AIエージェントプラットフォーム

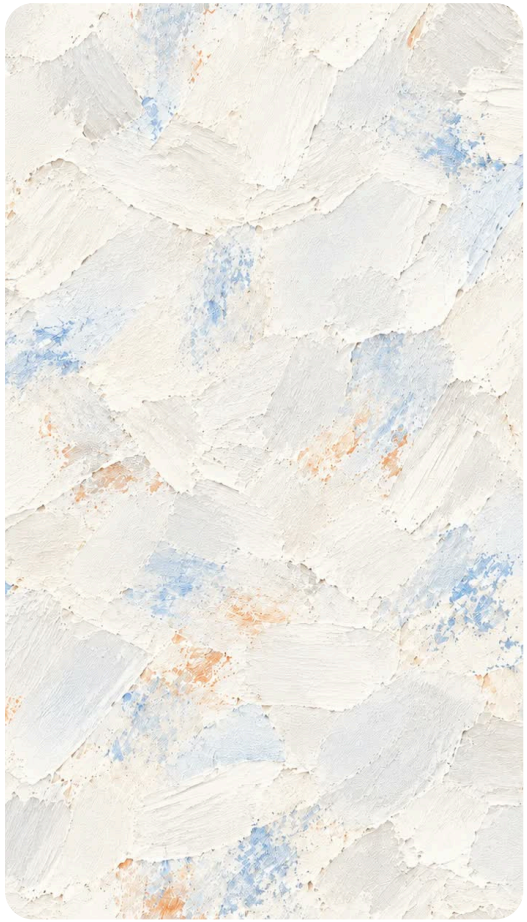
AgentWorks

AIエージェント構築・運用プラットフォーム

閉域網でも動作するノーコードのAgentic AIプラットフォーム。
機関の業務に合うエージェントを**自ら作り、運用**します。



このパンフレットは、セキュリティを重視する機関・企業がAIを導入する際に実際に直面する4つの課題から始まります。課題ごとにAgentWorksがどう解決するのか、そして実際の導入事例と始め方までを順にまとめました。



はじめに

はじめに	AI導入を前にした4つの課題	p.03
プラットフォーム	AgentWorksは機関の中のエージェント工場	p.04
構造	4つの層とひとつの関門	p.05

4つの課題と解決

課題 01	ネットワーク分離・内部規程で商用AIを使えない	p.06
課題 02	業務ごとに開発を発注するには予算と期間が重い	p.09
課題 03	汎用AIは機関の規程・文書・DBを知らない	p.12
課題 04	誰がどのAIに何を送ったか証明できない	p.14

事例と導入

導入事例	異なる機関が同じプラットフォームで働いています	p.17
導入の流れ	小さく始めて広げていく導入の流れ	p.19
お問い合わせ	試験導入のご提案・導入のお問い合わせ	p.20

よく伺う課題

セキュリティを重視する機関がAI導入で直面する4つの課題

AIが必要だという点には誰もが同意します。つまずくのはその先です。規程、人材、データ、そして責任です。

いま一番気になる課題から押してみてください。AgentWorksがその課題をどう解くかのページへ移動します。



課題 01	「ネットワーク分離と内部規程のため、商用AIを使えません。」	社内設置・自社モデル →
課題 02	「業務ごとに開発を発注するため、予算と期間が負担です。」	ノーコードビルダー →
課題 03	「汎用AIは、私たちの内部規程・文書・DBを知りません。」	データ連携 →
課題 04	「誰がどのAIにどの資料を送ったのか確認できません。」	二重の関門 →

機関の中のエージェント工場

AIが答えるだけで終わらず、機関の中で働くようにします。

AIエージェント構築・運用プラットフォーム

閉域網でも動作するノーコードのAgentic AIプラットフォームです。ひとつのチャットボットではなく、エージェントを作り続けるための基盤です。

01 · 構築 · 運用

現場が作って運用します

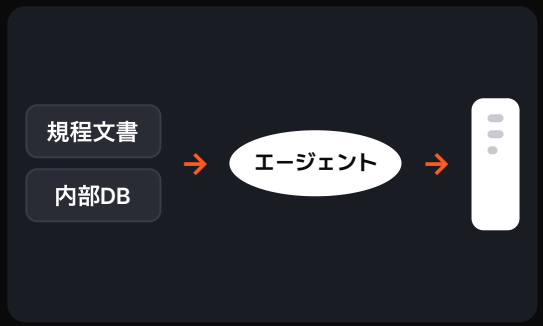
言葉で指示するとAIが作業を設計し、予約・キューで人手なしに実行します。



02 · 連携

機関の資料で働きます

内部文書 · DBから根拠を探し、システムとツールで成果物まで作ります。



03 · ガバナンス · セキュリティ

統制し、記録します

モデル · 権限 · 上限を決め、使用量と監査記録を機関の中に残します。



改善を繰り返す 利用記録と品質チェックの結果で作業を直し、業務ごとにエージェントを増やしていきます。

4通り	**10種**	**15種**	**9種**	**2重**	**GS認証**
エージェントの作り方	内蔵ツール	事務ツール	データコネクタ	AI呼び出しの関門	韓国の公共調達で購入可能

プラットフォームの構造

4つの層とひとつの関門で成り立つプラットフォーム

User Environment
使う場所 · 社員とシステムの入口

- **Webチャット** 社員が直接指示
- **既存の業務システム** Open API · 予約実行
- **新サービス** 専用アプリにAIを搭載

Agent Runtime
働く場所 · 実行エンジン

- **実行エンジン** 計画 → 実行 → 確認
- **サブエージェント** 複雑な仕事を分担
- **予約 · キュー** 人手なしで実行
- **安全装置** 反復 · 時間 · 予算 · 個人情報

課題 04

Agent Builder
作る場所 · ノーコード

- **作業のAI設計** 言葉で指示すると手順を生成
- **スキル** 業務ルールをまとめて再利用
- **文書書式** 機関の書式を登録
- **品質チェック** 正解例で採点

課題 02

Enterprise Connection
つなぐ場所 · 根拠とツール

- **資料庫** HWPなど文書の知識
- **データセット** DB · Excelへの問い合わせ
- **データコネクタ** 原本を自動同期
- **外部ツール** MCPで実際の業務を実行

課題 03

セキュリティ · 統制 機関の分離 · ロール権限 · 共有 · 委任 · 監査記録 · ログインロック

設置 社内設置（閉域網） · ハイブリッド · クラウド

AI Gateway · モデル · キー · 使用量の管理

- 部門別ゲートウェイ
- モデル · キー管理
- 使用量 · コストの記録
- クレジット上限

Egress Gateway
外部接続の単一経路 · 許可したアドレスだけに接続して記録 · 閉域網構成も可能

自社の小型モデル
機関内部のGPUサーバー

商用AI
許可時のみEgress経由

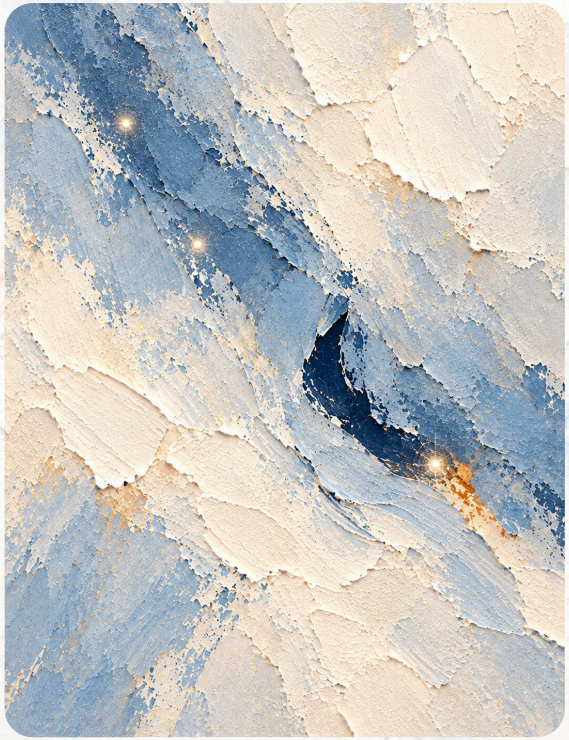
課題 01 課題 04

「課題」ボタンをクリックすると、その層が解く課題へ移動します。

課題 01 · 外部AI利用の制約

ネットワーク分離と内部規程のため、商用AIを使えません。

セキュリティを重視する公共 · 金融機関で最初に伺うお話です。



現場ではこんなことが起きています

AIは必要なのに道がふさがれている

ネットワーク分離とセキュリティ規程のため、インターネットの先にある商用AIへ業務資料を送れません。

禁止すると抜け道が生まれる

急ぎの業務が個人の端末やアカウントで処理され、かえって機関の統制の外に出ていきます。

自前の構築は重すぎる

機関の中にAIを入れるには、モデル · インフラ · 運用体制を一から揃える必要があります。

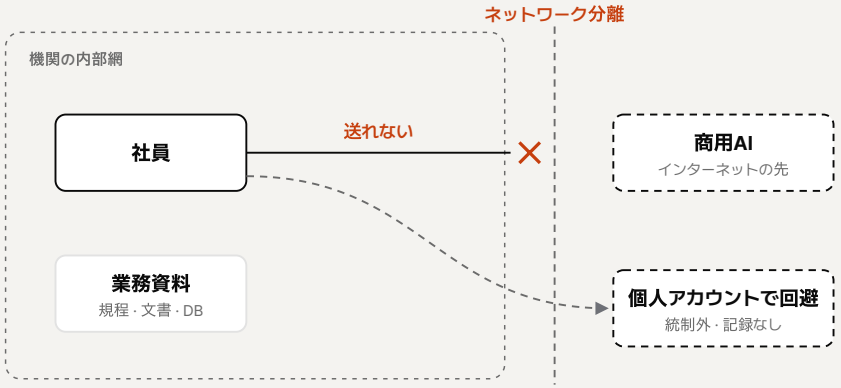
本当の不安 「セキュリティを理由にAI導入そのものを先送りし続けること」

AgentWorksの解決を見る →

解決 01 · 社内設置 + 自社AIモデル

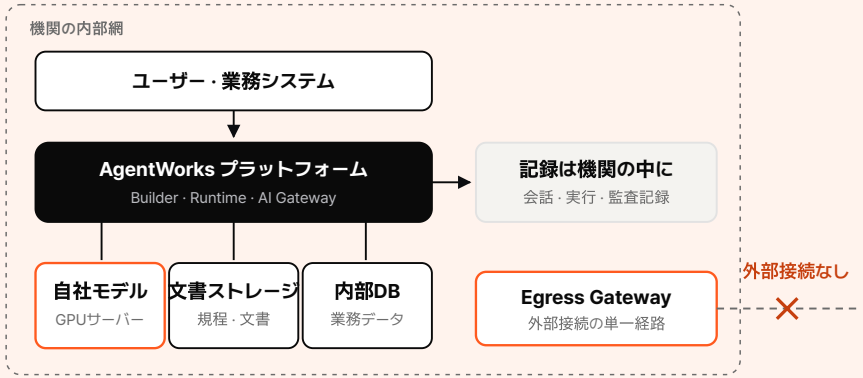
インターネットなしで、機関の中で最後まで動作します。

現状



内部網の外のAIは使えず、一部の業務は統制の外で回避されています。

AgentWorks導入後



会話 · 文書分析 · 作業実行を機関のGPUサーバーにある自社モデルで処理し、データと記録も機関の中に残します。

全工程を自社モデルで

会話 · 文書分析 · 作業実行を機関のGPUサーバーにある自社モデルで処理します。OpenAI互換方式なので、公開モデルをそのまま接続できます。

データと記録は機関の中に

文書インデックス · 会話 · 実行記録と監査記録を内部ストレージに保管し、機関（組織）単位でデータを分離します。

内部システムと内部網でつなぐ

DB · 共有フォルダ · SFTPはデータコネクタで同期し、既存の業務システムはOpen APIでエージェントを呼び出します。

外部接続はひとつの経路に

外部接続はEgress Gatewayの1か所にまとめます。許可リストを空にすれば、外部接続なしで運用できます。

お客様が得られること

- ✓ セキュリティ規程を守りながらAIを業務に使えます
- ✓ 閉域網構成ではデータと記録が機関の外に出ません
- ✓ モデルが変わってもプラットフォームはそのまま使えます

解決 01 · 機関の環境に合わせた設置

セキュリティ要件に合わせて設置方式を選べます。

社内設置（閉域網）

公共 · 金融

- インターネットなしで **自社モデル** で運用
- データ · 記録はすべて機関内部
- 許可リストを空にして外部を遮断



このような組織に
ネットワーク分離が必要な公共 · 金融機関

AIモデル	**機関のGPUサーバー**
データ · 記録	**機関内部**
外部接続	**なし**

ハイブリッド

機密度で使い分け

- 社内設置 + **一部の商用AI**
- 機密性の高い業務は内部モデルで
- 商用AIはEgressで許可先のみ



このような組織に
機密業務と一般業務が混在する機関 · 企業

AIモデル	**自社 + 許可した商用AI**
データ · 記録	**機関内部**
外部接続	**Egressの単一経路**

クラウド（SaaS）

迅速な試験導入

- 登録後 **すぐに利用**
- 試験導入後に社内設置へ移行
- 一般企業の業務に最適



このような組織に
まず効果を素早く確かめたい機関 · 企業

AIモデル	**商用AI**
データ · 記録	**クラウド**
外部接続	**インターネット**

お客様が得られること

- ✓ 機関のセキュリティ要件に合った方式を選べます
- ✓ 機密業務と一般業務を分けて運用できます
- ✓ クラウドで試験導入した後、社内設置へ移行できます

課題 02 · 開発人材の限界



業務ごとに開発を発注するため、予算と期間が負担です。

AIを業務に取り入れたい現場と情報システム部門が、ともに抱える悩みです。

現場ではこんなことが起きています

依頼は積み上がり、開発は進まない

部門ごとに任せたい業務はあっても、開発の人手と予算は限られ、順番待ちになります。

完成するころには業務が変わっている

要件を文書で伝えて結果を待つ間に業務のやり方が変わり、また発注し直します。

業務を知る人は直せない

業務を一番よく知る担当者はコードが分からず、自分で直したり改善したりする手段がありません。

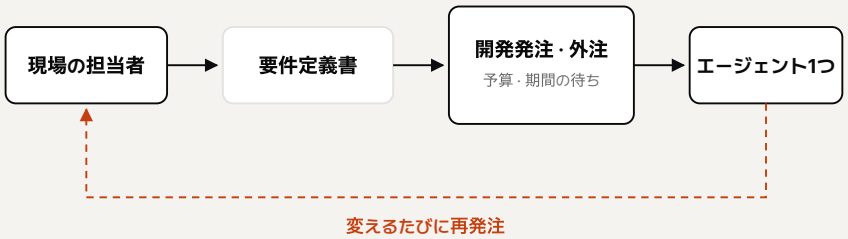
本当の不安　**「AI導入が、またひとつの開発案件になること」**

AgentWorksの解決を見る →

解決 02 · 現場が自ら作るノーコードビルダー

ひと言入力するだけで、毎週働くエージェントになります。

現状



業務をひとつ変えるだけでも、文書作成 · 発注 · 待ちをもう一度繰り返します。

AgentWorks導入後



担当者がひと言入力するとAIが作業として設計し、担当者は確認して直すだけです。

誰でも · 会話ですぐに

資料庫を指定して質問すれば、そのまま規程案内エージェントになります。

現場の担当者 · 言葉で設計

やることを文章で入力すると、AIが手順を設計し予約まで設定します。

業務の専門家 · スキルにまとめる

作成ルールと書式をスキルにまとめ、部門全体が同じ品質で使えます。

システム担当者 · Open API

専用アプリや他のシステムから作業をAPIで呼び出します。

お客様が得られること

- ✓ 別途の開発依頼や外注なしで始められます
- ✓ 業務が変われば担当者がすぐに直せます
- ✓ 部門全体が同じ基準と品質で使えます

解決 02 · 作り方の例

市民苦情の処理状況報告エージェントは、こう作ります。

担当者が入力した指示

「先週の苦情受付を種類別 · 部門別に集計し、処理の遅れと繰り返しの苦情を整理して週次報告書にして」

ステップ 1
指示の入力
欲しい結果を文章で書きます

ステップ 2
AIが計画を設計
照会 → 集計 → 遅延 · 反復の抽出 → 報告書

ステップ 3
資料の連携
苦情受付データセット + 苦情処理指針の資料庫

ステップ 4
予約
毎週月曜9時に自動実行

ステップ 5
結果
報告書（要約 · 表 · グラフ） · Word · PDF · メール通知

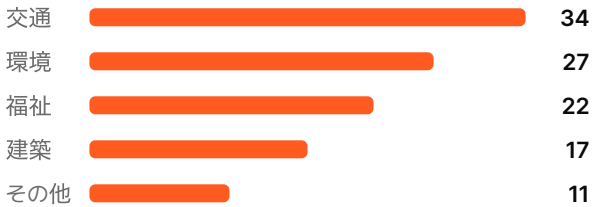
AIが設計した実行計画 · 例

1. 苦情受付データセットから先週の内容を照会
2. 種類別 · 部門別に件数を集計
3. 処理期限超過 · 同一申請者の繰り返しを抽出
4. 苦情処理指針から関連基準を確認
5. 週次報告書を作成 → 担当者にメール通知

週次 苦情処理状況 10月第3週 · 自動作成　メール送信済み

受付	処理完了	処理遅延	平均処理	繰り返し
128件	112件	9件	2.4日	4件

種類別の受付



要確認

処理期限超過	9件
同一申請者の反復	4件
指針違反の疑い	0件

出典 · 苦情受付データセット · 苦情処理指針

こんなエージェントも作れます
条項の根拠を示す規程問い合わせ
提案依頼書（RFP）分析
HWP文書の要約
言葉で聞く統計照会
定期報告書の自動作成
障害受付 · 原因分析
技術問い合わせの一次回答
音声から作る議事録
個人情報を隠して表示

画面の計画と報告書は、理解を助けるための例です。

課題 03 · 機関データ活用の難しさ



汎用AIは私たちの機関の内部規程・文書・DBを知りません。

AIを業務に使ってみた担当者が最初に感じる限界です。

現場ではこんなことが起きています

機関の文書を根拠に答えられない

規程や指針はHWP · PDFで蓄積されていますが、汎用AIはこれらの文書を根拠に答えられません。

どこから来た答えか分からない

どの規程 · どの条項に基づく答えなのかが見えず、そのまま業務には使えません。

データはシステムの中に閉じている

業務DBやExcelの数字を見るには、担当者が自分で抽出して整理する必要があります。

本当の不安 「結局、AIの答えを人がもう一度確認して直すこと」

AgentWorksの解決を見る →

解決 03 · 知識 · データ · システムの連携

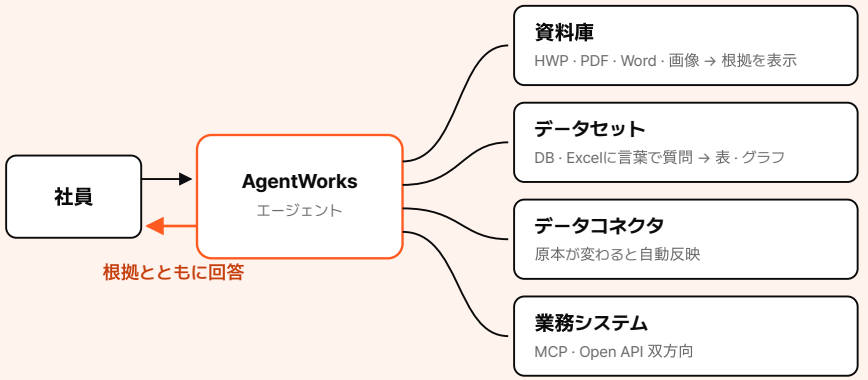
機関の文書 · DB · システムが エージェントの根拠であり手足になります。

現状



汎用AIは機関のデータを参照できず、結局担当者が探し直して確認します。

AgentWorks導入後



エージェントが機関の文書 · データ · システムから根拠を探し、ツールで成果物まで作ります。

資料庫 · 文書を知識に

PDF · Word · HWP · 画像（OCR）の文書を検索できる知識にし、回答ごとに根拠となる文書を表示します。

データセット · DBに言葉で質問

内部DB · Excel · CSVにSQLなしで質問すると、表とグラフで答えます。

データコネクタ · 自動反映

S3 · SFTP · 共有フォルダ · DB · Redmineなど9種のストレージを定期的に同期します。

外部ツール · 実際の業務を実行

内蔵ツール10種と、MCPでつないだ機関内部のツールで、照会 · 作成 · 送信まで処理します。

お客様が得られること

- ✓ 回答ごとに根拠文書をすぐに確認できます
- ✓ SQLを知らなくてもデータを表 · グラフで受け取れます
- ✓ 原本が変わると自動で反映されます

課題 04 · 統制と証跡の負担



誰がどのAIにどの資料を送ったのか、確認できません。

セキュリティ · 監査の担当者と管理者が、導入決定の直前に尋ねる質問です。

現場ではこんなことが起きています

利用履歴がばらばら

部門ごとに異なるAI · 異なるキーを使い、利用履歴全体を1か所で見られません。

個人情報がそのまま渡る

申請者の氏名 · 連絡先などの個人情報が、確認の段階なしにAIへそのまま入ることがあります。

コストと上限を決めにくい

どの部門がどれだけ使っているか分からず、予算を決めて守るのが難しくなります。

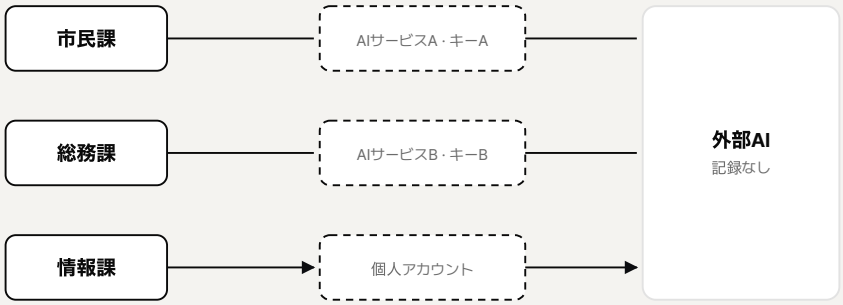
本当の不安 **「監査のときに証跡を出せないこと」**

AgentWorksの解決を見る →

解決 04 · AI Gatewayで一元化

AIの呼び出しは二重の関門で統制し、記録します。

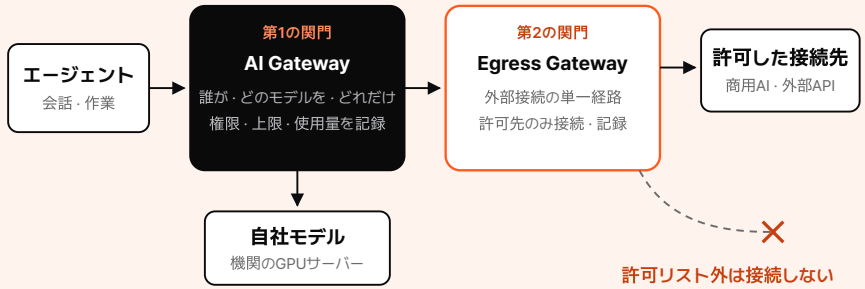
現状



利用履歴 · コスト · 送信記録がばらばら

部門ごとに異なるAIとキーを使い、誰が何を送ったのかを1か所で見られません。

AgentWorks導入後



すべての呼び出しが同じ2つの関門を通り、使用量と外部への接続が記録として残ります。

防ぐこと

許可していないAIサービスへの送信、権限のない部門のモデル利用、上限を超える利用を遮断します。

残すこと

モデル別 · ユーザー別の使用量、外部への接続、ログインと主要な操作を監査記録として残します。

部門別ゲートウェイ

グループごとにモデルとキーを指定し、無効にすれば即座に停止します。契約 · 期間 · ユーザー別のクレジット上限を設けます。

設定だけで適用するセキュリティ

機関単位のデータ分離、ロール別の権限 · 共有 · 委任、5回のログイン失敗でロック、セッション期限切れを標準で備えます。

お客様が得られること

- ✓ 誰が何を送ったのかを記録で証明できます
- ✓ 部門別の使用量とコストを1か所で確認できます
- ✓ 統制と証跡を開発なしで、設定だけで整えられます

解決 04 · 任せても安心できるように

エージェントが単独で働く間も、3つの安全装置が一緒に作動します。

実行の安全装置

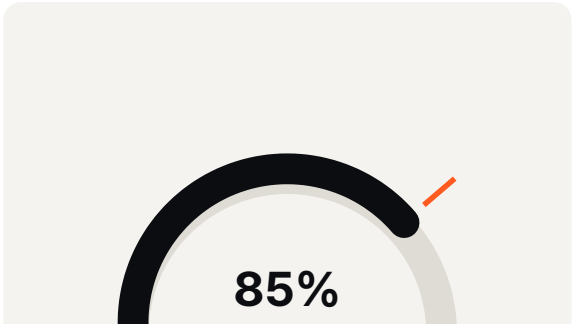
過剰な実行の防止



同じ動作の繰り返し、ステップ数の上限、
実行時間の上限を超えると**自ら停止**します。

予算 · 上限

コスト上限



作業別のトークン予算と、契約 · 期間 · ユーザーの
上限を超えると**新しい実行を遮断**します。

実行前のチェック

個人情報の保護



入力の段階で個人情報を検知し、
遮断するか隠してから実行します。

品質を
数字で確認

正解例の登録
よくある質問と必須 · 禁止条件を
ケースに

組み合わせ実行
モデル · 推論強度を変えて同じ
ケースを一度に

採点
ルール採点 · AI採点で合否を判定

比較 · 改善
合格率 · 点数 · 応答時間 · コスト、
回ごとの変更前後

取り消しのできない作業の担当者承認と、画面が変わっても続く自動復旧機能は準備中です。

導入事例

異なる機関が同じプラットフォームで働いています。

利用中

A社

公共向けAIコンサルティング

提案依頼書の分析・提案書作成

資料庫 / キャンバス / 文書書式

クラウド

利用中

B社

グループのITサービス企業

社内共通業務のAI

チャット / 資料庫 / 事務ツール

クラウド

構築中

C機関

公共・教育

教育情報網の障害受付・分析

Open API / 作業 / コネクタ

社内設置

試験導入

D社

ネットワーク機器メーカー

技術サポートセンターの自動化

資料庫 / 作業 / 個人情報の非表示

ハイブリッド

設計・構築予定

E機関

公共・エネルギー

大規模データの抽出・分析

データセット / 自社モデル

社内設置（閉域網）

導入形態マップ・セキュリティ要件が高いほど社内設置へ

クラウド
登録後すぐに利用
A社 B社

ハイブリッド
機密業務は内部・一部商用AI
D社

社内設置（閉域網）
自社モデル・外部接続なし
C機関 E機関

セキュリティ要件 低 ——— セキュリティ要件 高

共通点 業務もセキュリティ環境も異なりますが、すべて同じプラットフォームの上でエージェントを作り、運用しています。

お客様のご要望により、機関名は匿名で表記しています。状況は2026年10月時点です。

事例の詳細

事例で見る構築・連携・セキュリティの実際

C機関・公共・教育 **構築中・社内設置**

教育情報網の障害受付・分析

1,600件+ 根拠にする4年分の障害履歴

1. 教職員がログインなしにチャットで申告
2. 専用の受付アプリがOpen APIで作業を呼び出し
3. 類似事例を検索 → 原因候補・点検ガイド
4. 運用者が分析を見て判定・完了
5. 処理履歴が次の分析の参考資料に

経験ではなく機関の記録
類似事例から原因候補と点検方法を提示

処理期限の管理
業務時間基準で期限を計算・期限前に通知

使うほど蓄積される知識
処理完了と同時に参考資料へ追加

構築・運用	専用アプリがOpen APIで作業を呼び出し
連携	4年分の障害履歴を根拠に
ガバナンス・セキュリティ	5種のロール・地域単位の権限・IP・電話・パスワードの非表示

D社・ネットワーク機器メーカー

試験導入・ハイブリッド

技術サポートセンターの自動化

20万件 AIが検索・分析する過去の案件

1. 受付と同時に種類・重大度を分類し担当者へ通知
2. 類似案件の上位3件を根拠に一次対応案
3. ログを読んで原因候補を整理
4. エンジニアが確認してから反映
5. 処理結果を報告書とFAQに整理

最終判断は人
AIの結果はエンジニアが確認してから反映

既存の環境はそのまま
使っていたポータルとアカウント体系を維持

開発なしで有効にした機能
類似案件の検索・使用量制御・個人情報の非表示

構築・運用	一次対応案・自動分類の作業
連携	過去の案件20万件を検索
ガバナンス・セキュリティ	ロール権限・監査記録・個人情報の非表示・既存ポータルとアカウントはそのまま

E機関・公共・エネルギー **設計事例・構築予定**

大規模な閉域網データ分析

2万種以上

対象テーブル・数百TB・年間数万件の依頼

1. 分析依頼者が自然な言葉で質問
2. メタデータで必要な表だけを選びSQLを生成
3. 構文・実行計画の事前チェックで危険なクエリを遮断
4. 元データに読み取り専用で直接クエリ
5. 表・グラフと実行SQL・出典をあわせて提示

原則 1
データを移動しません

原則 2
メタデータで精度を高めます

原則 3
負荷・セキュリティの統制を最優先します

構築・運用	自然言語の依頼をSQL分析作業に
連携	データを移さず元データに直接クエリ
ガバナンス・セキュリティ	閉域網・自社モデル・時間・行数の制限・監査

導入の流れ

導入は小さく始めて広げていきます。

1 ご相談
業務とセキュリティ要件を確認します。

2 試験導入
代表的な業務1〜2つで効果を確かめます。閉域網での試験構成も可能です。

3 業務の選定・設計
エージェントにする業務と資料を整理します。

4 構築・教育
社内設置と担当者教育を行います。

5 展開
部門ごとにエージェントを追加します。

第1段階・試験
1部門・代表業務1〜2つ
市民課
効果がすぐ見える業務から始め、成果と運用方法を先に検証します。

第2段階・展開
部門ごとにエージェントを追加
市民課 総務課 情報化
検証済みの作業・スキルを他部門がそのまま使います。開発なしで部門別のエージェントを追加します。

第3段階・機関全体
機関の中のエージェント工場
市民 総務 情報化 監査 企画 +
部門ごとに作ったエージェントが同じ権限・上限・監査基準で運用され、管理者はAI Gatewayの1か所で管理します。

部門とエージェントの数は例です。

あわせて提供
教育・マニュアル・技術サポート

料金体系
設置方式・規模に応じてご相談

購入のお問い合わせ
VICS Technology

公共調達（韓国）
GS認証・調達購入が可能

次のステップ

貴社の実際の業務で 試験導入を ご提案します。

効果がすぐ見える業務1〜2つから始め、自社モデルで機関の中で検証し、その結果をもとに展開計画を一緒に立てます。

代表業務の選定
効果がすぐ見える業務1〜2つ

閉域網での試験構成
自社モデルで機関の中で検証

結果のご報告
効果と展開計画を整理

導入のお問い合わせ →

▶ デモ動画を見る



メール
sales@vicsnc.com

ウェブサイト
vicsnc.com