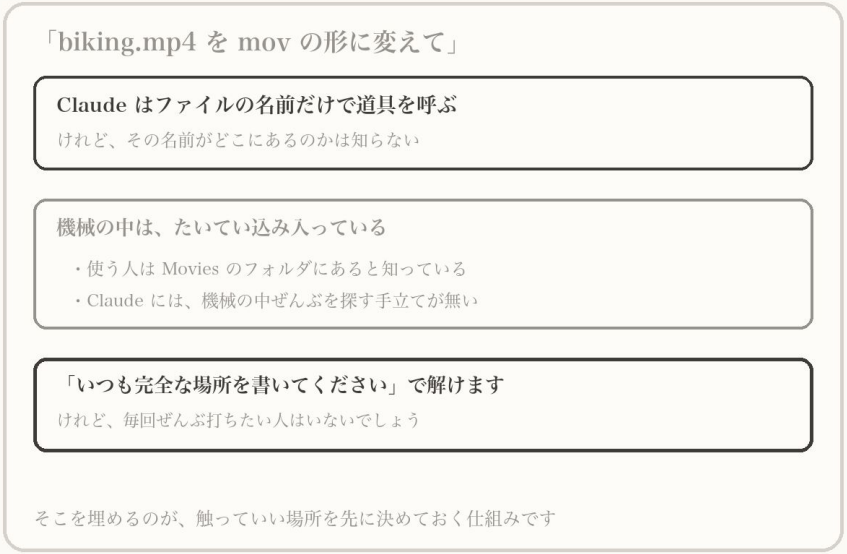
決まったファイルとフォルダを、サーバーに使わせる仕組みです

出どころ＝ Anthropic 公式 Claude Academy「MCP: Advanced Topics」／
https://academy.claude.com/courses/model-context-protocol-advanced-topics/roots ／ 非公式の日本語訳

① 名前は分かる。場所が分からない

原石工房

原題 The Problem Roots Solve



名前は分かる。場所が分からない

「biking.mp4 を変えて」と頼まれたとき

Claude は、その名前がどこにあるのかを知りません

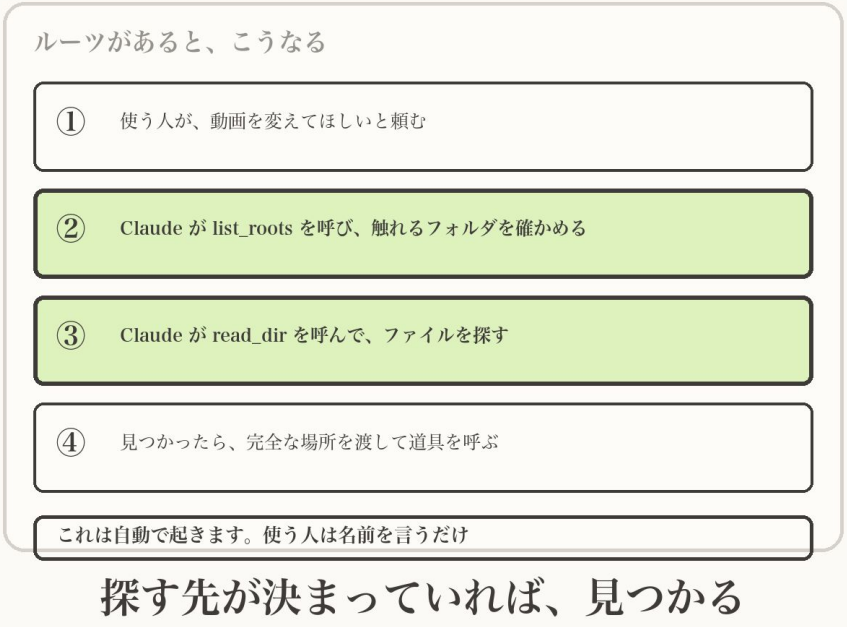
毎回ファイルの場所をぜんぶ打ちたい人はいないでしょう

出どころ＝ Anthropic 公式 Claude Academy「MCP: Advanced Topics」／
https://academy.claude.com/courses/model-context-protocol-advanced-topics/roots ／ 非公式の日本語訳

② ルーツがあると、4つの段

原石工房

原題 Roots in Action



探す先が決まっていれば、見つかる

list_roots を呼び、触れるフォルダを確かめます

read_dir を呼んで、その中からファイルを探します

見つかったら、完全な場所を渡して道具を呼びます

出どころ＝ Anthropic 公式 Claude Academy「MCP: Advanced Topics」／
https://academy.claude.com/courses/model-context-protocol-advanced-topics/roots ／ 非公式の日本語訳

③ 境目が、そのまま安全になる

原石工房

原題 Security and Boundaries

デスクトップだけを許せば、他の場所には触れません

外に触ろうとすると、間違いが返ります

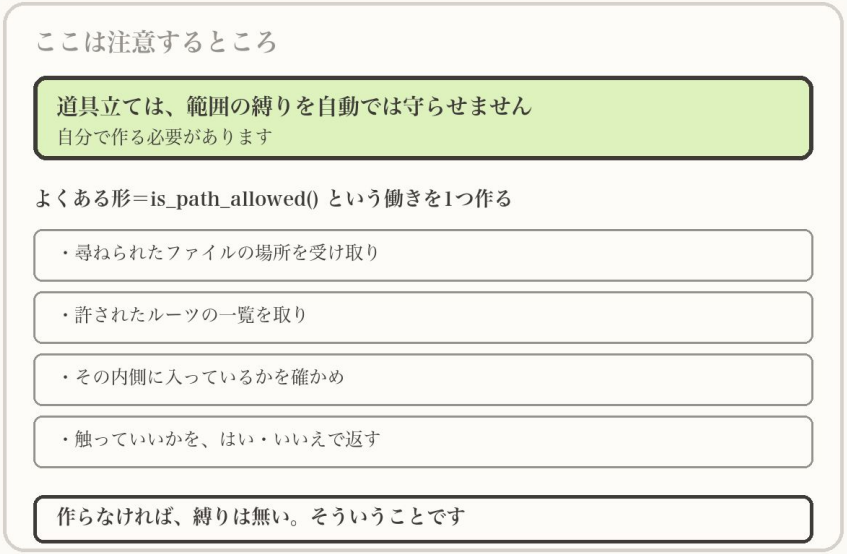
「いまの設定では触れません」と、使う人に伝えられます

出どころ＝ Anthropic 公式 Claude Academy「MCP: Advanced Topics」／
https://academy.claude.com/courses/model-context-protocol-advanced-topics/roots ／ 非公式の日本語訳

④ 縛りは、自分で作る

原石工房

原題 Implementation Details



ファイルに触る前に、必ず通す

道具立ては、範囲の縛りを自動では守らせません

is_path_allowed() のような働きを1つ作ります

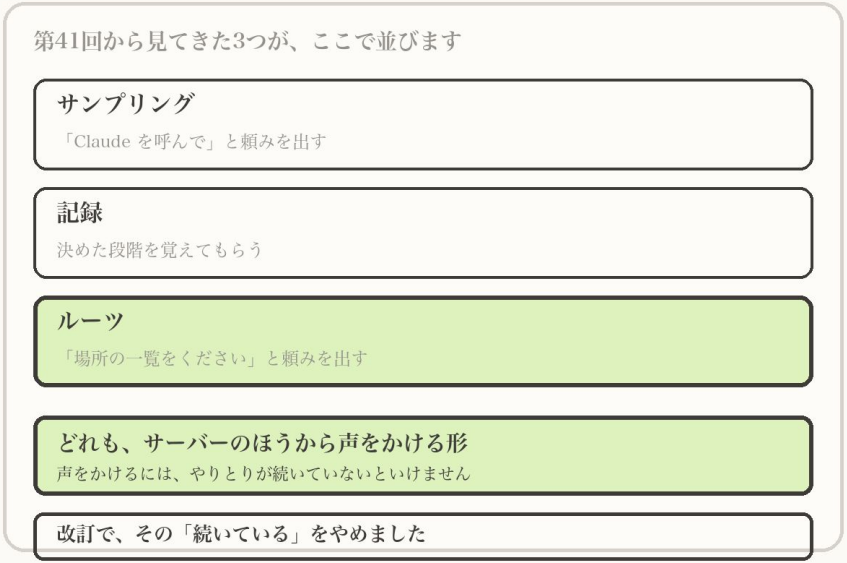
ファイルに触るすべての道具で、触る前に呼びます

出どころ＝ Anthropic 公式 Claude Academy「MCP: Advanced Topics」／
https://academy.claude.com/courses/model-context-protocol-advanced-topics/roots ／ 非公式の日本語訳

※ 補足　非推奨の3つに、共通すること

原石工房

ここから先は原文にありません



土台が変わって、上のものが落ちた

サンプリング・記録・ルーツが、ここで出そろいました

どれも、サーバーのほうから声をかける形でした

改訂で、やりとりが「続いている」ことをやめました

出どころ＝ Anthropic 公式 Claude Academy「MCP: Advanced Topics」／
https://academy.claude.com/courses/model-context-protocol-advanced-topics/roots ／ 非公式の日本語訳

※ 補足　境目を、先に決めておく

原石工房

許したフォルダの中

- Claude がここだけを探す
- 見つけるのが速い
- 完全な場所を打たなくていい

許していない場所

- 触ろうとすると間違いが返る
- 大事なファイルを守れる
- 「触れません」と使う人へ伝える

使いやすさと安全が、同じ1つの仕組みから出てくる

ただし、縛りを書かなければ、境目は存在しません

どこまで触らせるかを、先に決めておく

出どころ＝ Anthropic 公式 Claude Academy「MCP: Advanced Topics」／
https://academy.claude.com/courses/model-context-protocol-advanced-topics/roots ／ 非公式の日本語訳

※ 補足　考え方のほうは、残ります

原石工房

どこまで触らせるかを決めるのは、第16回で見た話と同じです

いちばん大事なのは、縛りを自分で書くところだと思います

書かなければ、境目は存在しません

出どころ＝ Anthropic 公式 Claude Academy「MCP: Advanced Topics」／
https://academy.claude.com/courses/model-context-protocol-advanced-topics/roots ／ 非公式の日本語訳

今回のまとめ

原石工房

ルーツは、触っていいファイルとフォルダを決める仕組み

使いやすさと安全が、同じ1つの仕組みから出てきます

非推奨。乗り換え先は、道具の引数・資料のURI・サーバーの設定

出どころ＝ Anthropic 公式 Claude Academy「MCP: Advanced Topics」／
https://academy.claude.com/courses/model-context-protocol-advanced-topics/roots ／ 非公式の日本語訳

どこまでなら、任せられますか



原石工房

隠れた才能に気づき、花開く