

個人情報保護・IT部門向けチェックリスト

Merlin ProjectでのAIアシスタントの利用を検討している個人情報保護の責任者およびIT部門向けの資料です。MCPサーバーの仕組み、組織の外に出るデータ、プロジェクトを共有する前に確認すべき点をまとめています。

1 MCPサーバーの概要

サーバーはどこで動作しますか？	ユーザーのMac上で、Merlin Projectの一部としてローカルに動作します。クラウド上にMerlinのサーバーはありません。
ネットワークからアクセスできますか？	いいえ。サーバーにはWebアドレスがなく、ネットワークからのアクセスも受け付けません。同じMac上で動作するAIアシスタントだけが接続できます。
AIはデータを変更・削除できますか？	いいえ。サーバーは読み取り専用です。サーバー経由でデータを変更、作成、削除することはできません。
どのプロジェクトが見えますか？	ユーザーが「AIツール」で明示的に共有したプロジェクトだけです。共有しない限り、AIはどのプロジェクトも参照できません。
共有は取り消せますか？	はい。いつでもプロジェクトごとに取り消せます。チェックを外すと、すぐに参照できなくなります。
アクセス中かどうか分かりますか？	はい。共有が有効な場合は「AIツール」アイコンが塗りつぶし表示になり、AIアシスタントの接続中は青色で強調表示されます。
Macの外に出るものは何ですか？	AIアシスタントが行った問い合わせの結果です。原則として、共有したプロジェクトのあらゆる情報が含まれる可能性があります。
データはどこに送られますか？	利用しているAIアシスタントの提供事業者です。たとえばClaudeを使う場合はAnthropicです。その事業者の利用条件が適用されます。

2 データの流れ

ユーザーは共有したプロジェクトについてAIアシスタントに質問します。アシスタントは必要なデータを自ら判断し、多くの場合は複数回に分けてMCPサーバーに問い合わせます。Merlin Projectは各問い合わせをローカルで処理し、アシスタントがその結果を提供事業者の言語モデルに渡して回答を生成します。その際、最終的な回答に関係しないデータが送信されることもあります。したがって管理のポイントは個々の項目ではなく、プロジェクトの共有そのものにあります。

3 AI提供事業者と契約

以下の項目はMerlin Projectではなく、組織で利用するAIアシスタントに関するものです。

- ☐ 提供事業者と利用プランが社内で承認されている
個人向けプランと法人向けプランでは、条件が大きく異なることがよくあります。
- ☐ データの取扱いに関する契約を締結している
個人データを提供する場合は、個人情報保護法などの適用法令に沿った対応が必要です。
- ☐ データの保存場所と外国への移転を確認している
外国にある第三者への提供に当たる場合は、その根拠と必要な手続きを記録します。
- ☐ モデルの学習へのデータ利用が除外されている
利用プランまたはアカウント設定で除外し、書面で確認します。
- ☐ チャットの保存期間と削除方法を把握している

-
- ☐ アカウントを一元管理している
管理コンソールなどを使い、アクセス権をいつでも取り消せるようにします。

4 プロジェクトと利用ルール

-
- ☐ 共有してよいプロジェクトが決まっている
-
- ☐ 人名を含むプロジェクトを確認している
リソースやメモに含まれる氏名は個人情報です。
-
- ☐ 特に機微な情報を除外している
給与、人事評価、健康情報など。内容を整理したコピーを共有するか、ローカルモデルを使用します。
-
- ☐ 顧客の機密情報を確認している
秘密保持契約により、AI提供事業者への提供が禁止されている場合があります。
-
- ☐ 従業員がルールを理解している
必要なプロジェクトだけを共有し、作業後は共有を解除します。
-
- ☐ 社内の取扱記録を更新している
個人データの取扱状況を社内の台帳などに記録します。
-
- ☐ リスク評価の要否を確認している
データの種類や量、適用法令に応じて判断します。

5 ITと運用

-
- ☐ MCPサーバーを含むバージョンのMerlin Projectがインストールされている
-
- ☐ AIアシスタントが同じMac上でローカルに動作している
この場合にのみ、MCPサーバーに接続できます。
-
- ☐ AIアシスタントの外向き通信を考慮している
ローカルモデルを使わない場合は、ファイアウォールやプロキシで提供事業者への接続を許可する必要があります。
-
- ☐ 機微なプロジェクト向けにローカル言語モデルを検討している
たとえばLM Studioを使えば、プロジェクトのデータはMacの外に出ません。ただし、ローカルモデルは一般に性能が劣ります。

6 確認結果

メモ・未解決の事項:

確認者

日付

署名

詳しくはMCPドキュメント (projectwizards.net/documentation/mcp) をご覧ください。本チェックリストは技術的な参考資料であり、法的助言ではありません。