

人間による内容確認済み | 所見採用は保留中 | 実行検査なし

メール送信の承認を実行まで結び付ける

Microsoft Agent Framework 制御設計レビュー

公開情報を対象に弊会が独自に作成したレビューサンプル候補。対象企業・対象プロジェクトから依頼・承認・認定を受けたものではありません。

レビュー情報	対象
レビューID / 版	CRS-PUB-MAF-EMAIL-20260929-001 / v0.1
方法 / レビュー日	STATIC_SOURCE / 2026-09-30
Repository / commit	microsoft/agent-framework @ 95e711a6280d0ed7bafa5bafb8ff38eba4cffd3e
Path scope	python/samples/03-workflows/human-in-the-loop/agents_with_approval_requests.py

EXECUTIVE SUMMARY

承認要求の生成と応答の接続を学べるサンプルです。一方、送信処理は模擬実装で、承認応答も自動です。業務へ採用する際は、承認者の権限、承認内容の固定、変更時の再承認、結果不明時の再送条件、送信証跡を追加の採用条件として決める必要があります。これは対象1ファイルの静的レビューに基づく提案です。

保護する作用とレビュー上の問い

実メール送信へ置き換えた場合の送信サービスへの要求発行。レビュー対象の send_email 自体は模擬実装。
承認した宛先・件名・本文を、実際に外部送信へ進む要求とどの条件で同一に保つか。

主な所見候補		
M-F1	承認者と有効期間を定める	採用保留
M-F2	承認対象と送信要求を一つに束ねる	採用保留
M-F3	承認後の内容変更を再承認へ戻す	採用保留
M-F4	結果不明時の再送を保留する	採用保留
M-F5	承認から作用までの証跡を残す	採用保留

状態欄は所見採用の保留を示します。根拠・推論・主張範囲は人間確認済みで、実行試験の可否や脆弱性判定ではありません。

人間による内容確認済み | 所見採用は保留中 | 実行検査なし

実装へ渡す条件と検証の問い

以下は人間確認済みの制御条件案です。所見採用は保留中で、既存実装の欠陥認定や実行検査結果ではありません。

制御条件案	実装後に確かめる問い
M-F1 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。	無権限・期限切れ・拒否済みの承認応答でも送信要求が模擬受付境界を越えるか。
M-F2 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。	宛先Aへの承認を、別要求IDまたは別主体の宛先Bへの要求に転用できるか。
M-F3 送信内容を変える処理を承認前に完了する。承認後の意味変更は旧承認を無効化し、変更後全体を再承認する。	承認後に本文・件名・宛先を変更しても、変更前の承認だけで送信要求が発行されるか。
M-F4 未送信・受付済み・結果不明を分ける。結果不明は自動再送せず照会へ戻し、同一業務作用の重複防止条件を固定する。	模擬受付成功後に応答を失わせたととき、同じ業務要求の再試行で二度目の受付が生じるか。
M-F5 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。秘密値を避け、必要内容の閲覧権限と保持方針を定める。	承認ログまたは受付ログが欠けた場合でも、実送信成功を確定表示してしまうか。

主張上限

公開情報を対象に、実案件で使用するレビュー構造・成果物形式に沿って作成した公開サンプル候補。根拠と主張の対応・推論・主張範囲は人間による内容確認済み。所見採用は保留中であり、静的レビューを実行結果・認証・実行許可・公開許可へ昇格させない。

人間による内容確認済み | 所見採用は保留中 | 実行検査なし

対象ソースと根拠

対象版はmoving ref ではなくexact commit で固定。行番号は取得したUTF-8 原本の始まりです。

- M-S1 L116-121

python/samples/03-workflows/human-in-the-loop/agents_with_approval_requests.py / read_historical_email_data

履歴メール読取に always_require を指定。
- M-S2 L178-186

python/samples/03-workflows/human-in-the-loop/agents_with_approval_requests.py / 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

python/samples/03-workflows/human-in-the-loop/agents_with_approval_requests.py / 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

python/samples/03-workflows/human-in-the-loop/agents_with_approval_requests.py / 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

python/samples/03-workflows/human-in-the-loop/agents_with_approval_requests.py / 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。

人間による内容確認済み | 所見採用は保留中 | 実行検査なし

所見と制御条件の対応

各行の根拠と推論を分け、所見採用は保留中のままです。

M-F1 承認者と有効期間を定める

Fact: 承認要求を表示した後、すべて `approved=True` へ変換している。

Inference: 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。

M-F2 承認対象と送信要求を一つに束ねる

Fact: 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。

Inference: 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。

M-F3 承認後の内容変更を再承認へ戻す

Fact: 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。

Inference: 本文化・宛先展開などを後段に追加するなら、どの変更で承認を失効させるかを先に決める必要がある。

M-F4 結果不明時の再送を保留する

Fact: `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ない。

Inference: 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。

M-F5 承認から作用までの証拠を残す

Fact: 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。

Inference: 画面表示やAgent の自然文だけでは、誰の承認でどの要求が外部受付されたかを後から照合する証拠として不足する。

人間確認済みなのは根拠と主張の対応・推論・主張範囲です。正式所見採用、実行検査、安全性保証、認証、実行許可ではありません。

人間による内容確認済み | 所見採用は保留中 | 実行検査なし

M-F1 承認者と有効期間を定める

内容確認済み / 所見採用は保留中 / 根拠: M-S4

ソース事実

承認要求を表示した後、すべて `approved=True` へ変換している。

推論と所見候補

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。

将来の検証質問

無権限・期限切れ・拒否済みの承認応答でも送信要求が模擬受付境界を越えるか。

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。

人間による内容確認済み | 所見採用は保留中 | 実行検査なし

M-F2 承認対象と送信要求を一つに束ねる

内容確認済み / 所見採用は保留中 / 根拠: M-S2, M-S4

ソース事実

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。

推論と所見候補

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。

将来の検証質問

宛先Aへの承認を、別要求IDまたは別主体の宛先Bへの要求に転用できるか。

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。

人間による内容確認済み | 所見採用は保留中 | 実行検査なし

M-F3 承認後の内容変更を再承認へ戻す

内容確認済み / 所見採用は保留中 / 根拠: M-S2, M-S4, M-S5

ソース事実

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。

推論と所見候補

本文文化・宛先展開などを後段に追加するなら、どの変更で承認を失効させるかを先に決める必要がある。

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

送信内容を変える処理を承認前に完了する。承認後の意味変更は旧承認を無効化し、変更後全体を再承認する。

将来の検証質問

承認後に本文・件名・宛先を変更しても、変更前の承認だけで送信要求が発行されるか。

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。

人間による内容確認済み | 所見採用は保留中 | 実行検査なし

M-F4 結果不明時の再送を保留する

内容確認済み / 所見採用は保留中 / 根拠: M-S2, M-S5

ソース事実

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ない。

推論と所見候補

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・結果不明を分ける。結果不明は自動再送せず照会へ戻し、同一業務作用の重複防止条件を固定する。

将来の検証質問

模擬受付成功後に応答を失わせたととき、同じ業務要求の再試行で二度目の受付が生じるか。

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。

人間による内容確認済み | 所見採用は保留中 | 実行検査なし

M-F5 承認から作用までの証拠を残す

内容確認済み / 所見採用は保留中 / 根拠: M-S2, M-S4, M-S5

ソース事実

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。

推論と所見候補

画面表示やAgent の自然文だけでは、誰の承認でどの要求が外部受付されたかを後から照合する証拠として不足する。

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。秘密値を避け、必要内容の閲覧権限と保持方針を定める。

将来の検証質問

承認ログまたは受付ログが欠けた場合でも、実送信成功を確定表示してしまうか。

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。

人間による内容確認済み | 所見採用は保留中 | 実行検査なし

主張上限と次工程

未観測範囲と成果物の来歴

- ・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。

人間による内容確認

根拠と主張の対応、推論・代替説明、主張上限を人間確認済み。所見採用は保留中で、正式所見・実行検査結果・安全性保証・認証・実行許可には昇格していません。確認時刻はCRS記録に保持します。

AI支援と助言関与

OpenAI / ChatGPT Work 上のAIが資料読解、所見候補、改善条件案、文書生成と体裁確認を支援。作成と助言は同一工程で、独立第三者レビューではありません。

主張上限

公開情報を対象に、実案件で使用するレビュー構造・成果物形式に沿って作成した公開サンプル候補。根拠と主張の対応・推論・主張範囲は人間による内容確認済み。所見採用は保留中であり、静的レビューを実行結果・認証・実行許可・公開許可へ昇格させない。