

FlashDesk セキュリティの説明 — AIに操作させるとき

まず押さえる点

1. **AI連携は初期OFF**：MCPはAIツールが動く 端末側のFlashDesk設定でONにしたときだけ使える。AI Workspaceはリモート端末側で許可されている場合だけ使える。
2. **承認は人の接続と同じ**：AI経由で開いた接続も、リモート端末側の承認またはパスワードを通る。
3. **ネットワークに公開されない**：MCPサーバーはローカルの標準入出力で通信し、ネットワークには公開されない。FlashDeskが起動していなければ要求はエラーになり、勝手に何かを起動しない。
4. **画面は隠れない**：AI経由のセッションでも、リモート画面ウィンドウは通常どおり表示される。

記録

- Proの管理画面でセッションログを確認できる。

通信

- 画面と操作の通信はセッションごとに暗号化（ECDH P-256／HKDF-SHA256／AES-256-GCM）。直接接続を優先し、つながらない場合は中継経由でも暗号化されたまま。
- 専用経路モード（Pro）で通信を決まった経路に限定できる。

データの扱い

- サーバログは30日で自動削除、SSHトンネルのデータ内容はマスク。端末の秘密鍵はサーバに保存しない。決済情報は決済事業者が扱う。

脆弱性報告

- お問い合わせページから件名に [Security] を付けて連絡。