



 SBB CFF FFS |  Adfinis | お客様のケーススタディ

現代の鉄道会社に適した最新の シークレット管理

世界で最も時間に正確な鉄道会社の 1 つが、HashiCorp Vault を使った最新のシークレット管理を導入し、デジタル戦略の基盤を築いています。

// インフラにより実現するイノベーション

SBB 社について

Swiss Federal Railways (SBB) 社は、運行時間の正確さでは世界のトップ 3 に入る鉄道会社です。1902 年に設立し、旅客サービス、不動産、貨物サービス、およびインフラを中核事業としています。また、およそ 34,000 人の社員を抱える、スイスで最大規模の企業の 1 つでもあります。SBB 社は毎日、100 万人近い人々を安全かつ確実に輸送し、時間通りに目的地に送り届けています。同社はスイス全土に線路を張り巡らせているだけでなく、世界一の長さで知られるアルプス山脈のゴッタルドベーストンネルを通じ、スイスと欧州を結んでいます。

SBB 社の鉄道は遠距離輸送を中心として人気が高く、時間に正確で、毎日、11,260 本の列車を運行しています。各列車が定刻から 3 分以内に出発、到着する確率は 91.9% です。この素晴らしい運行実績を維持し、さらに柔軟な消費者エクスペリエンスを提供しながら二酸化炭素排出量を削減するため、SBB 社は 2030 年に向けた戦略に基づき、デジタルトランスフォーメーションに乗り出しています。この戦略では、信頼性の高い運行体制の強化を目指す 4 つの柱で構成されています。

SBB 社の基本情報



適切な形でセキュリティを強化



定時運行に対する顧客の期待に応えられるよう IT システムを安定化



開発者の俊敏性を高めてビジネスリスクを低減



開発者ファーストのアプローチにより、自社システムとのシームレスな統合を実現



重要な IT システムのセキュリティを自動化



継続的なトランスフォーメーションのガイドとなるユースケースを構築

「Vault は回復力と安定性に優れた、可用性の高い製品です。また、そのシークレット管理はスイスのアーミーナイフのように多機能で、さまざまな統合機能をすぐに利用できるため、スピーディーなロードマップにも対応できます」

ANDREAS MEISTER 氏
エンジニアリングチーム責任者兼セキュリティアーキテクト

鉄道を超えたつながり

SBB 社のデジタル戦略は、同社の顧客志向のアプローチの強化、効率の向上、中核事業の成長、それにカーボンニュートラルの達成を目標としています。このような目標を達成するには、鉄道ネットワークとそのコンポーネントやシステムとの相互接続性を高める必要があります。これには、発券システムや交通管理システム、顧客情報システム、各種 IoT デバイス、IT バックボーン、そして最も重要な存在である顧客が含まれます。SBB 社の各列車は、いわば線路を走る小さなデータセンターなのです。

これらのシステムを更新、接続するために、SBB 社のチームは自社のあらゆるツールで安全に認証できる仕組みを必要としていました。そのための証明書、トークン、またはログインクレデンシャル（「シークレット」）をアクセス可能にしながら、権限のないユーザーから保護しなければならなかったのです。堅牢な認証を実現するには、拡張性と信頼性に優れ、機能の豊富なシークレット管理が不可欠です。デジタル化を成功させるには、どのようなソリューションを採用したとしても、ハードコード化されたシークレットやプレーンテキストのシークレットを排除してセキュリティ体制を強化し、重要な IT システムのセキュリティを自動化する必要があります。

課題



SBB 社の IT チームは、開発者ファーストのアプローチを採用したソリューションを必要としていました。



SBB 社はきわめて複雑な鉄道ネットワークを 24 時間休みなく運営しているため、どのようなシークレット管理ソリューションを実装するとしても、高可用性の実現に最適な状態と柔軟なオプションを必要としていました。



未来志向のデジタル化を実現するために、緊密に統合できるソリューションを求めています。シークレット管理ツールは、汎用性が高く、スピーディーなロードマップに対応できることが条件でした。

「どれほど優れたプラットフォームであっても、使わなければ当社にとって意味がありません。そのため、私たちは開発者のトレーニングと彼らへの周知に努めるだけでなく、自動化にも投資したのです」

ANDREAS MEISTER 氏
エンジニアリングチーム責任者兼セキュリティアーキテクト

Vault を選んだ理由: シークレット管理の取り組み

エンジニアリングチームの責任者兼セキュリティアーキテクトの Andreas Meister 氏は、同社のデジタル化で中心的な役割を果たしています。同氏がシークレット管理に関して社内から問い合わせを受けたのは、かなり前の 2019 年 3 月のことでした。クレデンシャルの保護は、同社のトランスフォーメーションの間、重要なポイントになりました。

Meister 氏とチームは、想定するシークレット管理ソリューションに求められる要件をまとめました。どのようなプラットフォームを選ぶとしても、シークレットを適切に保管し、シークレットへのアクセスを簡素化し、ビジネスリスクを最小化できることが条件でした。このような要件から、HashiCorp Vault が SBB 社のニーズを最も満たすものであることが、すぐに明らかになりました。

「私たちが Vault を選んだ理由は主に 3 つあります」と、Meister 氏は述べています。「開発者ファーストのアプローチであることが、SBB の IT チームに最適でした。Vault は回復力と安定性に優れた、可用性の高い製品です。また、スイスのアーミーナイフのように多機能なシークレット管理のおかげで、多くの統合機能をすぐに利用できるため、スピーディーなロードマップにも対応できます」

スタートから半年で本稼働を実現

「プロジェクトを成功させるには、適切な人々との協力が不可欠です」と、Meister 氏は強調します。コラボレーションは、Vault 導入のあらゆる面で鍵となるものです。アプリケーションセキュリティチームは、SBB 社の ID アクセス管理 (IAM) チームと協力しました。また、SBB 社のすべての関係者が、クラウドネイティブな Linux ベースのワークロードの計画、構築、実行を手がけるグローバルなオープンソースサービスプロバイダである Adfinis 社と連携しました。

Adfinis 社で最高技術責任者を務める Michael Hofer 氏は、両社の提携を次のように振り返ります。「コラボレーションはきわめて重要で、両社の関係の核となるものでした。私たちはスタートから本稼働まで、Vault 環境を提供しました」Adfinis 社は、戦略、アーキテクチャ設計、エンジニアリングなどの面で SBB 社による Vault の導入をサポートしました。ここで重要なのは、コラボレーションによって SBB 社のサイト信頼性エンジニアが、Vault の運用で中核的な役割を果たせるようになったことです。

SBB 社と Adfinis 社は、SBB 社が運用する OpenShift プラットフォームで 4 つの Vault クラスタを実装しました。これらのプライマリクラスタは、AWS とセカンダリクラスタ、Swiss OTC、T-Systems のプライベートクラウドプラットフォームを利用しています。

「プラットフォームの構築にあたり、私たちが重視したのは自動化プロセスです。これは構成全体のコード化を意味しており、GitOps はたんなる用語ではありません。チームは、あるクラウドから別のクラウドへの完全な移行を数時間で実現できました」と、Hofer 氏は述べています。

そして、関係者全員の協力によって Vault をシームレスかつ迅速に稼働させることができました。「私たちの仲間が Vault プラットフォームを半年足らずで構築し、すでに最初の顧客を獲得していることは驚異的な事実です」と、Meister 氏は述べています。

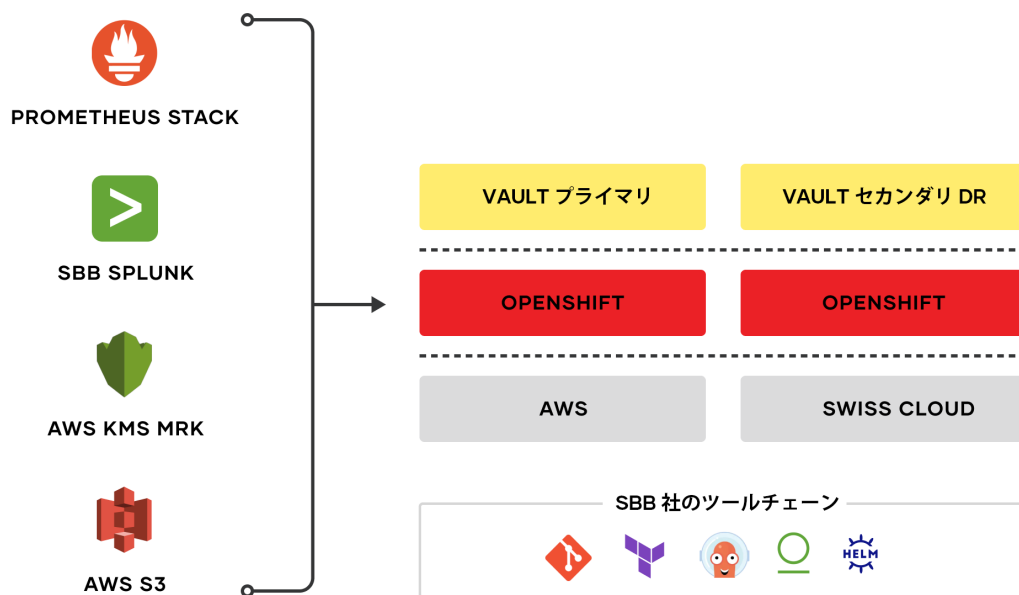


図 1: Vault プラットフォームのテクノロジスタック

顧客志向を改めて重視

「どれほど優れたプラットフォームであっても、使われなければ当社にとって意味がありません。そのため、私たちは開発者のトレーニングと彼らへの周知に努めるだけでなく、自動化にも投資したのです」と、Meister 氏は説明します。

SBB 社の AppSec チームは Vault を実装するだけでなく、さまざまなプレゼンテーションを作成し、Vault のトレーニングを企画しました。また、Meister 氏のチームは、開発者向けのチュートリアルをはじめとする包括的なドキュメントをまとめました。あらゆるものを連携させ、開発者が Vault に簡単にアクセスできるようにするため、チームは SBB 社の開発者向けセルフサービスポータルを強化しました。今では、開発者は手動プロセスを行うことなく、Vault（およびその他のツール）へのアクセスをリクエストできます。このプロセスを自動化し、提供する特権アクセスを最小限に抑えることによって、強固な Vault 管理を実現しています。

今後の取り組み

Meister 氏は、このシークレット管理の取り組みが将来のトランスフォーメーションの基盤になるだろうと考えています。

「このユースケースが私たちのガイドとなりました」と、同氏は言います。

今では、Vault とネイティブに統合されていないものも含め、SBB 社が利用している他のアプリケーションも Vault の恩恵を受けています。他のアプリケーションが Vault をすでに活用できているという事実は、Vault がガイドとしての役割を果たしている何よりの証拠です。このソリューションのおかげで、SBB 社の開発者は、機密性の高いクレデンシャルの漏えいを恐れることなく、必要なツールを必要なタイミングで入手できるようになりました。Vault は SBB 社のセキュリティを適切な形で強化しています。

結果



高度な自動化によって開発者のシークレットを安全に保管し、IT の俊敏性向上とビジネスリスクの低減を実現



API やデータベースでシークレットのハードコード化やプレーンテキストへの保存を排除し、セキュリティ体制を大幅に強化



SBB 社の重要な IT システムのセキュリティを自動化することによって、顧客の高い期待に応えながら将来の IoT 強化の基盤を構築

ソリューション

Vault のセットアップは安全性と回復力に優れ、シンプルで、SBB 社のコンテナファーストのマルチクラウド戦略とシームレスに統合できます。すぐに使える各種統合機能を備えた Vault は、回復力と信頼性に関する SBB 社の要件を満たし、同社が世界で最も時間に正確な鉄道会社の地位を維持できるよう支援しています。

SBB 社のパートナー



Andreas Meister 氏は、ソフトウェアアーキテクチャ、アジャイルメソッド、コード設計、DevSecOps、およびエンジニアチームの仕事に熱意を持って取り組んでいます。また、大規模プロジェクトと SME 環境の両方で培った豊富な経験を生かして、SBB 社のエンジニアリングチームを統括し、大規模な鉄道ネットワークの技術的基盤を継続的に改善しています。

Andreas Meister 氏
エンジニアリングチーム
責任者兼セキュリティ
アーキテクト

Adfinis 社のパートナー



Michael Hofer 氏
エンジニアリング責任者

Michael Hofer 氏が設計しているオープンソースのソリューションは、同氏が余暇に作っているパティセリーのように、緻密で美しく、バランスが取れています。Adfinis 社でエンジニアリング責任者を務める同氏は、デジタル化のギャップを埋め、組織をサポートすることに注力しています。



Simon Nussbaum 氏
クラウドネイティブエンジニア

Simon Nussbaum 氏は、Adfinis 社のクラウドネイティブチームに所属しています。エンジニア兼アーキテクトとして、コンテナ、シークレット管理、サービスメッシュに関連したあらゆる業務のガイダンスを作成し、提供しています。



Pascal Reeb 氏
クラウドネイティブエンジニア

Pascal Reeb 氏は Adfinis 社のクラウドネイティブエンジニアとして、Kubernetes、HashiCorp Vault、Consul などのエンジニアリングソリューションについて世界中の組織をサポートしています。

テクノロジースタック

- インフラ: AWS および Swiss Cloud
- コンテナランタイム: OpenShift
- オーケストレータ: OpenShift、Kubernetes
- CI/CD: Argo CD、Jenkins
- バージョン管理: Bitbucket
- プロビジョニング: HashiCorp Terraform OSS、Helm
- 構成管理: ServiceNow
- セキュリティ管理: HashiCorp Vault

Adfinis 社について

オープンソースは Adfinis 社の中核事業です。

Adfinis 社は 20 年以上前にオープンソースソリューションの市場に参入した大手サービスプロバイダです。Adfinis 社は企業としてオープンソースコミュニティに深く関与し、革新的かつ持続可能で、信頼性の高い IT インフラの開発に貢献しています。HashiCorp、Red Hat、SUSE、GitLab などのパートナーと提携し、初めての問い合わせからソリューションの最適化まで、さまざまな場面で顧客を支援しています。これには、統合の計画策定から 24 時間年中無休の運用やマネージドサービスまで、あらゆる業務が含まれます。

Adfinis 社は、スイス、オランダ、オーストラリアに拠点を持ち、90 人以上の従業員を抱えています。また、従業員は社内でのどのような役割を担っていても、常に「技術者精神」を持っていることに誇りを抱いています。

詳細はこちら: adfinis.com

