生成 AI の「情報漏洩リスク」と「社員の活用格差」を解消―chai+、企業向け「汎用 AI チャット」を提供

デフィデ株式会社（東京都港区、代表取締役：山本 哲也）は、法人向け AI サービス「chai+（チャイプラス）」の「汎用 AI チャット」機能を追加しました。生成 AI を業務に導入する企業では、社員ごとの活用スキルの差、個人契約ツールへの機密情報入力、部署ごとの AI 契約の乱立が課題となっています。本機能は、GPT・Claude・Gemini などの複数モデルを一つの環境で利用でき、業務別プロンプトテンプレートで利用を支援。入力・回答の両方を検査するガードレールと部署・役職別の権限・ログ管理により、生成 AI の利便性と企業のガバナンスの両立を支援します。

生成 AI は資料作成や文章要約、企画立案など幅広い業務で活用が進む一方、利用者のスキルや契約形態によって成果とリスクに差が生じています。特に、個人アカウントでの利用が先行すると、企業が入力情報や利用実態を把握しにくくなります。

また、社員がそれぞれ異なる AI サービスを利用することで、費用の重複、管理の煩雑化、情報セキュリティ方針の徹底不足といった問題も起こり得ます。AI を禁止するだけでは生産性向上の機会を逃すため、企業として安全に使える共通環境の整備が求められます。

「chai+ 汎用 AI チャット」は、主要 AI モデルの横断利用、業務別テンプレート、多層ガードレール、権限・利用ログ管理を組み合わせ、全社での生成 AI 活用を支えるサービスです。

■社員ごとの AI 活用格差を、業務別テンプレートで縮小

生成 AI の成果は、質問や指示の出し方によって変わります。プロンプト作成に慣れた社員だけが成果を得られる状態では、全社的な業務改革につながりません。

本機能では、資料作成、分析、議事録要約、メール文面などに対応する業務別プロンプトテンプレートを用意。利用者は目的に合ったテンプレートを選び、必要事項を入力することで、生成 AI を日常業務に取り入れやすくなります。

企画部門の資料構成案、営業部門の提案書ドラフト、管理部門の議事録要約、情報システム部門の技術文書作成など、職種ごとの業務を支援します。

■GPT・Claude・Gemini など複数モデルを一つの環境で利用

生成 AI モデルにはそれぞれ特性があり、文章作成、要約、分析、技術支援など、目的に応じた選択が重要です。しかし、部署や社員が個別に契約すると、ツールの乱立や管理コストの増加を招きます。

「chai+ 汎用 AI チャット」は、GPT・Claude・Gemini などの主要モデルを用途に応じて切り替えて利用できます。社員が複数の個人契約を使い分けるのではなく、企業が用意した共通の利用環境へ集約できます。

月間利用クレジットを設定する料金体系により、利用状況に応じた運用とコストの可視化にも対応します。

■入力だけでなく AI の回答も検査。情報漏洩リスクへの対策を多層化

企業で生成 AI を利用する際には、顧客情報や個人情報、認証情報などを誤って外部 AI に送信するリスクへの備えが欠かせません。社員個人の注意や利用ルールの周知だけでは、運用の徹底に限界があります。

本機能では、AI への送信前に入力内容を検査し、個人情報や機密情報を条件に応じてマスキングまたはブロックします。添付ファイルのリスク判定や、内部情報の取得を狙う不適切な指示への対策にも対応しています。

さらに、AI から返された回答も再検査し、個人情報や認証情報などの不適切な出力を抑制します。こうした仕組みにより、社員の利便性を保ちながら、企業の情報管理方針に沿った利用を支援します。※リスクの完全な排除を保証するものではありません。

■部署・役職別の権限と利用ログを一元管理し、シャドーAI 対策へ

AI の業務利用が進むほど、情報システム部門や DX 推進部門には、誰がどのモデルを利用できるか、どのような利用傾向があるかを把握する仕組みが求められます。

「chai+ 汎用 AI チャット」は、部署・役職単位で利用可能なモデルやテンプレートなどの権限を設定できます。また、利用ログやガードレールの検知結果を一元的に管理し、利用状況の把握と運用改善に活用できます。

監査向けには検知結果・ルール名・日時などを記録し、個人情報や認証情報の実データは保存しない方針を採用。全社共通の利用環境を整えることで、管理外の個人契約 AI への依存を減らすことを目指します。

■AI を「禁止する」から「管理して活用する」へ

生成 AI の活用を一部の社員に任せるだけでは、組織全体の生産性向上とガバナンスの両立は困難です。企業が利用ルールを定め、使いやすい環境を提供し、利用状況に応じて改善することが重要になります。

デフィデは、法人向け RAG・AI エージェント「chai+」のサービス群を通じ、社内ナレッジを活用した問い合わせ対応に加え、汎用 AI チャットによる日常業務の支援を提供しています。企業の業務や管理体制に合わせた生成 AI 活用を後押しします。

「chai+ 汎用 AI チャット」紹介ページ：https://lp.chatbothub.ai/general-ai-chat
「chai+」サービスサイト：https://lp.chatbothub.ai/
試用環境や導入に関するお問い合わせは、上記サービスサイトから受け付けています。

■デフィデ株式会社について

会社名： デフィデ株式会社
所在地： 東京都港区赤坂 2-4-6-6F
代表者： 山本 哲也
事業内容：戦略 AI コンサルティング／生成 AI 基盤構築支援／社内業務クラウド（SmartOps）／RAG 型 AI チャットボット・特許取得（chai+）／HR Tech（JOB Scope・生成 AI ワークバリュー・スコア分析・HR キャピタルダッシュボード）
Web サイト： https://www.defide-ix.com/
主なサービス一覧：
SmartOps（業務改革 AI プラットフォーム）：https://smartops.jp/
chai+（RAG 型 AI チャットボット・特許取得）：https://lp.chatbothub.ai/
chai+ Full Duplex AI ボイスボット（特許取得）：https://lp.chatbothub.ai/voicebot
JOB Scope（タレントマネジメント）： https://jobscope.ai/
生成 AI ワークバリュー・スコア分析（特許取得）：https://jobscope.ai/ai-survey/

HR キャピタルダッシュボード（JOBScope ISO30414）： https://jobscope.ai/hrcapital/
AI Future Talks：https://www.defide-ix.com/ai/ai-future-talks
JOB Scope マガジン： https://marketing.jobscope.ai/media/

【メディア・記者向けお問い合わせ先】

デフィデ株式会社　広報担当
Email：SalesRep@defide-ix.com
TEL：03-6551-2921
URL：https://www.defide-ix.com/