

根拠付録 | 公開見本の補足

本体2ページとは別冊です。実案件の付録・対象範囲は着手前に合意します。改訂確認用。

対象版と根拠の位置

microsoft/agent-framework @ 95e711a6280d0ed7bafa5bafb8ff38eba4cffd3e
python/samples/03-workflows/human-in-the-loop/agents_with_approval_requests.py

根拠	行・関数	ソースで確認できること
M-S1	L116-121 read_historical_email_data	履歴メール読取に always_require を指定。
M-S2	L178-186 send_email	to・subject・bodyを受け取る always_require の関数。待機して成功文字列を返す模擬送信。
M-S3	L226-255 main / Agent / WorkflowBuilder	Agentへ履歴読取・送信ほかのToolを渡し、前処理からAgent、終了処理へ接続。
M-S4	L269-290 approval request loop	要求の型と function_call の存在を検査。関数名と解析した引数を表示し、request_idごとに approved=True を返す。
M-S5	L264-297 workflow.run	初回実行と応答を渡す再開処理。承認要求がなくなるまでループし、最後にAgentの出力を表示。

承認から送信へ、どこまで追えるか

位置	コード上の接続	読み取れること
L178-186	send_email(to, subject, body)	承認必須の関数として登録。実メール配送は行わない。
L282-284	function_call.parse_arguments()	承認要求の関数名と引数を表示する。
L286-290	request_id / approved=True	デモ用の自動承認応答を要求IDへ対応付ける。
L292-293	workflow.run(responses=responses)	応答を渡して再開する。SDK内部の保持・照合方式は対象外。

要求IDに承認応答を対応付ける処理は読めます。しかし、実送信アダプターが存在しないため、承認内容と最終配送要求の同一性はここでは確認できません。採用先は、照合責任を置く地点と、照合する内容・主体を決めます。

既存のSDK内部や採用先アダプターに同等の制御があれば、追加実装せずその根拠を確認する判断も可能です。

ソース参照: https://github.com/microsoft/agent-framework/blob/95e711a6280d0ed7bafa5bafb8ff38eba4cffd3e/python/samples/03-workflows/human-in-the-loop/agents_with_approval_requests.py

M-F1 承認者と有効期間を定める

根拠: M-S4 / 決める時点: 導入前

ソースの事実	承認要求を表示した後、すべて approved=True へ変換している。
推論	この応答処理だけでは、業務で権限を持つ人が有効期間内に承認したと説明できない。
代替説明	自動承認は明記されたデモ目的。採用先UIや認証基盤に本人・権限・期限確認が実装される可能性がある。
必要な制御条件案	承認の主体・役割・対象業務・時刻・期限・取消状態を固定し、欠落・拒否・失効時は送信要求を発行しない。
確認すべき問い	無権限・期限切れ・拒否済みの承認を、送信要求の発行条件から除外できるか。
主張できないこと	Microsoft製品に本人確認機能がないという主張。
未観測範囲	認証・承認UI・権限失効・並行承認。

M-F2 承認対象と送信要求を一つに束ねる

根拠: M-S2, M-S4 / 決める時点: 導入前

ソースの事実	送信引数は to・subject・body。承認ループは関数名と解析済み引数を表示し、request_id に応答を対応付ける。
推論	表示と応答の対応は確認できるが、実配送要求まで同じ内容が固定されることは対象ファイルだけでは立証できない。
代替説明	SDKが呼出しを不変に保持する可能性や、送信アダプターが同一性を検査する可能性がある。
必要な制御条件案	承認対象にTool・宛先・件名・本文・送信主体・業務範囲を結び付け、外部要求を構成する地点で照合する。
確認すべき問い	承認した要求と最終送信要求の、識別子・内容・送信主体を同じ対象として照合できるか。
主張できないこと	誤送信や承認転用が実際に発生したという主張。
未観測範囲	SDK内部の保持方式、配送アダプター、CC/BCC・添付。

M-F3 承認後の意味変更を再承認へ戻す

根拠: M-S2, M-S4, M-S5 / 決める時点: 導入前

ソースの事実	承認対象の引数を表示して応答を返し、workflow.runへ渡す。承認後変更の扱いを規定する業務処理はこのファイルにない。
推論	宛先展開や本文加工を後段に追加するなら、承認を失効させる変更を先に定める必要がある。
代替説明	対象SDKが引数の書換えを許さない可能性がある。追加アダプター側で再承認を実装する場合もある。
必要な制御条件案	宛先・本文等の意味を確定してから承認する。承認後の意味変更は旧承認を無効化して再承認し、意味を変えない加工の扱いは採用先が定める。
確認すべき問い	承認後の意味変更を検出し、変更後全体の再承認へ戻せるか。
主張できないこと	当該サンプルで変更攻撃が成功するという主張。
未観測範囲	添付・署名追加・テンプレート展開・宛先正規化。

M-F4 結果不明時の再送条件を定める

根拠: M-S2, M-S5 / 決める時点: 実送信接続前

ソースの事実	send_emailは待機後に固定の成功文字列を返す。配送要求IDや実サービス受付結果は、この関数にはない。
推論	この成功文字列を実送信完了の証拠へ流用できない。実配送でタイムアウトした際は未送信と区別して扱う必要がある。
代替説明	模擬関数なので配送の失敗・重複を表さない。実サービスの冪等性機能が重複を防ぐ可能性がある。
必要な制御条件案	未送信・受付済み・結果不明・配達結果を区別する。結果不明は照会・保留を基本とし、重複防止が保証される範囲の再試行条件を採用先が定める。
確認すべき問い	受付結果が不明なとき、重複作用を避ける条件と再送判断の責任者が定まっているか。
主張できないこと	SDKが二重送信するという主張。
未観測範囲	配送事業者の保証、配達完了、SDK内部の再試行。

M-F5 送信結果と証拠の充足状態を分ける

根拠: M-S2, M-S4, M-S5 / 決める時点: 実送信接続前

ソースの事実	要求詳細とAgent最終出力をprintする。模擬送信は固定文字列を返す。
推論	画面表示やAgentの自然文だけでは、承認した要求と外部受付を後から照合できるとは限らない。証拠欠落から送信失敗を推定せず、結果状態と証拠の充足状態を分ける必要がある。
代替説明	SDKのトレースや採用先の監査ログが別途記録している可能性がある。
必要な制御条件案	承認・照合判断・送信試行・受付結果を同じ識別子群へ結び付ける。送信結果と証拠不足を別々に表示し、閲覧権限・保持方針を定める。
確認すべき問い	送信の結果状態と、承認から受付までを裏付ける証拠の充足状態を分けて説明できるか。
主張できないこと	ログが製品全体に存在しないという主張。
未観測範囲	トレース保存、改変対策、保持・削除、実受信。

前提・主張範囲・次工程

前提: 実メール送信へ接続し、人間承認と照合可能な送信履歴を業務要件に含める採用構成を想定します。

- ・ソースを静的に読んだ結果であり、対象SDKやサンプルを実行していない。
- ・実顧客の採用済み方針、稼働環境、非公開資料、運用ログは受領していない。
- ・必要条件は弊会の提案。対象プロジェクトが同じ業務要件を約束しているとの主張ではない。
- ・最新バージョンや製品全体への一般化、脆弱性・安全性・適合性の判定は行わない。

各所見は採用先への設計提案です。詳細な検査手順、具体的な障害注入、実行結果は本付録に含めません。実装後の検査が必要な場合は、対象と条件を別途合意します。

公開見本には採用先がないため、所見の採否は未決定です。各所見は設計提案であり、実行検査結果ではありません。旧版の内容確認記録は保持し、改訂版は公開前の人間確認に回します。

AIの支援で作成し、根拠・推論・主張範囲を人が確認する工程を設けています。作成と助言は同一工程であり、この資料自体を独立第三者検証の結果とは扱いません。