HashiCorp

vodafone | お客様のケーススタディ

可能性を解き放つ

Vodafone 社は HashiCorp Vault を使用してカスタムプラグイン機能を開発し、シークレット管理と高速の暗号化エンジンを強化しています。

Vodafone 社について

世界的な大手通信会社の Vodafone 社は、より良い未来のために人々をつなぐことを使命としています。顧客をつなぎ、将来のデジタル社会の構築を支援するために、先進的な製品やサービスを多数開発しています。Vodafone 社は 21 の国で移動通信網と固定通信網を展開し、47 以上の国で移動通信事業者と提携しています。2022 年 9 月 30 日時点では、同社の移動通信サービスの利用者は 3 億人超、固定ブロードバンドサービスの利用者は 2,800 万人超、テレビサービスの利用者は 2,200 万人でした。また、Vodafone 社はモノのインターネット（IoT）の世界的なリーダー企業として、1 億 5,000 万を超えるデバイスとプラットフォームを接続しています。

移動通信サービスの利用者は
3 億人

1 時間あたり 360 億回の
データ暗号化に対応できる
低遅延と高スループットを実現

プラグインアーキテクチャで機能と
拡張性を強化するフレームワークを
提供

21 か国で事業を展開

17 ペタバイトのデータレイクに
対応できる安全な暗号化技術を
実現

複数のエンジニアリングチームに
サービスとして暗号化機能を提供

> あなたが Vault Enterprise の顧客なら、何ができるかに目を向けてください。自社独自の要件に合わせてプラグインを作成し、可能な限り迅速かつ簡単に動作させることができます」

ANDY SHACKLADY 氏
VODAFONE 社、クラウドテクノロジプラットフォームエンジニアリング担当マネージャー

分析ストリームを保護

Vodafone 社の分析・データエンジニアリングチームは、大規模なクラウド環境を管理し、分析用の機械学習（ML）、AI、およびビジネスインテリジェンスのあらゆるユースケースを Google Cloud で利用する多くの内部顧客に対応しています。プラットフォームエンジニアリングマネージャーの Andy Shacklady 氏とクラウドプラットフォームエンジニアリング責任者の Lee Whittingham 氏が率いる Vodafone 社のチームは、HashiCorp Vault を使用して Google Cloud でシークレットを管理しています。Vodafone 社は、個人を特定できる情報（PII）のデータ用として、大量のボリュームに対応できる独自の低遅延の認証付き暗号（AEAD）サービスを実装するために、Vault と拡張可能なプラグインアーキテクチャの使用を検討することにしました。

世界の大手通信事業者の 1 つである Vodafone 社は、3 億を超える移動通信サービス利用者と IoT デバイスからのデータを扱っています。Vodafone 社のエンジニアリングチームは、シークレット管理に Google Kubernetes Engine（GKE）で Vault を使用しながら、ML、AI、ダッシュボード用の Google サービス群を使用しています。この使用を促進するため、Vodafone 社はデータ移動技術または（ユースケースによっては）BigQuery で取り込む PII を匿名化することで、安全を確保し、データプライバシーに関する規制に準拠しています。匿名化が完了すると、AI、ML、およびダッシュボードツーによってビジネス価値が引き出されます。

高速な暗号化に向けた改良

Vodafone 社は当初、いくつかの大きな問題に対処する必要がありました。「PII データ用に Google Tink を実装したかったのですが、私たちには特殊な難しい要件がありました」と、Andy 氏は言います。

Tink はオープンソースの暗号ライブラリで、暗号化と復号化のために AEAD を実装しています。AEAD の実装にはいくつかのパターンがあり、その 1 つが Vault の Key-Value ストアに AEAD 鍵を保存してクライアント側で使用する方法ですが、さらに安全な方法として、サーバー側でデータを匿名化し、AEAD 鍵がクライアントに公開されないようにできます。ただし、このためには転送エンジンのカスタム実装を作成しなければなりません。最も機密性の高い情報は、誰にも知られないようにする必要があります。

また、この新しいソリューションでは、サーバー側での処理に切り替えるだけでなく、1 日につき数十億ビットのデータを匿名化、つまり 1 秒につき最大 1,000 万回の暗号化が必要になります。Vodafone 社が選択するソリューションは、この作業を迅速かつ大規模に行わなければなりません。Vault とその豊富な機能について豊富な知識を持つ Andy 氏とチームは、このソリューションで他にできることはないか探ることにしました。

課題

大量のボリュームに対応できる低遅延の暗号化で、データ取り込みフレームワーク用の Vault または分析ツール用の BigQuery に安全に保管された AEAD 鍵を同期できる機能

サーバー側での鍵のローテーションとライフサイクル管理

管理、暗号化、復号化のロールを分離できる RBAC（ロールベースのアクセスコントロール）のポリシーの作成

プラグインで既成の枠組みを超える

Vodafone 社は、すぐに使える機能と将来のプロジェクトをサポートできる拡張性を兼ね備えた Vault Enterprise に投資しました。Andy 氏のチームは、すでにシークレット管理と複数のデータ分析ストリームに Vault を使用していました。Vault Enterprise が備えているこのような機能、および豊富なガバナンスとポリシー機能によって、Vodafone 社はチームメンバーに付与する権限（データの暗号化や復号化など）を管理するポリシーを作成することができました。また、Vault Enterprise は「きわめて堅牢な」バックアップとリカバリのソリューションでもあり、修復機能も備えています。

チームは、Google Tink エンジンでデータ暗号化を大規模にサポートできるツールも必要としていました。このタスクは Vault の機能ですぐに解決できるものではありませんでしたが、Vodafone 社はこのプラットフォームに可能性を見いだしていました。「私たちは Vault のテストを始め、何ができるのかを探りました。データを大規模に匿名化し、あらゆる種類の鍵を迅速に処理できる機能が必要だったのです」

- チームは Vault の可能性を探るために、独自のプラグインを作成しました。完成したプラグインは、主に次のような機能を備えていました。

- Vault に対応したカスタムシークレットエンジンプラグインでは、匿名化のために Google Tink の鍵セットでデータを暗号化および復号化できます。

- サーバー側で匿名化し、鍵のライフサイクルを管理し、BigQuery と同期します。

- 一時的またはステートレスな暗号化と復号化し、構成と鍵については Vault で安全に保管されます。

「サーバー側での暗号化は演算負荷の高いタスクです」と、Lee 氏は言います。「私たちは、Kubernetes の拡張性を利用して、変化するワークロードの需要に対応することにしました」演算とストレージを分離するために、Lee 氏は 2 つのクラスタをプロビジョニングしました。1 つは Consul for HA ストレージを稼働させるためのクラスタ、もう 1 つは Vault 用の Autopilot クラスタで、高速化のために Vault コンテナイメージに Tink プラグインがプリインストールされていました。これらのクラスタで、高性能な内部ロードバランサ経由の通信が行われました。この分離によって、バックエンドストレージに不要な影響を与えることなく、Vault をすばやくスケールアップできるようになったのです。

Vault の拡張性で新しい可能性を解き放つ

Vodafone 社のチームがプラグインを自力で作成した後、HashiCorp のアーキテクトとソリューションエンジニアが Vodafone 社と協力し、そのプライグインをブラッシュアップしました。Vodafone 社はソリューションをシームレスに動作させるため、HashiCorp のチームの支援を受けながら細かな調整を行い、アーキテクチャとスケーリングのアプローチを見直しました。

Vodafone 社が作成したプラグインによって、運用の変更が可能になりました。この変更のおかげで、Vault で鍵をクライアントに配布する代わりに、データを暗号化してクライアントに送り返せるようになったため、鍵の配布が不要になりました。「私たちはすでに Vault を利用したことがあり、使い方については知識がありました」と、Andy 氏は振り返ります。「そのため、問題は Vault で他に何ができるのかということでした。以前は Vault をシークレット管理ツールとして使っていましたが、今では暗号化エンジンとしても使用しています」

実際、Vault は暗号化エンジン以上のものになっています。Vodafone 社にとって、Vault はセキュリティを組み込んだ完全な実行フレームワークです。Vodafone 社は独自にプラグインを作成できたため、そのプラグインの機能のためのエンドポイントを独自に作成することもできます。Vault は、特定のニーズを満たすものから、どのようなことができるのかを Vodafone 社に示す包括的なツールとなったのです。

Andy 氏は、Vault の可能性に感銘を受けたといいます。「あなたが Vault Enterprise の顧客なら、何ができるかに目を向けてください。自社独自の要件に合わせてプラグインを作成し、可能な限り迅速かつ簡単に動作させることができます」

結果

Vodafone 社は、Vault を拡張し、Google Tink を使ってデータを暗号化および復号化するために、カスタムプラグインを作成し、特定の目的に合わせて細かな調整を行いました。

Google Cloud の水平スケーリングを使用することで、Vodafone 社はテストベッドで、1 秒あたり最大 1,000 万件の暗号化を実現しました。これは 1 時間あたり 360 億件に相当します。

ソリューション

Vodafone 社は HashiCorp と提携し、自社独自のニーズに合わせて Vault を拡張しました。また、独自のプラグインを作成して、Vault をシークレット管理プラットフォームから暗号化エンジンに変えながら、1 時間に数十億バイトを匿名化するのに必要なスピードと精度を確保しました。

Vodafone 社のパートナー

Andy 氏はソフトウェアエンジニアリングマネージャーで、世界的な大手金融機関や通信会社で 20 年にわたってエンジニアリングチームを管理した実績があります。現在は、Google Cloud を使用した Vodafone 社の分析用プラットフォームエンジニアリングに注力しているほか、Infrastructure as Code、クラウドベースのサービス、セキュリティなどを担当しています。Andy 氏は家族と愛犬と一緒にロンドンに住んでいます。

Andy Shacklady 氏
クラウドテクノロジプラットフォーム
エンジニアリング担当マネージャー

仮想化、コンテナ化、およびセキュリティを専門とする Lee 氏は、IT 業界で 30 年以上の経験があります。主に銀行や通信業界で仕事をしてきた同氏は現在、Vodafone 社で Google Cloud プラットフォームエンジニアリング責任者を務めています。住まいはロンドン近郊で、家族とともに生活しています。

Lee Whittingham 氏
クラウドプラットフォーム
エンジニアリング責任者

テクノロジスタック

- **インフラ:** Google Cloud と Anthos
- **ワークロードの種類:** シークレットとカスタムエンジン
- **コンテナランタイム:** コンテナ化
- **オーケストレータ:** Kubernetes – GKE と Anthos
- **CI/CD:** インフラ用 GoCD
- **バージョン管理:** GitHub


HashiCorp