

ADOPTION ASSESSMENT

by Teastia

導入判定書

SUBJECT

| 検査対象

(名前の無いアプリ: 設定ファイル package.json に名前がありません)

teastia 3.6.0 / 検査日 2026-08-23 / 検査した範囲: 指定したフォルダ全体 (72 ファイル)

teastia 3.6.0 / Inspected 2026-08-23 / Scope: entire specified folder (72 files)

OVERALL VERDICT

| 総合判定

導入不可

NOT APPROVED

1 項目が「該当」。直して再検査するまで導入できません（ほかに条件つき 3 項目）。判定できない 2 項目は質問票の回答などで埋まります。

EIGHT STOP-CONDITION CHECKS

| チェック 8 項目 (STOP 条件)

#	何を見たか / What was checked	判定	理由 (1 行)
1	鍵やパスワードがプログラムの中に書かれていないか	該当なし	問題は見つからなかった (5 個のチェック)
2	会社が知らない場所にデータを送っていないか	判定できない	質問票の「許可した送り先の一覧」の回答待ち
3	会社が知らない AI 会社・モデルを使っていないか	判定できない	AI 会社を機械で見つけられなかった
4	AI が人の許可なしに、消す・実行する・払うをできないか	該当	道具 edit_file が ファイルを消す (道具が呼んでいる関数の中で。filesystem/lib.ts 341 行目、fs.unlink) 、道具 write_file が ファイルを消す (道具が呼んでいる関数の中で。filesystem/lib.ts 216 行目、fs.unlink) 。人が承認・確認するコードなし
5	AI が人の許可なしに、データを外に出せないか	該当なし	道具 24 件の中身を、呼んでいる関数の 2 段先まで読み、外に出す (送る・外のサービスに書く) 処理は見つからず
6	誰の権限で動いているか分かるか	条件つき	ログインの仕組みが見当たらない
7	古くて危ない部品 (依存) を使っていないか	条件つき	部品の版が固定されていない (ロックファイルが無い)
8	問題が起きたとき止められるか	条件つき	利用回数・量の上限が見当たらない

判定に使う言葉は 4 つだけです: 該当 (直すまで導入できない) / 条件つき (直せば導入できる) / 該当なし / 判定できない (答えが足りない)。点数は付けません。

ADOPTION ASSESSMENT

導入判定書 | 根拠にした制度

REGULATORY BASIS

| 根拠にした制度

判定の根拠は、AI 事業者ガイドライン第 1.2 版（総務省・経済産業省、2026 年 3 月 31 日）の指針番号で示します。

項目 / Item	AI 事業者ガイドライン（共通の指針）	だれの決まりか（主体別）	法令・海外の技術基準
1 鍵・パスワード	5) セキュリティ確保 ①	作った会社 P-5) i / 使う会社 U-5) i	CWE-798、OWASP LLM02
2 データの送り先	4) プライバシー保護 ①、5) セキュリティ確保 ①	作った会社 P-4) i / 使う会社 U-4) i	個人情報保護法 27・28 条、OWASP LLM02
3 AI 会社の把握	7) アカウンタビリティ ①⑥	作った会社 P-7) ii / 使う会社 U-7) ii	個人情報保護法 28 条
4 勝手な操作	2) 安全性 ②、3) 公平性 ②	作った会社 P-2) i / 使う会社 U-2) i	OWASP LLM06、Agentic ASI02/05
5 勝手な持ち出し	2) 安全性 ②、4) プライバシー保護 ①	作った会社 P-2) i / 使う会社 U-2) i	OWASP LLM06、Agentic ASI02/07
6 誰の権限か	7) アカウンタビリティ ①、6) 透明性 ①	作った会社 P-6) i / 使う会社 U-7) i	OWASP ASVS V2、CWE-306
7 古い部品	5) セキュリティ確保 ②	作った会社 P-5) ii	CWE-1395、OWASP LLM03
8 止められるか	5) セキュリティ確保 ①（侵害時の措置：停止）、7) アカウンタビリティ ③	使う会社 U-5) i / 作った会社 P-2) i	OWASP Agentic ASI08

HOW TO READ

| 読み方

「5) セキュリティ確保 ①」= 10 ある指針の 5 番目の、1 つ目の決まり。「作った会社 P-5) i」= アプリを作った会社（AI 提供者）向けの決まり、「使う会社 U-5) i」= 使う会社（お客様 = AI 利用者）向けの決まり。番号はガイドラインの表 1 のとおりなので、別添 7 のチェックリストにそのまま引けます。

根拠の欄は AI 事業者ガイドライン第 1.2 版の指針番号です。ガイドラインや情報セキュリティサービス基準への適合を認定・保証するものではありません。

This report cites guideline clause numbers only. It does not certify or guarantee conformity to any standard.

ADOPTION ASSESSMENT

導入判定書 | AI が呼べる道具

AI TOOL INVENTORY (1/2)

| AI が呼べる道具（機械が見つけたもの）

AI アプリの危なさは、AI にどんな「手」を握らせているかで決まります。機械がコードから見つけた道具の一覧です。

道具 24 件。 機械が「消す・実行する・払う・外に出す」処理を見つけたのは 2 件（edit_file、write_file）。

道具 / Tool	説明（開発会社書いたまま）	引数	中身（機械が読んだ結果）	どこ
create_directory	Create a new directory or ensure a directory exists. Can create multiple	path	危ない処理は見つからず	filesystem/index.ts
directory_tree	Get a recursive tree view of files and directories as a JSON structure.	path, excludePatterns	危ない処理は見つからず	filesystem/index.ts
edit_file	Make line-based edits to a text file. Each edit replaces exact line sequences	path, edits, dryRun	消す（fs.unlink、呼んでいる関数の中）・人が承認・確認するコードなし	filesystem/index.ts
get_file_info	Retrieve detailed metadata about a file or directory. Returns comprehensive	path	危ない処理は見つからず	filesystem/index.ts
list_allowed_directories	Returns the list of directories that this server is allowed to access.	—	危ない処理は見つからず	filesystem/index.ts
list_directory	Get a detailed listing of all files and directories in a specified path.	path	危ない処理は見つからず	filesystem/index.ts
list_directory_with_sizes	Get a detailed listing of all files and directories in a specified path, including sizes.	path, sortBy	危ない処理は見つからず	filesystem/index.ts
move_file	Move or rename files and directories. Can move files between directories	source, destination	危ない処理は見つからず	filesystem/index.ts
read_file	Read the complete contents of a file as text. DEPRECATED: Use read_text_file instead.	—	危ない処理は見つからず	filesystem/index.ts
read_media_file	Read a file and return it as a base64-encoded content block with its MIME type.	path	危ない処理は見つからず	filesystem/index.ts
read_multiple_files	Read the contents of multiple files simultaneously. This is more	paths	危ない処理は見つからず	filesystem/index.ts
read_text_file	Read the complete contents of a file from the file system as text.	path, tail, head	危ない処理は見つからず	filesystem/index.ts
search_files	Recursively search for files and directories matching a pattern.	path, pattern, excludePatterns	危ない処理は見つからず	filesystem/index.ts
write_file	Create a new file or completely overwrite an existing file with new content.	path, content	消す（fs.unlink、呼んでいる関数の中）・人が承認・確認するコードなし	filesystem/index.ts

ADOPTION ASSESSMENT

導入判定書 | AI が呼べる道具

AI TOOL INVENTORY (2/2)

| AI が呼べる道具 (つづき)

道具 / Tool	説明（開発会社書いたまま）	引数	中身（機械が読んだ結果）	どこ
add_observations	Add new observations to existing entities in the knowledge graph	observations	危ない処理は見つからず	memory/index.ts
create_entities	Create multiple new entities in the knowledge graph	entities	危ない処理は見つからず	memory/index.ts
create_relations	Create multiple new relations between entities in the knowledge graph. Relations should be in active voice	relations	危ない処理は見つからず	memory/index.ts
delete_entities	Delete multiple entities and their associated relations from the knowledge graph	entityNames	危ない処理は見つからず	memory/index.ts
delete_observations	Delete specific observations from entities in the knowledge graph	deletions	危ない処理は見つからず	memory/index.ts
delete_relations	Delete multiple relations from the knowledge graph	relations	危ない処理は見つからず	memory/index.ts
open_nodes	Open specific nodes in the knowledge graph by their names	names	危ない処理は見つからず	memory/index.ts
read_graph	Read the entire knowledge graph	—	危ない処理は見つからず	memory/index.ts
search_nodes	Search for nodes in the knowledge graph based on a query	query	危ない処理は見つからず	memory/index.ts
sequentialthinking	—	thought, nextThoughtNeeded, thoughtNumber, totalThoughts, isRevision, revisesThought, branchFromThought, branchId, needsMoreThoughts	危ない処理は見つからず	sequentialthinking/index.ts

・説明は開発会社がコードに書いたままです（多くは英語。teastia は翻訳しません。自己申告と同じ扱い）

・「中身」は、道具の処理と、そこから呼んでいる同じアプリ内の関数を 2 段先までたどり、teastia の一覧（teastia effects: 消す・実行する・払う・外に出す・外のサービスに書く・外向きの通信、89 の書き方）に当たるものを挙げています。一覧に無い書き方は見つけられません。「人が承認・確認するコード」は、あるかどうかまでで、効いているかは人が確かめます

・「危ない処理は見つからず」は、呼んでいる関数の 2 段先まで読んだ結果です

ADOPTION ASSESSMENT

導入判定書 | 導入条件・確認事項

CONDITIONS FOR ADOPTION

| 導入するための条件

01	4・該当	道具 edit_file が ファイルを消す（道具が呼んでいる関数の中で。filesystem/lib.ts 341 行目、fs.unlink）、道具 write_file が ファイルを消す（filesystem/lib.ts 216 行目、fs.unlink）。人が承認・確認するコードなし。 直し方: 人が承認・確認する仕組みを挟む／その道具を AI から外す／権限を絞る（詳しくは Fix Pack の CAP-01）
02	6・条件つき	ログインの仕組みが見当たらない。詳しく: 認証ライブラリが依存に無く、質問票 Q-identity-1 も未回答。認証の仕組みを確認する
03	7・条件つき	部品の版が固定されていない（ロックファイルが無い）。詳しく: 版が固定されておらず、照合結果も再現しない
04	8・条件つき	利用回数・量の上限が見当たらない。詳しく: レート制限のパッケージが依存に無く、質問票 Q-ops-2 も未回答。上限の有無を確認する
05	8・条件つき	動きを記録する仕組み（監視・ログ）が見当たらない。詳しく: 監視・ログのパッケージが依存に無い。障害と誤動作をどう検知するかを確認する

OPEN ITEMS

| 確認が必要なこと

01	2	質問票の「許可した送り先の一覧」の回答待ち。詳しく: 2 件の送信先がある（modelcontextprotocol.io, raw.githubusercontent.com）。このうち送ってよいものを質問票 Q-egress-1 に
02	3	AI 会社を機械で見つけられなかった。詳しく: AI 事業者を機械で見つけられなかった。AI 機能の有無と SDK を質問票で確認し、未検査範囲に書く
03	6	質問票の「ログインなしで AI を使えるか」の回答待ち
04	7	部品を危険リスト（OSV）と照合していない。詳しく: OSV と照合していない。teastia osv で応答を取り、--osv で渡す
05	8	質問票の「AI を止めるスイッチ」の回答待ち
06	8	質問票の「障害時の連絡先と止め方の文書」の回答待ち

ADOPTION ASSESSMENT

導入判定書 | 質問票・未検査範囲

QUESTIONNAIRE RESPONSES

| 質問票の答え

番号 / No.	聞いたこと	答え
Q-secrets-1	鍵の保管場所	未回答
Q-egress-1	許可した送り先の一覧	未回答
Q-providers-1	契約している AI 会社の一覧	未回答
Q-cap-1	AI が許可なしに消す・実行する・払う経路があるか	未回答
Q-cap-2	AI が許可なしにデータを外に出す経路があるか	未回答
Q-identity-1	ログインの仕組み	未回答
Q-identity-2	ログインなしで AI を使えるか	未回答
Q-ops-1	AI を止めるスイッチ	未回答
Q-ops-2	利用回数・量の上限	未回答
Q-ops-3	障害時の連絡先と止め方の文書	未回答

答えは自己申告です（機械では確かめていません）。「分からない」は未回答と同じ扱いで、判定は「判定できない」のままです。質問票は teastia interview --paper で出せます。

OUT OF SCOPE

| この紙で見えていないこと（未検査範囲）

- ・ python (13 files) のファイルは読んでいない（teastia は JavaScript / TypeScript しか読みません）
- ・ アプリの版（commit）が分からなかった（.git が無い）。質問票で版を確認します
- ・ 部品の一覧（ロックファイル）が無く、部品の版が固定されていない
- ・ 部品を危険リスト（OSV）と照合していない
- ・ AI の道具の中身は、teastia の一覧（teastia effects）にある書き方だけを、呼んでいる関数の 2 段先まで読みました。一覧に無い書き方・3 段目より先・実行時にしか決まらない呼び先は見えていません

ADOPTION ASSESSMENT

導入判定書 | 調べた記録

INSPECTION RECORD

| 調べた記録

調べたもの	(名前の無いアプリ: 設定ファイル package.json に名前がありません)。言語 ts
検査モジュール	teastia 3.6.0 (お客様の環境の中だけで動き、コードは外に出しません)
AI 探索	未実施 (teastia ai の候補による読み直しは行っていません)
チェック 28 個の内訳	該当 1 / 条件つき 6 / 該当なし 15 / 判定できない 6。細かい根拠 (ファイル名・行番号) は rules.json にあります
検査日	2026-08-23
検査した範囲	指定したフォルダ全体 (72 ファイル)

DISCLAIMER

| この紙の位置づけ

この紙は、決めた範囲を、その日に調べた記録です。「絶対に安全」を保証するものではありません。

This document is a record of what was inspected, within a defined scope, on the stated date. It is not a guarantee of safety, nor a certification of conformity to any standard.

ISSUED

2026-08-23

INSPECTED BY

teastia 3.6.0

SIGNATURE