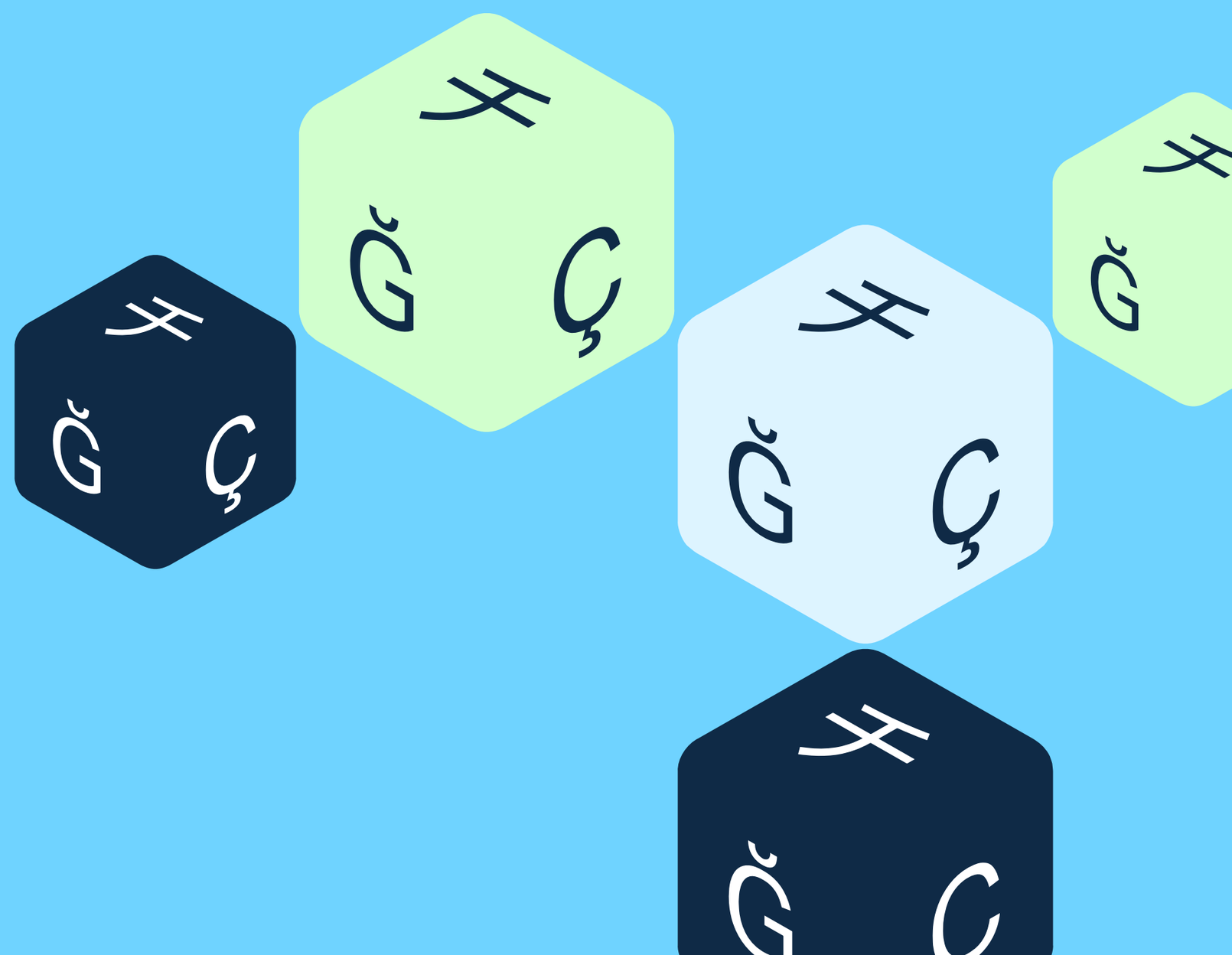
DeepL

レポート

セキュリティおよびデータレジデンシーに関するホワイトペーパー：ハイブリッドインフラストラクチャモデルAWSとプライベートデータセンターの連携におけるアーキテクチャ上の安全対策



要旨

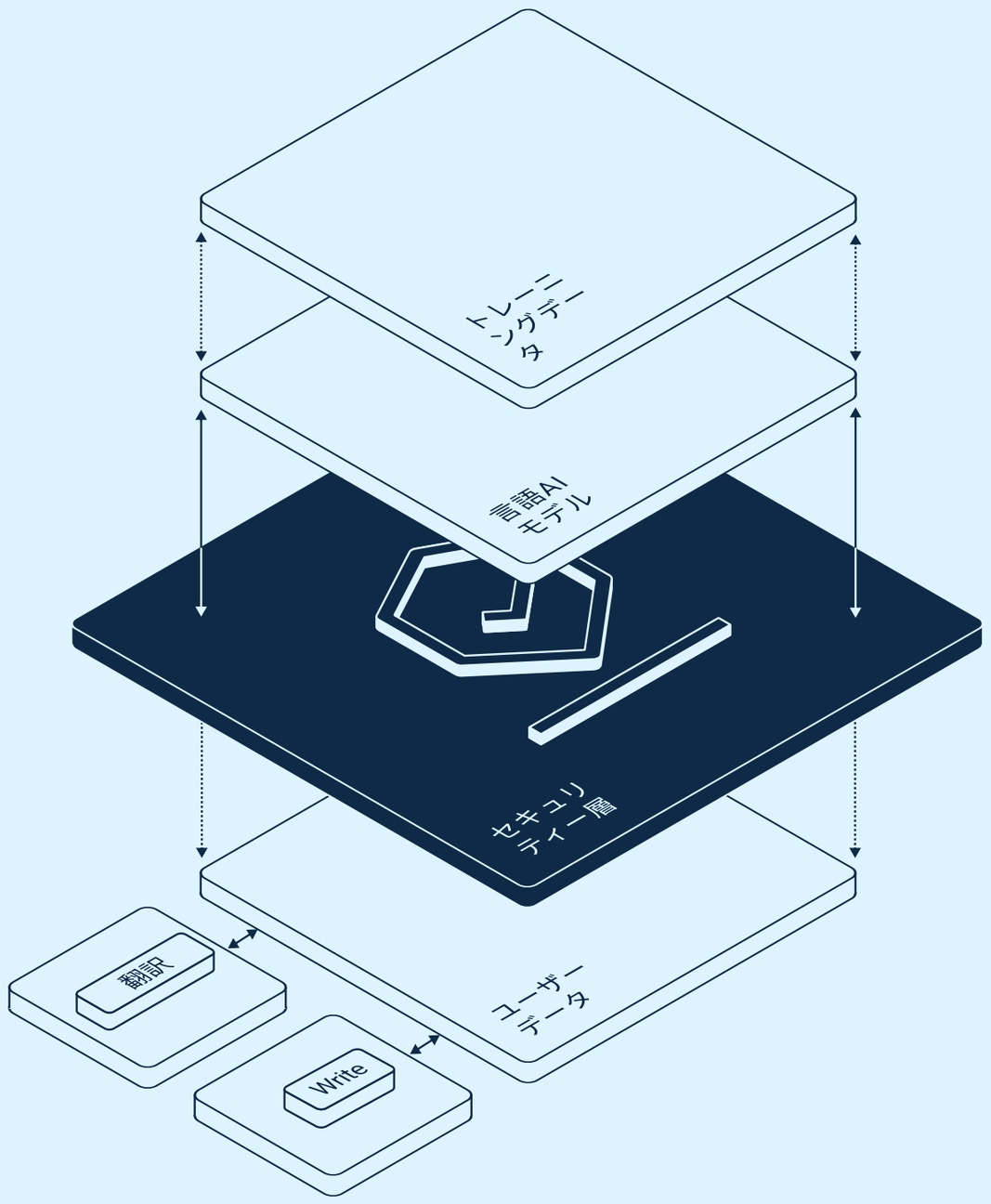
ハイブリッドインフラへの移行には、オンプレミスのデータセンターと同等の要件を備えるセキュリティモデルが必要だ。
DeepLのアーキテクチャはプライバシーを重視する組織向けに特別に設計されており、AWSの拡張性とプライベートデータセンターインフラにおける高度な管理を兼ね備えている。

ハイブリッドなアプローチを採用することで、AWSの専門知識を活かして極めて堅牢なデータベースサービスを安全に運用しつつ、より信頼性が高く効果的なサービスやプロダクトを提供することに注力できるなど、よりよいサービスを提供できると考える。

当社のセキュリティへの強い関心は、業界標準の認証によって保証されており、お客様のハイブリッドモデルに移行する際にもその法令遵守体制が妨げられることはない。

- 法令遵守：
  SOC2 Type IIとISO 27001に完全に準拠、および認証取得済み

- 特定の範囲内サービスおよびリージョン（AWSストックホルム（eu-north-1）を含む）については、BSIクラウドコンピューティングコンプライアンス基準カタログ（C5）に準拠



DeepL

ハイブリッドセキュリティアーキテクチャ

以下の図と説明は、DeepLのインフラの大まかな流れを示し、セキュアエッジであるAWSストックホルムと、プライベートデータセンター環境の連携を表す。

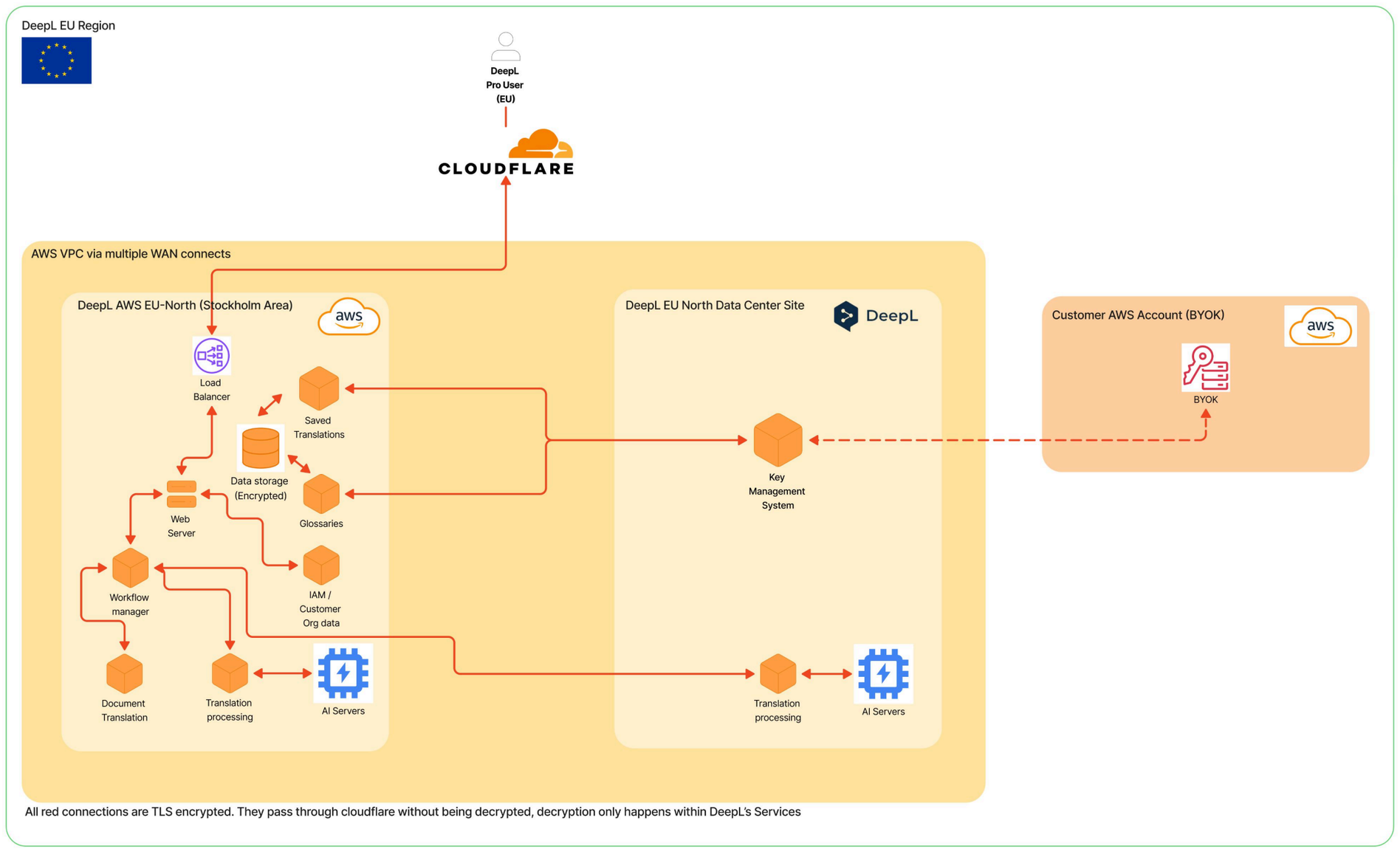


図1

図1に示されている通り、リクエストはまずDeepLのCDNであるCloudflareを経由する。Cloudflareは悪意のある「ボット」によるリクエストや試行をフィルタリングして取り除くことで、セキュリティ層を提供している。

フィルタリングされたリクエストは、暗号化されたままDeepLのサーバーへ転送される。画像やJavaScriptなどの静的なウェブコンテンツは、すべてのユーザーのページ読み込み速度を上げるため、Cloudflareにより提供される。

リクエストは、DeepLのロードバランサーによって復号化され、その後、内部のTLS暗号化レイヤーを使用して処理を行う下流サービスへと渡される。

翻訳リクエストは、例えば言語ペア等を評価された後、DeepLの翻訳エンジンに送信される。翻訳エンジンはAWSとオンプレミス環境の両方に配置されており、これによりコンピューティングリソースを可能な限り効率的に活用することができる。

データセンター間を伝送されるリクエストは、低遅延かつ高速の仮想プライベートリンク（TLSアプリケーション層 + MACSecフォールバック）で暗号化される。

ユーザーが用語集や保存済みの訳文を利用する場合、このコンテンツはDeepLが自社管理するKMSサービスを用いて暗号化（エンベロープ暗号化）される。これには、DeepLのオンプレミスサービスでホストされる自社管理の暗号化キーがデフォルトで使用される。
お客様が自身のAWSアカウントを通じてキーを提供する方法である、BYOK（私有キー）オプションにも対応する。

このようにエンベロープ暗号化されたデータ自体は、保存時暗号化が有効なストレージデバイスに保管される。保存時暗号化はAWSにより提供され、AWSのキーとKMSを使用する。

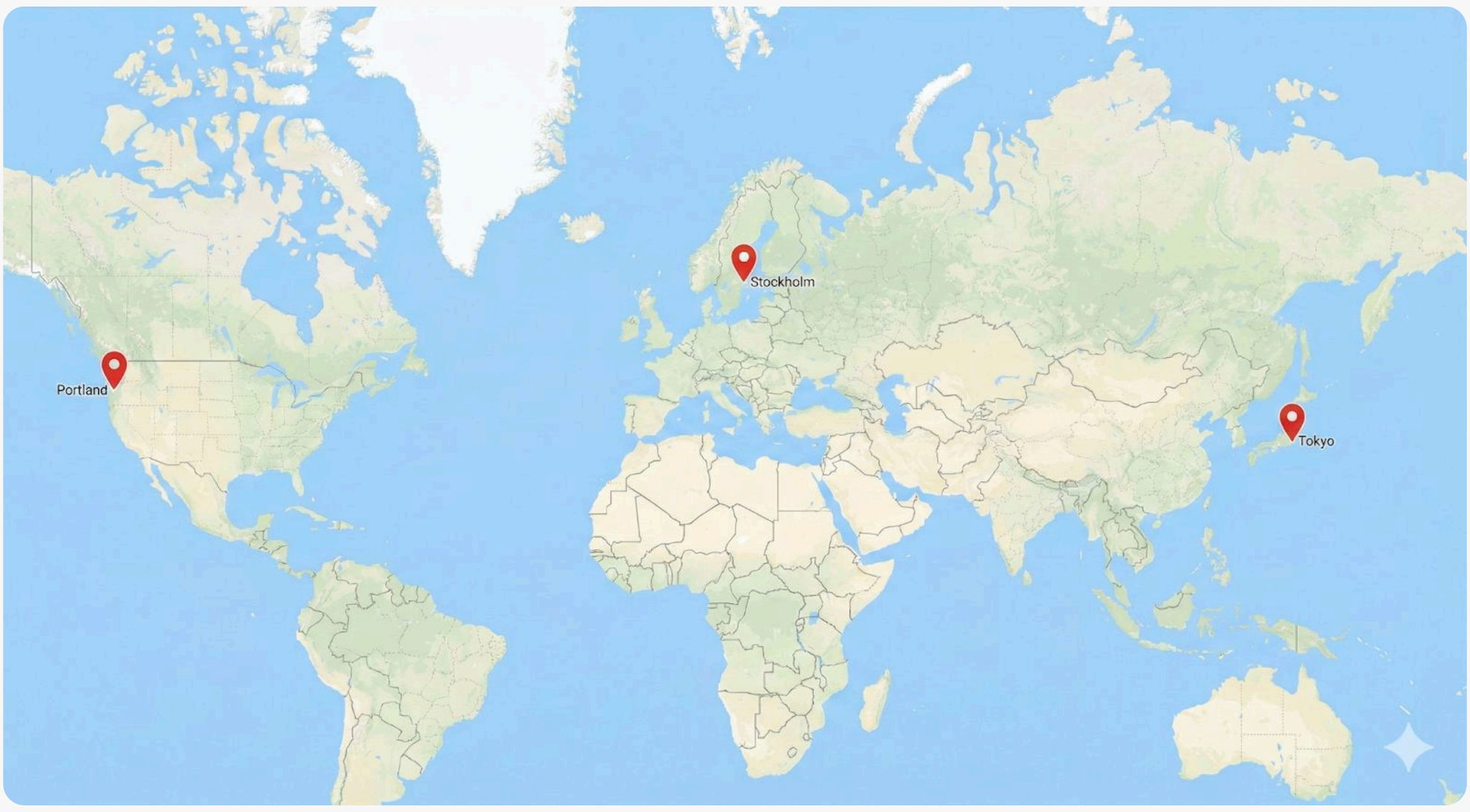


図2

図2は、DeepLがグローバル設定で使用しているリージョンを示したものだ。オレゴンと東京は、DeepLの地域別顧客サービスにおけるAWSベースのリージョンである。
一方ストックホルムはDeepLのハイブリッドリージョンであり、AWSと自社のデータセンターサイトを組み合わせて欧州地域を支えている。

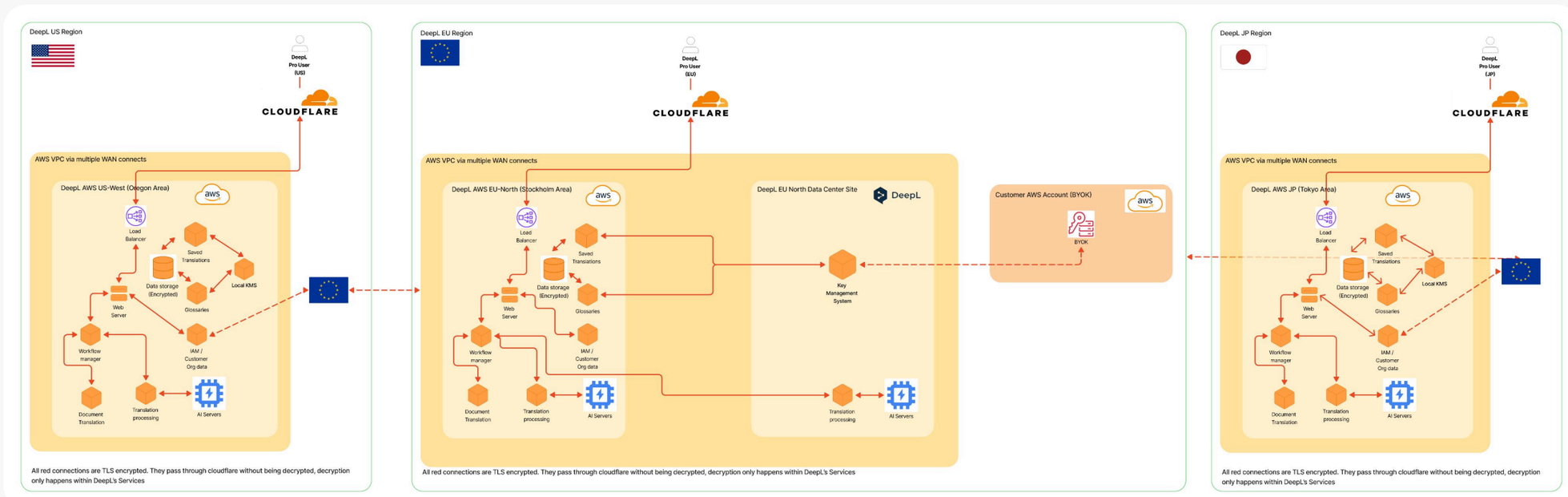


図3

図3に示されている通り、DeepLの地域別デプロイではスタック全体が組み込まれており、ユーザーのインタラクションが優先地域内で確実に処理されるようになっている。
ヨーロッパ地域においてのみ、キーはAWS外で管理される。私有キーの利用はすべての地域で利用可能で、AWSを基盤としている。IAM（認証、ライセンス）の設定は、欧州サイトからの一方向同期により運用されている。

データレジデンシーを保証

DeepLでは、法令遵守の簡素化および内部監査要件の充足のため、有料アドオンを通じてデータレジデンシー保証を提供している。データレジデンシーを希望するお客様向けの情報は以下で確認できる。

- **有料アドオンによる地域限定処理：** お客様のデータは、選択した地域でのみ処理および保管される。

- **ハイブリッド主権：**DeepLでは、欧州連合域内のAWSリージョン（ストックホルムなど）を利用しているが、暗号化キーマテリアルは、お客様がAWS機能に依存する私有キーの利用（BYOK）を選択しない限り、DeepLのアグノスティックなKMSを介してAWS外の欧州域内データセンターに保管される。

- その他のリージョンでは、キー素材はプロバイダーに依存しないKMSサービスを使用してAWS上に保存される。

- データレジデンシーのアドオンを購入されないお客様については、DeepLはお客様のデータをいずれのリージョンでも処理する権利を留保する。

防御強化とエッジにおけるゼロトラスト

DeepLはグローバルトラフィックに対し、「ゼロトラスト」アプローチを採用している。すなわち、DeepLはCloudflareの優れた可用性を利用しているが、ユーザーのコンテンツはエッジプロバイダーに対して「ブラックボックス」のまま保たれる。

- **暗号化されたパススルー：**Cloudflareはボット検知とDDoS対策を管理するが、翻訳リクエストを復号化することはできない。

- **転送中のTLS暗号化：**すべてのリクエストは、ユーザー端末からDeepLのセキュアな環境まで、TLS暗号化（図中の赤線で示される）により保護される。

一時的な「インフライト」データ処理

API、Webサイト、アプリでの操作において、DeepLはデータ最小化の厳格なポリシーを遵守している。

- **ゼロレジデンシー：**テキスト操作は「インフライト」で処理される。標準的な操作中にユーザーの原文や訳文がディスク上に保存されることはない。
- **ジャストインタイム復号化：**データは、DeepLサービスへの入力時点でのみ復号化され、出力時には再度暗号化される。

データ主権（KMSおよびBYOK）

DeepLでは、クラウドの柔軟性とオンプレミス環境での制御との間の溝を埋めるため、自社のキー管理アプローチを採用している。

- **アグノスティックなKMS：**当社のキー管理サービス（KMS）は、AWSとは独立したサービスであり、欧州では当社の専用データセンターに設置されている。そのため、AWSインフラを利用する場合でも、「信頼の基点」がDeepLの監査済み物理的管理下にあることが保証される。
- **私有キーの利用（BYOK）：**AWSのKMSから直接組織のキーをインポートすることで、最終的な権限を維持できる。
- **文書レベルの保護：**保存されたコンテンツについては、クライアントアプリケーションがキーを保持する「エンベロープ」暗号化方式を採用しているため、コンテンツは二重に暗号化される。オブジェクト層とストレージ層（保存時暗号化）の双方で保護され、権限のない第三者はアクセスできないようになっている。文書ファイルの翻訳には同様の二重暗号化が適用されるが、エンベロープ暗号化ではなく文書レベルの対称暗号化を使用する。

セキュリティマトリックス

機能	保護機構	セキュリティ上のメリット
転送中データ	TLS 1.2以上	TLSは、転送中のデータを暗号化する標準的な方法として認知されており、最高水準のセキュリティ基準を要求される各国の機関で採用されている。
エッジ保護	復号化しないCDN	DeepLでは、静的アセット（Webサイトの画像やJavaScriptなど）の配信を高速化し、パフォーマンスを改善するためにCDNを利用している。 加えてCDNは、ボットやDDoS攻撃に対する最初の防御層の役割も果たすが、DeepLサービスへの暗号化された接続の中身は一切見ることができない。
保存データ	アグノスティックKMS + オプションのBYOK	DeepLのストレージにおける通常の保存時暗号化に加え、その上に暗号化レイヤーを導入しているため、オンプレミス環境とクラウド環境の両方で、キーマテリアルと暗号化マテリアルの管理を維持できる。
処理	インフライトデータの一時的復号化	トラフィックの復号化は可能な限り最終段階で実施しており、復号化のポイントをDeepLサービス側へとより近づける取り組みを継続していく。

用語集

AWS
Amazon Web Services

BSI
ドイツ連邦共和国IT・セキュリティ当局

BYOK
私有（暗号化）キーの利用

GDPR
EU一般データ保護規則

DDoS
分散型サービス拒否攻撃

KMS
キー管理システム

TLS
トランスポート層セキュリティ

VPC
仮想プライベートクラウド

WAN
広域ネットワーク

IAM
IDおよびアクセス管理

お問い合わせはこちら
info@deepl.com