



信頼できる変革

Pega Blueprintでデータ、プライバシー、AIを安全に管理する方法をご紹介します。

● Pega Blueprint™のセキュリティとプライバシー

Dashboard Pega GenAI + Blueprint™

RETAIL BANKING (BP-206181)

Retail Loan Origination

Select the Case Type to define the workflow details: ☐ Secured Retail Loan Application

Case Lifecycle Case Data Model

This case type defines a secured Retail Loan application process, from submission, approval, and disbursement, ensuring efficient communication with applicants. This case type represents the process of handling and approving a secured retail lending products like vehicle loans.

Primary Steps:

Capture Applicant Inf...	Eligibility and Evaluat...	Additional Document...	Loan Amount and Te...	Loan Agreement and ...
<ul style="list-style-type: none">Collect Applicant InformationCollect Financial InformationCollect Collateral Information + Add Step	<ul style="list-style-type: none">Eligibility CheckCredit CheckValidate Financial DocumentationCheck Collateral TypeValidate Guarantor's Financial DataRetrieve Guarantor's Credit ScoreCheck Guarantor's EligibilityOffer Risk Reducing Product to Client + Add Step	<ul style="list-style-type: none">Additional Documentation CheckCollect Additional DocumentationCollect CollateralValidate CollateralValuation of CollateralApprove/Reject Loan + Add Step	<ul style="list-style-type: none">Loan Amount CheckLoan Terms CalculationLoan Terms Approval + Add Step	<ul style="list-style-type: none">Prepare Loan AgreementReview and Sign AgreementApprove Loan DisbursementUpdate Loan Account InformationUpdate Collateral SystemsLoan DisbursementNotify Applicant for Loan Disbursement + Add Step

Save & Close Next

Table of contents



01 Pega Blueprintとは

ユーザー
運用モデル
ビジネス価値

02 Blueprintアーキテクチャ

クラウドアーキテクチャ
導入地域

03 アクセスと認証

ユーザー管理
シングルサインオン (SSO)
権限

04 データプライバシー

データフロー
ストレージと暗号化
可視化とアクセス

05 クラウドセキュリティ

オペレーション
脅威モデリング
障害からの復旧

06 AIガバナンス

LLMの利用
リスクとコントロール
LLMガバナンス

Pega Blueprint™ セキュリティと プライバシーの概要

Pega GenAI Blueprint™は、お客様のプライバシーとセキュリティを優先事項として構築しました。私たちは、お客様のプロセスは単なる図やワークフローではなく、競争優位性につながるものであると考えています。



アクセスは企業側で管理

Blueprintへのアクセスは、企業のシングルサインオンと連携できます。

- Blueprintは、ロールベースのアクセス制御を通じてデータアクセスを管理し、作成されたBlueprintが積極的に共有されない限り、作成者の非公開情報として維持します。
- ユーザーが企業を退職した場合、組織のSSOプロバイダーでそのユーザーのステータスやロールが更新された時点で、そのユーザーは組織のBlueprintにアクセスできなくなります。

企業のBlueprintとAI学習を分離

プロンプト、データ、設計がAIモデルの学習に使用されることはありません。

- Blueprintは、AWS上のAnthropicモデル、Google Gemini、MS Azure上のOpenAIなど、複数のLLMを内部で活用しています。
- すべてのLLMは、継続的に管理され、パフォーマンステストが行われ、コンテンツフィルタリングに関するプロバイダーのベストプラクティスが活用されています。

データの秘密性を保持

Blueprintの詳細は、暗号化されたクラウドデータベースに保存されます。

- 米国、英国、EUなど、各企業に最適な地域のクラウド上に展開されます。
- Pegaのクライアントやパートナー間においてデータを共有しません。
- Blueprintは、積極的に共有しない限り、作成者の非公開情報に留まります。
- 権限のあるユーザーがPega内で活用する活動レベルのレポートデータのみ（メールアドレス、作成日時、作成者名）を保存します。

エンタープライズグレードのクラウドセキュリティ

Blueprintのデータは、次のとおり、本番環境のPega Cloudと同じように強固に保護されます。

- 保存データには、256ビットAES暗号化を、転送データにはHTTPS/TLS保護を適用します。
- ホストベースのウイルス対策および侵入防止システムにより、継続的なモニタリングを行います。
- 物理的および環境的なセキュリティを重視した最先端のオペレーションセンターを備えています。
- DDoS攻撃に対する組み込み型の保護機能および既知の悪意のあるIPアドレスの自動ブロックで保護します。



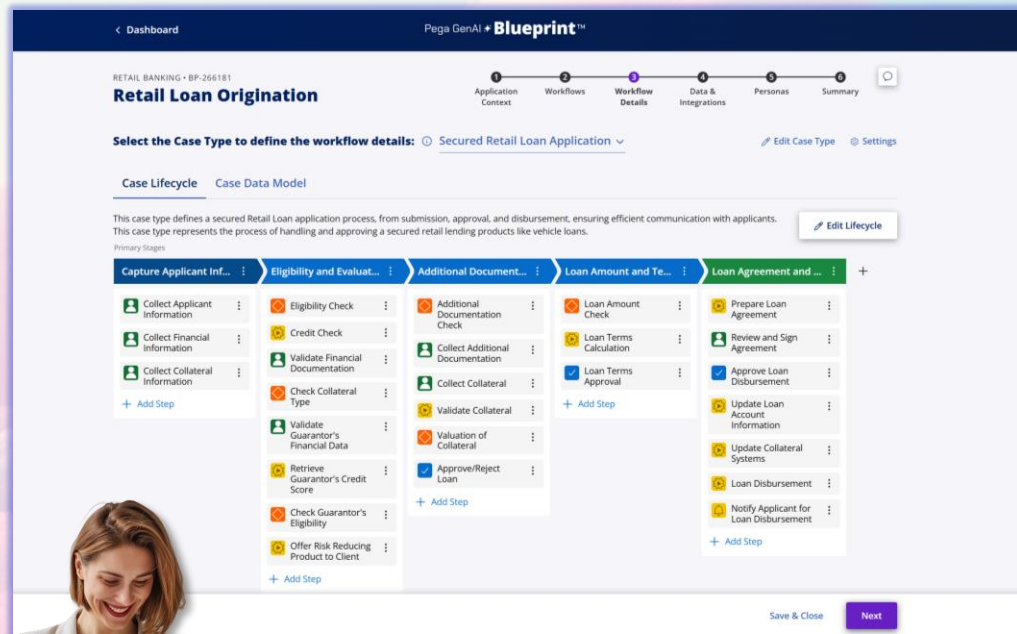
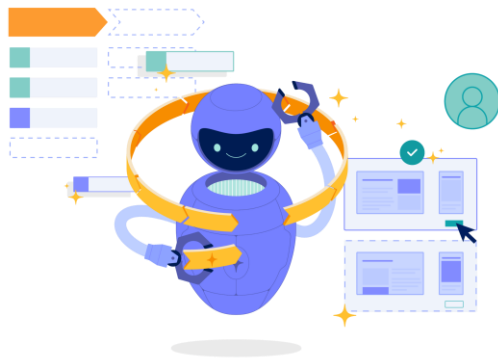
01

Pega Blueprintとは



変革の推進力

Pega Blueprintでは、AIを活用した企業向けワークフローを開発することができます。人とAIを結びつけ、自動化の促進と変革の高速化に重点を置いています。



仕組みについて



#1

レガシー分析を高速化

レガシーシステムを手作業で分析するのではなく、次の情報をアップロードすることで、インサイトを自動的に抽出します。

- ドキュメント（SOPなど）
- ソースコード分析
- ビデオおよび画面

#3

シームレスにコラボレーション

Blueprintは、100%共同作業型であり、すべての業務部門とIT部門の関係者を追加して、以下を実現します。

- AIの提案をスピーディに適用
- 通常の言葉づかいで要件を記述
- 全体的なアプリのプレビュー

#2

ベストプラクティスを活用

要件に基づき、BlueprintのバックグラウンドにあるAI エージェントは、以下の情報に基づいて開始点となるアプリケーションを作成します。

- 業界のベストプラクティス
- Pegaおよびパートナーの専門知識
- 組織の知識

#4

開発を高速化

長い要件収集プロセスを省略し、開発者がスピーディな本番稼働を実現できるようにします。

- Blueprintをインポートして、数秒でアプリを生成
- ユーザーストーリーのバックログを自動生成
- Pega App Studio全体でAIを活用し、新しいアプリをスピーディに完成して導入

SDLCでBlueprintを活用

迅速な設計で開発を高速化



*設計時のユースケースに基づくと、これらの段階でPIIを管理することは推奨されません。

02

Blueprintアーキテクチャ



Pega Blueprint™ アーキテクチャ

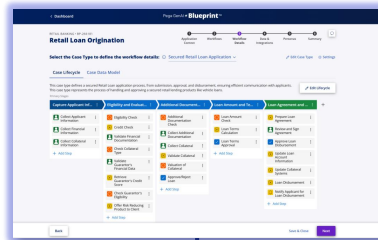
Blueprintは、Pega Cloud® on AWSで安全に実行され、主要なクラウド標準に従って管理および運用されます。

アーキテクチャの概要：

- Blueprintの認証は、企業のシングルサインオンプロトコル（SSO）と連携します。
- Pegaは、Pega Cloud製品に特化した、地理的にセグメント化されたデータ保存サービスを提供しています。Blueprintの地域は、企業の所在地（米国東部、英国、または欧州連合内）に基づきます。
- Blueprintの処理は、Pega Cloudサービスの運用基盤を十分に活用した安全で信頼性の高いPega Infinityアプリケーション上で実行され、エンタープライズレベルの信頼性、コンプライアンス、セキュリティ、障害復旧を実現しています。
- Blueprintは、ユースケースとパフォーマンスに基づいてLLMを活用します。主にAWS Bedrock上で動作するClaudeモデルを使用しています。
- BlueprintのデータはAIの学習に使用されません。
- Blueprintのデータは、TLSを使用して転送中に暗号化されます。
- Blueprintのデータは安全に保存され、保存時に暗号化されます。



Pega.com
フロントエンドWebアプリ



Pega.com
認証サービス

企業の
SSO

従業員
{user}@{your-org}.com

次の地域全体で完全に分離：
米国・英国・EU

PEGA Cloud® AWS

Blueprintアプリケーション

ユーザーリクエストのコア処理とBlueprintの機能
Pega Infinity™上に構築



業界知識サービス

ユーザーのリクエストに基づいて、ワークフローとデータモデルのベストプラクティスに関する情報をBlueprintに提供するRAG（検索拡張生成）サービスです。

Pega Knowledge Buddy™上に構築され、Pegaの業界固有の知的財産が含まれています。クライアントやユーザーのデータは保存されません。



Pega Cloud AIオーケストレーションサービス

LLMへの選好をオーケストレーション

AWS上に構築され、プロンプト、クライアントデータ、またはユーザーデータを保存しません。



AWS Bedrock
主なLLMプロバイダー
Claude, Haiku, Sonnet



Google
Gemini
Flash



Azure
OpenAI
GPT

ユースケース/パフォーマンスに基づいてさまざまなLLMを活用しています。すべて同じ地域内で処理され、ユーザーや企業のデータを利用してAIの学習を行うことはありません。



安全なデータストレージ

企業向け保存データ暗号化（DARE）

すべてのクライアントデータはボリュームに格納され、データベースは256ビットで保護されます。デフォルトでは、暗号化キーは定期的にローテーションされ、FIPS 140-2に準拠した安全なKMSに安全に保存されます。ご要望に応じて、企業専用プライベート暗号化キーをご利用いただけます。



プライベートファイルストレージ

Pega Cloudレポトリに接続

Blueprintのアクティビティに関連するすべてのファイル（例：アップロードされたドキュメントやビデオ）は、企業用のプライベートS3フォルダーに保存されます。デフォルトでは、これがBlueprintが企業のために管理するS3フォルダーになります。Pega Cloudのクラウドオンプレミス、リクエストに応じて、Pega Cloudインスタンスに直接付けられた非公有のプライベートS3リポトリにBlueprint関連ファイルを保存することも選択できます。

Pega Blueprint™データ保存場所

企業の所在地：

EU

- ストレージおよびコンピューティング：
AWS EU-Central（フランクフルト）
- [AIモデルの実行](#)：地域内

プロバイダー	モデル/プロバイダー	LLMの地域
 AWS Bedrock <small>主なプロバイダー</small>	Anthropic	AWS Bedrock : EU
 Google Gemini	Flash	Google Vertex : EU
 Microsoft Azure	GPT	Microsoft Azure : EU

企業の所在地：

英国

- ストレージおよびコンピューティング：
AWS EU-West-2（ロンドン）
- [AIモデルの実行](#)：地域内

プロバイダー	モデル/プロバイダー	LLMの地域
 AWS Bedrock <small>主なプロバイダー</small>	Anthropic	AWS Bedrock : 英国
 Google Gemini	Flash	Google Vertex : 英国
 Microsoft Azure	GPT	Microsoft Azure : 英国

企業の所在地：

オーストラリア



- ストレージおよびコンピューティング：
AWS AP-SOUTHEAST-2（シドニー）
- [AIモデルの実行](#)：地域内

プロバイダー	モデル/プロバイダー	LLMの地域
 AWS Bedrock <small>主なプロバイダー</small>	Anthropic	AWS Bedrock : シドニー
 Google Gemini	Flash	Google Vertex : スウェーデン
 Microsoft Azure	GPT	Microsoft Azure : スウェーデン

企業の所在地：

全世界

- ストレージおよびコンピューティング：
AWS US-East
- [AIモデルの実行](#)：地域内

プロバイダー	モデル/プロバイダー	LLMの地域
 AWS Bedrock <small>主なプロバイダー</small>	Anthropic	AWS Bedrock : 米国
 Google Gemini	Flash	Google Vertex : 米国
 Microsoft Azure	GPT	Microsoft Azure : 米国

Pegaパートナー向け

Blueprintの機能説明ページの組織名フィールドで、Blueprintを作成する対象となる企業を定義すると、作成されたBlueprintは、その企業のために地域内で自動的に保存および管理されます。

Blueprintをどの地域に保存するか定義

EU、オーストラリア、または英国内で保存および管理されている場合は、地域の識別子を持つBlueprint IDを確認してください。

03

アクセスと認証



Pega Blueprint™

アクセスと認証

シングルサインオン（SSO）でBlueprintへのアクセスを設定します。

組織のIDPに対するユーザー認証を有効にすると、Blueprint、My Support PortalなどのすべてのPegaサイトとアプリケーションへのアクセスを、認証ユーザーに限定できます。

フェデレーション認証が有効になっている場合、ユーザーはログイン時にパスワードの入力を求められず、IDプロバイダーに対して認証を行うようリダイレクトされます。

クライアント組織のITリーダーは、当社の統合アカウントチームと協力して、フェデレーション認証を有効にすることができます。

必要な情報：SAML 2.0の設定詳細、またはOAuthの設定詳細

次のアプリケーションへのログインには、フェデレーション認証が使用されます。Blueprint、Pega.com、community.Pega.com、academy.Pega.com、support.Pega.com、docs.Pega.com、partners.Pega.com、saleshub.Pega.com、partner-logo-generator.Pega.com、My Support Portal、My Pega Cloud、My Pega、PDC、Deployment Manager、Pega Trials

Blueprintは、積極的に共有しない限り、見ることができるのは作成者のみです。

デフォルトでは、Blueprintは、Blueprintを作成したユーザー（Blueprintの所有者）以外には表示されません。**

Blueprintの所有者は、Blueprintを他のステークホルダー（チームメイト、パートナーなど）と共有できます。ユーザーは、編集者または閲覧者としてメールでユーザーを招待できます。

Share this Blueprint

Invite Collaborators

Only collaborators with a business email address will be able to access Pega GenAI Blueprint

Emails, comma separated

Editor ▼

Send

ユーザーが企業を退職した場合、そのユーザーのBlueprintを持ち出すことはできません。

企業がPegaのデジタル資産（Blueprintなど）とSSOを連携している場合、そのSSOに有効なアクセス権を持つユーザーのみがBlueprintにログインできます。

ユーザーがPega.comのプロファイルに登録されているドメインを変更すると（例：組織を変更する）、古いドメイン内に作成したBlueprintは表示されなくなります。

これらのBlueprintへのアクセスは、リクエストに応じて組織内の他のユーザーに対して復元できます。

04

データプライバシー



Pega Blueprint™

データ処理

収集される情報とその処理方法

#	データポイント	フォーマット	LLMによる処理	AI学習への利用	保存先	表示対象
1	クリエイター情報	メタデータ（名前、メール、組織）	なし	なし	Pega Cloudデータストレージ 完全に暗号化*	Pega
2	アプリケーションの説明	メタデータ（業界、アプリ名）	あり（最初のBlueprintテンプレートを通知）	なし	Pega Cloudデータストレージ 完全に暗号化*	Pega
3	テキストベースのアプリケーションの説明	暗号化されたテキスト	あり（最初のBlueprintテンプレートを通知）	なし	Pega Cloudデータストレージ 完全に暗号化*	Blueprintの作成者と招待者のみ**
4	レガシードキュメント	.PDF、.DOC、.DOCX	あり（最初のBlueprintテンプレートを通知）	なし	Pega Cloudファイルストレージ 保存時に暗号化*	Blueprintの作成者と招待者のみ**
5	レガシービデオと画像	.MOV、.MP4、.JPG、.PNG	あり（最初のBlueprintテンプレートを通知）	なし	Pega Cloudファイルストレージ 保存時に暗号化*	Blueprintの作成者と招待者のみ**
6	プロセス図	.BPMN	あり（最初のBlueprintテンプレートを通知）	なし	Pega Cloudファイルストレージ 保存時に暗号化*	Blueprintの作成者と招待者のみ**
7	統合とデータドキュメント	.YAML、.SQL、.DDL、.CRD	あり（最初のBlueprintテンプレートを通知）	なし	Pega Cloudファイルストレージ 保存時に暗号化*	Blueprintの作成者と招待者のみ**
8	Blueprintの編集と最終デザイン	暗号化されたメタデータ（暗号化されたBlueprintファイルとしてエクスポート）	なし	なし	Pega Cloudデータストレージ 完全に暗号化*	Blueprintの作成者と招待者のみ**

*Blueprintデータは、Pegaサポートを通じてリクエストすることで完全に削除できます。

**権限を持つPega管理クラウド運用担当者のみが閲覧できます。

Pega Blueprint™

データ表示

データの秘密性を保持

Blueprintの詳細は、暗号化されたデータベースに保存されます。これらの詳細情報は、権限を持つPega管理者のみが閲覧できます。また、Blueprintに入力したデータは、当社が使用するAIモデルの学習には使用されません。データ（プロンプトや応答）はLLMプロバイダーと共有されず、クラウドプロバイダーはアクセスできません。情報はお客様だけのものです。



Pegaのユーザーが見ることができる情報

システムを安定して稼働させ、必要なときにサポートするために必要な最小限の情報のみです。

- Blueprintの**システム生成識別子**。BlueprintによるPegaケース作成、ケースID
- Blueprintを作成した人の**メールアドレス**
- Blueprint用に指定された**略称**

その他の情報

すべて非公開です。プロセスの説明、ワークフロー、データモデル、およびアップロードするドキュメント（アプリケーションドキュメント、BPMNファイル、API定義、統合設定など）は、前述のとおり非公開のままです。

05

クラウドセキュリティ





詳細については、[Pega Cloudトラストセンター](#)をご覧ください

Pega Blueprint™ クラウドセキュリティ

Pega Blueprintは、Pegaの実証済みのPega Cloud® サービス上で実行され、エンタープライズグレードのセキュリティを確保します。

信頼できる変革

- 24時間年中無休の運用監視、管理、サポート
- 厳格なアクセス制御と運用上の安全対策により、自動化を通じて人手による作業を最小限に低減。設計段階からセキュリティを考慮したアーキテクチャ運用
- エンタープライズグレードのコンプライアンス、稼働率、障害復旧、脅威モデリング

オペレーション

24時間365日のモニタリング、環境サポート、先回りの対応
[詳細](#)

アクセス

自動化された運用管理と厳格なアクセスプロトコルで管理された環境
[詳細](#)

コンプライアンス

20以上の業界標準に厳密に準拠
[詳細](#)

障害からの復旧

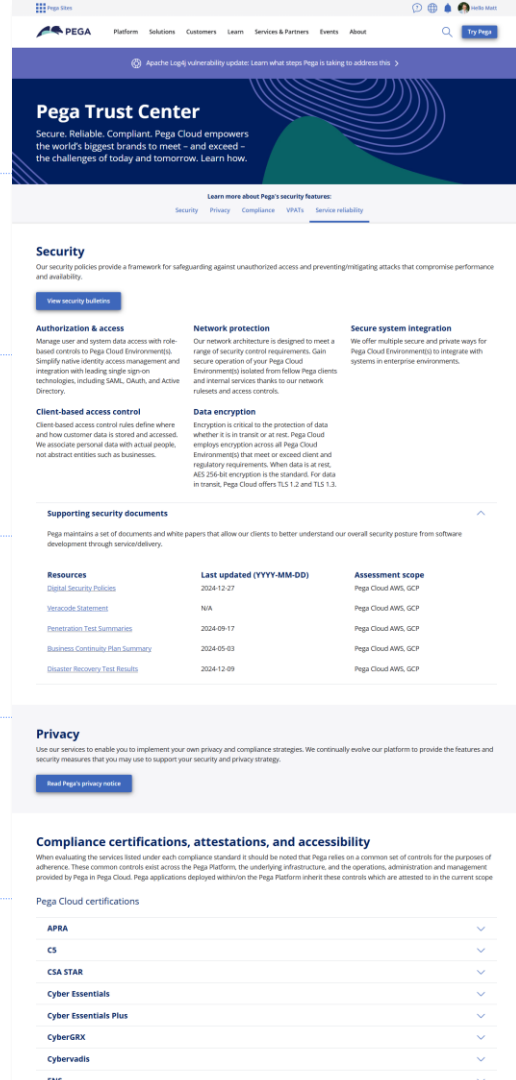
包括的なデータとサービスのバックアップ、フェイルオーバー、復旧
[詳細](#)

脅威モデリング

OWASP Top 10に基づくレッドチーム手法を適用
[詳細](#)

可用性

アーキテクチャは、組み込みの高可用性と障害復旧を活用して、ほぼ継続的な稼働率をサポート
[詳細](#)



06


AIガバナンス



Pega Blueprint™により各種の 最先端モデルを組み合わせ スピーディな変革を支援

モデルはすべて安全に管理され、製品に組み込まれ、
有効性とパフォーマンスのバランスが保たれています。

2025年第3四半期現在
Pegaでは、適切なタスクに適切なモデルを使用できるようLLMを継続的に評価しています。現在内部で活用されているのは、次のモデルです。

ハイパースケーラー	LLMプロバイダー	Blueprintの地域	LLMの地域
 AWS 主なプロバイダー	Anthropic	AMS（米国）	AWS Bedrock : 米国
		EU	AWS Bedrock : EU
		英国	AWS Bedrock : 英国
 Google Cloud	Google Gemini	AMS（米国）	Google Vertex : 米国
		EU	Google Vertex : EU
		英国	Google Vertex : 英国
 Microsoft Azure	OpenAI - GPT	AMS（米国）	Microsoft Azure : 米国
		EU	Microsoft Azure : EU
		英国	Microsoft Azure : 英国

ハイパースケーラーとのすべての契約には、ハイパースケーラーやLLMプロバイダーのいずれも、Pegaやクライアントから送信されたプロンプトやデータにアクセスしないという誓約が含まれています。

*2025年6月現在

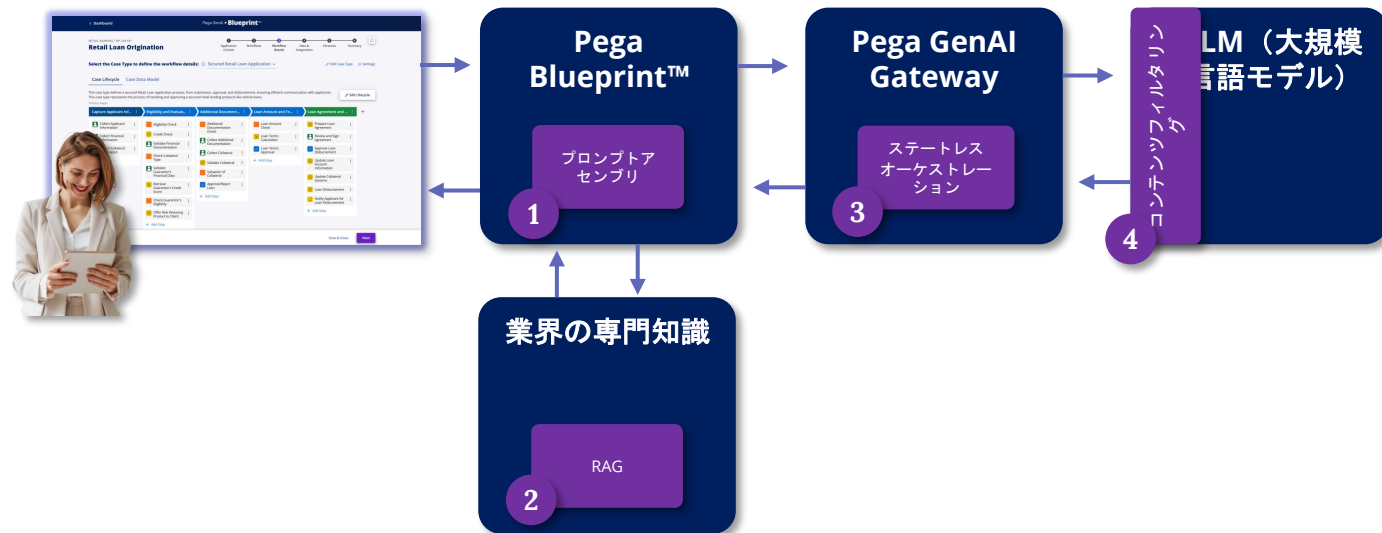
**pega.comに常に最新情報を掲載

AIデータフロー

Pega Blueprint™

保護された安全なAI処理：

1. Pega Blueprintは、ユーザーが入力した情報に基づいて、アプリケーションを説明する**プロンプト**を作成します。
2. Pega Blueprintは、Pega Knowledge Buddyで実行されるPegaの**業界専門知識**ナレッジベースを呼び出し、Blueprintのユースケースに基づいて業界のベストプラクティスを統合し、LLMプロンプトとBlueprintの作成を強化します。
3. LLMの呼び出しは、すべてPega Cloud上の**Pega GenAI Gateway Service**によって仲介されます。このサービスは、大規模言語プロバイダーとの通信において、信頼性の高いセキュリティ、セグメンテーション、スケーラビリティのレイヤーを提供します。
4. 暗号化されたプロンプトを安全なLLMに送信する場合、**コンテンツフィルタリング**が適用され、プロンプトや完了画面に含まれる有害なコンテンツを検出して防止します。



コンテンツフィルタリングのアプローチ

Pegaは、生成AIを利用するPega機能の提供において、実績のある大規模言語モデルプロバイダーを利用しています。各モデルには、有害、非倫理的、害意のある応答が発生する可能性を軽減する堅牢なコンテンツフィルタリング機能が用意されています。機能は堅牢ですが、これらは緩和策に過ぎず、回避される可能性は依然として残ります。さらに、責任ある倫理的なAIで同じ成果を達成するアプローチは、モデルプロバイダーによって異なります。

つまり、分類モデル、しきい値、検出のカテゴリは異なる可能性があるということを意味します。別のモデルを使用すると、別のコンテンツ分類とフィルタリングが適用されます。クライアントがPega GenAI Connectを使用する際には、こうした潜在的な差異を認識し、テストを実行して検証する必要があります。

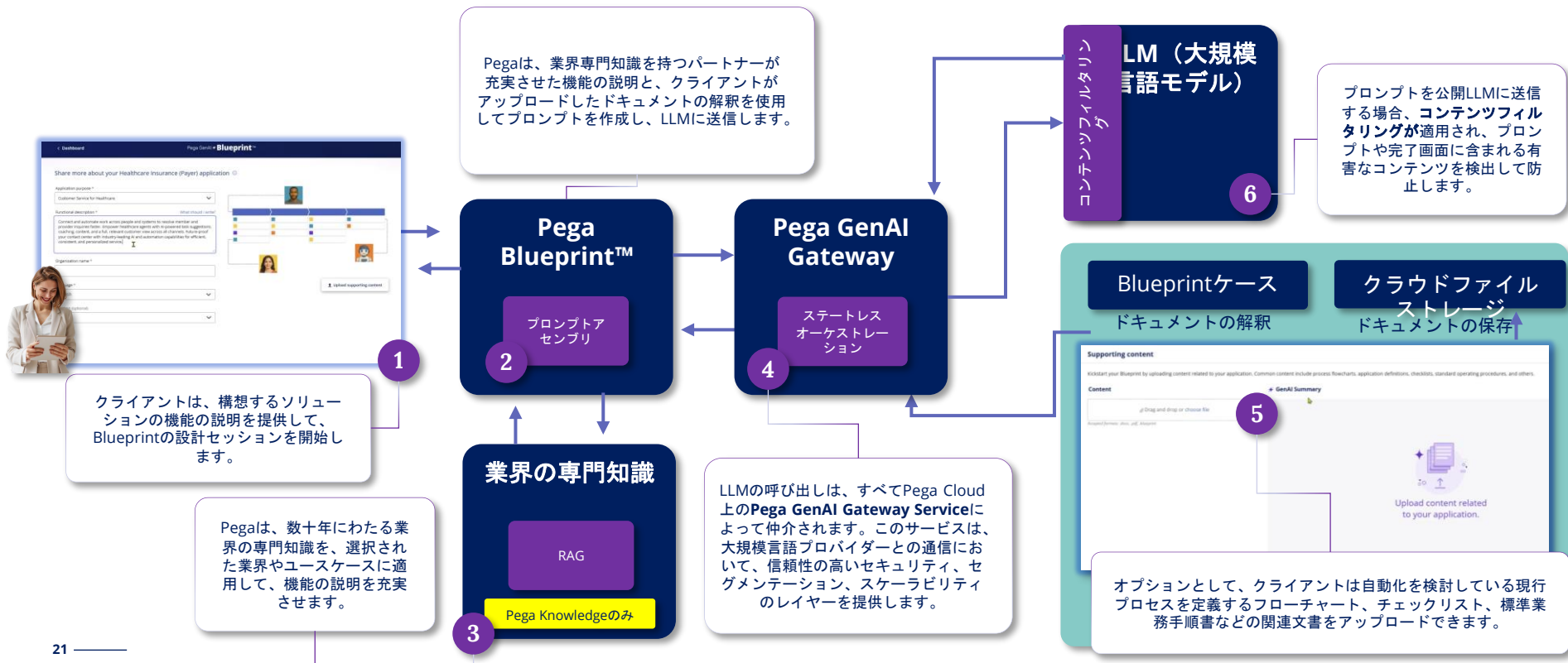
AIデータフロー

Pega Blueprint™

コンテンツフィルタリングのアプローチ

Pegaは、生成AIを利用するPega機能の提供において、実績のある大規模言語モデルプロバイダーを利用しています。各モデルには、有害、非倫理的、害意のある応答が発生する可能性を軽減する堅牢なコンテンツフィルタリング機能が用意されています。機能は堅牢ですが、これらは緩和策に過ぎず、回避される可能性は依然として残ります。さらに、責任ある倫理的なAIで同じ成果を達成するアプローチは、モデルプロバイダーによって異なります。

つまり、分類モデル、しきい値、検出のカテゴリは異なる可能性があるということを意味します。別のモデルを使用すると、別のコンテンツ分類とフィルタリングが適用されます。クライアントがPega GenAI Connectを使用する際には、こうした潜在的な差異を認識し、テストを実行して検証する必要があります。



AIデータフロー

Pega Blueprint™



Pegaにおける AIガバナンス

エンドツーエンドの監視

PegaのAIガバナンス委員会は、クラウドセキュリティチームによって運営され、Pega製品全体のAI活用を監督しています。

製品、クラウドセキュリティ、クラウド運用、IT、法務、市場開拓の各分野のエキスパートと企業経営者が参加しており、PegaにおけるAIのあらゆる利用の安全性、責任、セキュリティを維持しています。

戦略的パートナーシップ

Pegaは、企業クライアント固有のニーズを満たすために、AWS、Google Cloud、Microsoftと戦略的關係および包括的な契約を締結し、共同でAIイニシアティブを推進しています。

PegaとLLMサービスのクラウドプロバイダーは定期的に会合を行い、モデルオプション、パフォーマンス、セキュリティ、諸問題を確認しています。

セキュリティ第一

PegaのAIガバナンス委員会は、Pega Blueprintを含むすべてのAI活用型機能の継続的なセキュリティ評価を組織および実行します。

セキュリティ評価には、以下が含まれます。

1. Microsoft AI Red Team手法
2. OpenAIの安全性に関するベストプラクティス
3. Microsoftが指定する緩和策
4. LLMアプリケーション向けOWASP Top 10
5. クラウドネイティブアプリケーションセキュリティのOWASP Top 10





Pega is the leading Enterprise Transformation Company™ that helps organizations Build for Change® with enterprise AI decisioning and workflow automation. Many of the world's most influential businesses rely on our platform to solve their most pressing challenges, from personalizing engagement to automating service to streamlining operations. Since 1983, we've built our scalable and flexible architecture to help enterprises meet today's customer demands while continuously transforming for tomorrow. For more information on Pega (NASDAQ: PEGA), visit <http://www.pega.com>