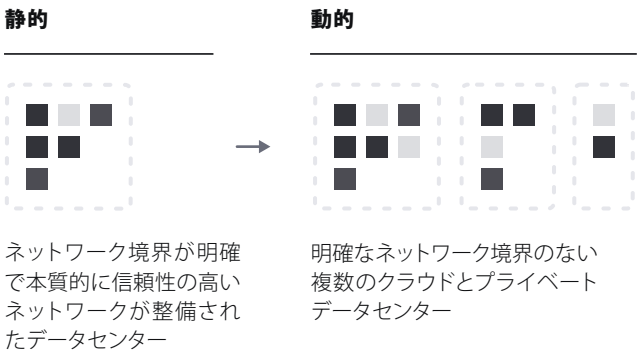
Vault

クラウドセキュリティの自動化

パブリッククラウドやプライベートクラウドで
シークレットを管理し機密データを保護

インフラのセキュリティ上の課題

クラウドを導入すると、静的なインフラから脱却して、動的なインフラのプロビジョニングと管理へと移行することができます。動的なインフラでは、無制限の容量およびサービスの配信、一時性とイミュータビリティの導入、複数の環境へのデプロイを実現できます。

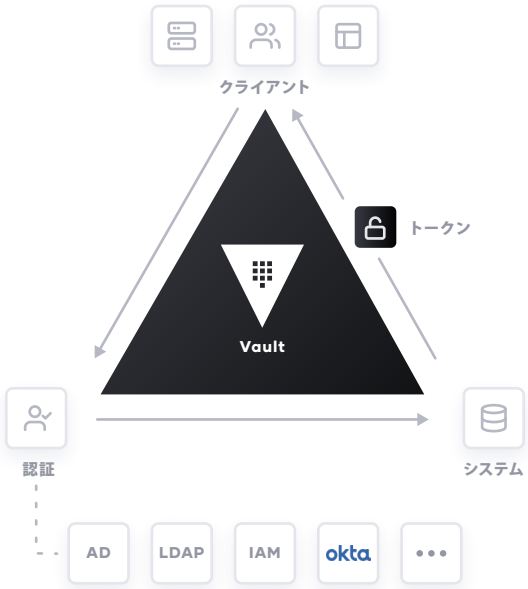


HashiCorp Vault

Vault では、UI、CLI、または HTTP API を使ってトークン、パスワード、証明書、暗号化キーなどの機密データを保護および保存し、機密データへのアクセスを厳密に制御できます。

こうしたシークレット操作をすべて一元管理することで、システム、ライセンス、オーバーヘッドを削減し、生産性を向上させてコストを節減できます。また、シークレットを一元化してハードコードされた静的なクレデンシャルを取り除くことで、セキュリティ侵害のリスクの低減にも役立ちます。

- **アイデンティティの違いを吸収**：多様なクラウドでの認証、多様なクラウドへのアクセス、ポリシーの実施、容易な自動化を実現
- **単一のワークフロー**：既存のインフラと連携させてコストを削減し、統一された監査証跡を作成。
- **オープンソースで拡張が可能**：強力なオープンソースコミュニティ、大規模なパートナーのエコシステム、フル装備のマルチクラウドシークレットエンジンを提供。



ソリューションとメリット

データ漏えいのリスクが低減

Vault で一元管理および保護された暗号化キーを使い、転送中と保管中の機密データを暗号化します。すべて単一のワークフローと API を通じて行われます。

セキュリティ侵害のリスクが低減

Vault でシークレットを一元管理し、信頼性の高いアイデンティティに基づいてアクセスを厳密に制御することで、ハードコードされた静的なクレデンシャルを取り除きます。

生産性が向上

開発チームはアプリケーションデリバリプロセス中に自動的にシークレットを使用でき、単一の API を使ってプログラムにより機密データを保護できます。

統合

- 信頼性の高いアイデンティティを使い、多種多様なクラウド、システム、エンドポイントを認証しこれらにアクセス
- キーの一元管理と、シンプルな API を使ったデータの暗号化と復号によって、アプリケーションデータのセキュリティを確保
- トークン、パスワード、証明書、暗号化キーといった動的なシークレットの一元的な保管、アクセス、配布が可能
- 異機種混合環境で統一されたサポートを提供。現在使用しているワークフローやテクノロジと連携可能

導入企業

Adobe

BARCLAYS

SAP Ariba

SPACEFLIGHT

cruise

credit karma

機能

	Open Source 個人向け	Enterprise 大規模企業向け
動的なシークレット	✓	
シークレット用ストレージ	✓	
安全なプラグイン	✓	
詳細な監査ログ	✓	
シークレットのリースと破棄	✓	
ACL テンプレート	✓	
Vault Agent	✓	
ワークフローの初期化と Unseal	✓	
キーのローテーション	✓	
クラスタ管理用 UI	✓	
エンティティおよびアイデンティティグループ	✓	
アクセス制御ポリシー	✓	
アイデンティティ用プラグイン	✓	
Encryption as a Service	✓	
トランジットバックエンド	✓	
暗号化キーのローテーション	✓	
エンティティおよびアイデンティティグループ	✓	
アクセス制御ポリシー	✓	
アイデンティティ用プラグイン	✓	
AWS KMS での自動 Unseal	✓	
Azure Key Vault での自動 Unseal	✓	
GCP Cloud KMS での自動 Unseal	✓	
Integrated Storage	✓	
Open Source 版の全機能		✓
ディザスタリカバリ		✓
ネームスペース		✓
データレプリケーション		✓
データレプリケーションフィルタ		✓
Read 処理専用のノード		✓
制御グループ		✓
HSM での自動 Unseal		✓
多要素認証		✓
Sentinel との統合		✓
FIPS 140-2 とシールラップ		✓
KMIP のサポート		✓
Transform		✓

HashiCorp

www.hashicorp.com