# EntrustとHashiCorpは安全性の高い集中型シークレット管理を企業に提供

Entrustハードウェア・セキュリティ・モジュールは、HashiCorpの集中型シークレット管理ソリューションで使用されるマスター鍵をラップして保護します

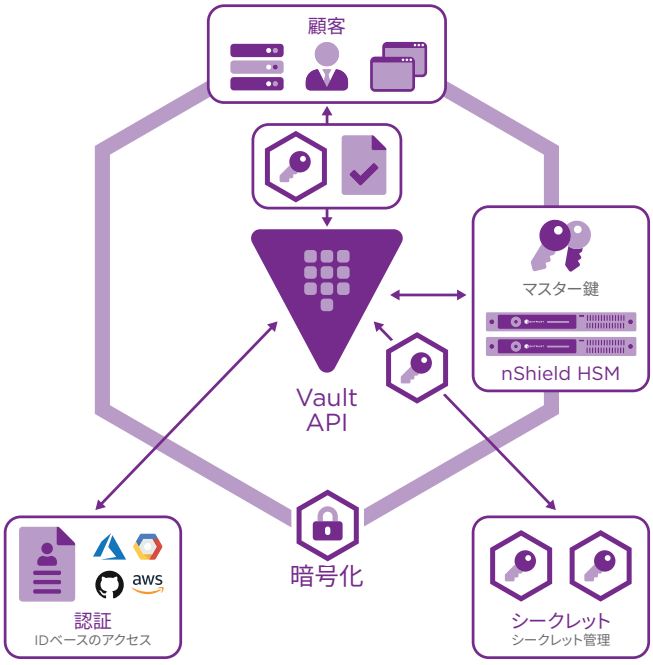
**ハイライト**

- 秘密資産の安全な生成、暗号化、復号を実現
- 複数環境にわたる企業のコンピューティングのニーズをサポート
- シークレット管理を一元化・集約することで生じるリスクを軽減
- 規制された市場のニーズに対応し、リスクを低減して規制に準拠
- FIPS 140-2レベル3およびコモンクライテリアEAL4+認定の信頼の基点を提供

## 問題: シークレット資産の管理に対する一貫したセキュリティポリシーがない

シークレット資産を保管するための安全な独自のリポジトリを提供する企業アプリケーションが増加するにつれ、企業のサイロ化が明るみになってきており、部署ごとに異なるライフサイクル管理と保護ポリシーによって異なるシークレットを保有している状態が見受けられます。一元管理されていない限り、トークン、パスワード、証明書、API鍵などのシークレットはさまざまな場所に存在する可能性があります。

シークレットの保管場所を把握せずに一貫性のない管理ポリシーを適用すると、リスクと監査上の課題が生じます。組織全体でシークレット管理を一元化することで、ポリシーを一律に施行し、監査と規則への準拠を容易にすることができますが、同時に高度なセキュリティが必要となります。




nShield®ハードウェア・セキュリティ・モジュール(HSM)は、企業秘密、資格情報、その他のシークレット資産を暗号化するVaultのマスター鍵をラップすることにより、HashiCorp Vaultの開封に使用される鍵を保護します。

**詳細をチェック:ENTRUST.COM/ja/HSM**

# 安全性の高い集中型シークレット管理を提供

## 課題: 集中型シークレット管理アーキテクチャ全体でのリスク管理

シークレット管理を組織全体で一元化することで、一貫したセキュリティポリシーの実施が可能になり、シークレットの無秩序な増加を排除できます。しかし、シークレットを1か所に集約するには高度なセキュリティが必要となります。企業がさまざまなオンプレミス環境やマルチクラウド環境においてコンピューティングリソースにアクセスできるよう、集中型シークレット管理リポジトリを保護する信頼の基点を確立することが重要です。

## ソリューション: HashiCorp Vaultによる、Entrustの高セキュリティHSMの信頼の基点を使用した集中型シークレット管理

HashiCorp Vaultは、企業秘密を単一で安全な集中型リポジトリに集約し、一貫したライフサイクル管理とポリシーへの準拠を実現します。このソリューションを使用することで、企業はアプリケーションのデータへのアクセスを許可すると同時に、秘密を保護することができます。HashiCorp Vaultは、動的シークレットを一元的に保存、アクセス、配信することで、アプリケーションとアプリケーションが処理するデータを安全に保ちながら、一貫したセキュリティポリシー準拠の監査を容易にします。

集中管理モデルの下で秘密を集約することによって生じる潜在的なリスクを軽減するため、HashiCorp Vaultは、Entrust nShield ConnectのオンプレミスHSMやnShield as a ServiceのクラウドベースHSMと統合して、Vaultのマスター鍵を保護する堅牢な信頼の基点を確立します。この統合ソリューションにより、信頼できるアイデンティティとポリシーの実施に基づいてアクセスが集中管理され、シークレットの無秩序な増加を排除できます。

## Entrust nShield HSMとHashiCorp Vaultを併せて使用する理由は?

認定取得済みのHSMの暗号境界外で処理される暗号鍵は、攻撃に対して非常に脆弱であり、重要な鍵の侵害につながる可能性があります。重要な暗号データの保護または監査を可能する、実績のある方法はHSMのみです。Entrust nShield HSMはHashiCorp Vaultと統合し、Vault内のデータを開封するマスター鍵に対する包括的で論理的、かつ物理的保護を可能にします。また、これらを組み合わせることで、セキュリティポリシーを実施するための監査可能な方法を提供し、規制への準拠を容易にします。

Entrust nShield ConnectとnShield as a Serviceを使用することで、HashiCorpユーザは次のことが可能になります。

- 堅牢なアクセス制御メカニズムを用いて慎重に設計された暗号境界内でVaultのマスター鍵を保護し、鍵は使用目的の許容範囲を制限可能
- 高度な管理、保管、冗長性機能を使用してマスター鍵の可用性を認証し、HashiCorp Vaultが必要なときにいつでも鍵にアクセス可能
- 要求の多いマルチクラウドアプリケーションに対応する、優れたパフォーマンスが可能

# 安全性の高い集中型シークレット管理を提供

## Entrust HSM

Entrust nShield HSMは、最高のパフォーマンスを発揮し、非常に安全で、簡単に統合できるHSMソリューションのひとつであり、規制への準拠を促進すると同時に、企業、金融機関、政府機関に最高レベルのデータセキュリティとアプリケーションセキュリティを提供します。

当社独自のSecurity World鍵管理アーキテクチャは、鍵へのアクセスおよび鍵の使用を厳重かつきめ細かく制御します。

## HashiCorp

HashiCorpは、マルチクラウドインフラストラクチャ自動化ソフトウェアにおけるリーダー企業です。同社のソフトウェアスイートにより、企業は一貫したワークフローを採用し、さまざまなアプリケーションのあらゆるインフラストラクチャをプロビジョニング、保護、接続、実行することができます。HashiCorpのオープンソースツールは、グローバル2000の企業で広く採用されています。同社の企業向け製品は、共同、運用、管理、マルチデータセンター機能を促進する機能を備えており、それらのオープンソースツールを強化します。

**www.hashicorp.com**

## 詳細

Entrust nShield HSMの詳細については、**entrust.com/ja/HSM**をご覧ください。アイデンティティ、アクセス、通信、データに関するEntrustのデジタルセキュリティソリューションの詳細については、**entrust.com/ja**をご覧ください。

Entrust nShield
HSMの詳細はこちら：

**HSMinfo@entrust.com**
**entrust.com/ja/HSM**

## ENTRUSTについて

Entrust は信頼できる認証、支払い、データ保護を実現することで、動き続ける世界をセキュアにしています。今日、支払いや国際取引、電子政府サービスへのアクセス、そして企業ネットワークへの認証において世界中でより安全で円滑なユーザ体験が求められています。Entrust はこれらの要となる部分において、他に類を見ない幅広いデジタルセキュリティとID発行ソリューションを提供しています。2,500人を超える従業員、グローバルパートナーネットワーク、そして150カ国以上におよぶ顧客に支えられ、世界で最も信頼されている組織から信頼されています。

詳細は下記URLをご覧ください。
**entrust.com/ja/HSM**



**お問い合わせ：**
**HSMinfo@entrust.com**