

MCPAIエージェント 導入前セキュリティチェック

限データ承認ログを、導入前に一度整理するためのシート

使い方 該当する項目にチェックを入れ、空欄は者と期限を決めてください。すべてを一度に解決する必要はありません。

接と限

- ☐ 接するサービスと操作（む作る更新削除）を一にした
- ☐ AI用アカウントと認情報を用意した
- ☐ 必要な範だけに限を絞り、まずはみ取り用にした
- ☐ 外部サービスへの送信公開削除は人の承認が必要になっている

データと安全

- ☐ 公開情報社限定個人情報機密情報を分類した
- ☐ 外部から取得した文章を命令として行しない設計にした
- ☐ 本番ではなくダミ匿名化データでした
- ☐ AIが判できないときに推測せず停止するルールがある

運用と復

- ☐ AIの指示照データ行結果を後から確認できる
- ☐ 異常時にAPIキや接を停止する方法が分かる
- ☐ 退職異動時の限削除が決まっている
- ☐ 連携先や限を定期的に見直す予定がある

最初は「み取り用+人の確認」で始め、メル送信金理公開更新などの自動行は、後に範をげます。

相談メモ

者	確認日
---	-----