Entrust KeyControl BYOK

暗号化されたワークロードのためのマルチクラウドの鍵管理

ハイライト

クラウドを利用しつつ、暗号鍵の制御を最大化したいと考えている組織にとって、Bring Your Own Key (BYOK)は安全な鍵の出どころを保証できるだけでなく、クラウドプロバイダーから独立してライフサイクル管理、自動化、鍵のバックアップ機能を自社で確保することができます。

- 鍵のライフサイクル管理機能によって、下記のきめ細かな制御および自動化が可能:
  - 鍵の交換
  - 鍵の期限
  - 鍵の破棄
  - 鍵のバックアップ
- シングルクラウド、マルチクラウト、そしてハイブリッドクラウドにも対応
- 簡単な統一プラットフォームで下記のような管理が可能:
  - KeyControlで生成した鍵やネイティブMicrosoft Azure Key VaultやAWS KMSの鍵
- Microsoft AzureやAWSのクラウド環境におけるBYOK機能は、暗号鍵の生成や制御を御社で行うことが可能
- 鍵生成のための高品質なエントロピーソースを活用するため、FIPS 140-2 レベル3認定取得済みのEntrust nShield® ハードウェア・セキュリティ・モジュール(HSM)とのシームレスな統合が可能

仮想化環境におけるワークロードのセキュリティ管理は、管理者にとって複雑な課題

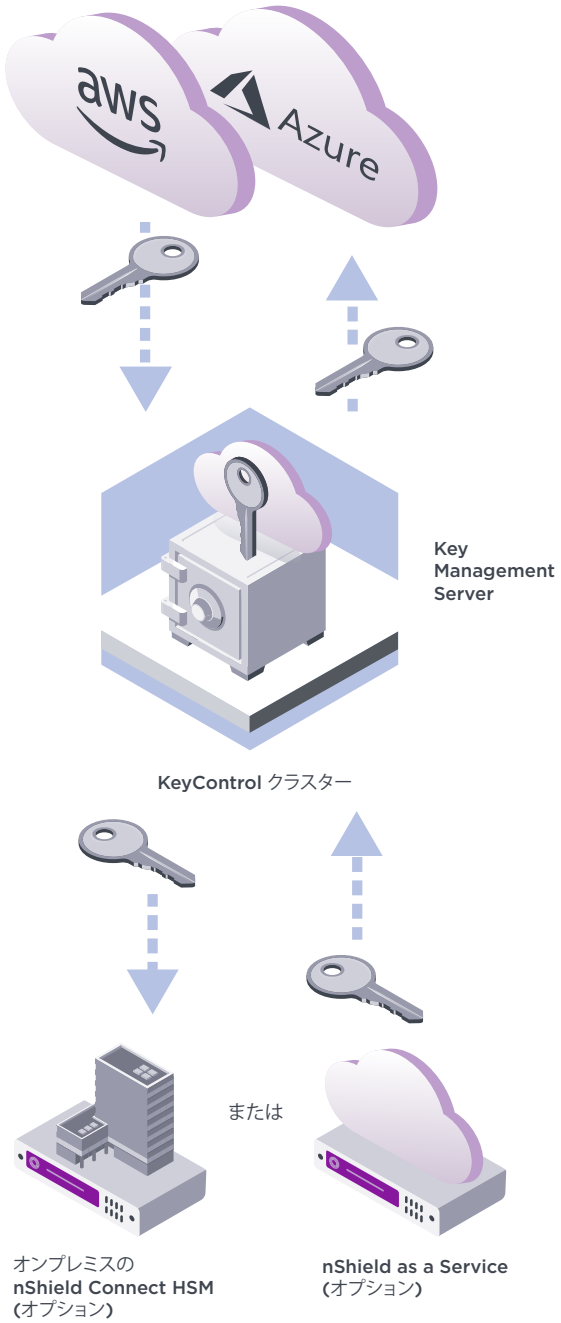
ワークロードをクラウドに移行したいと考えている組織でも、クラウドサービスプロバイダー(CSP)によって使用される鍵の制御は維持したいと考えていることでしょう。それには下記の理由があります。

- 暗号鍵はクラウドで使用するアプリケーションに必要
- セキュリティを重視している組織は、ライフサイクルを通して鍵を制御したいと考えている
- CSPが生成した鍵はそのCSPへの依存度が高く、他のCSPへの移行が困難である
- CSPは透明性が低い – 自分たちの鍵がどこでどのように作成され、どこにバックアップされたのかを確認することができない
- 多くの組織は鍵管理プロセスを最初から最後まで自動化したいと考えている

Entrust KeyControl BYOK(旧HyTrust製品)を使用することで、大量の暗号鍵を容易に管理することができます。FIPS(連邦情報処理規格)140-2準拠の暗号化で、KeyControl BYOKは自社で管理しているオンプレミスで鍵を生成し、鍵のストレージ、分配、交換、廃棄を含む暗号鍵のライフサイクルを自動化および簡素化し、BYOKプロセスを簡素化することができます。

KeyControl BYOKの詳細は、entrust.com/ja/cloud-securityをご覧ください。

Entrust KeyControl BYOK



主な機能および特長

エンタープライズレベルの拡張性と性能

KeyControl BYOKはすべての仮想マシンとデータストアの暗号鍵を管理し、大規模な運用においては、数千もの暗号化ワークロードをサポートできるまでに拡張することができます。1つのクラスターに最大8つの鍵サーバを追加することができます。

AzureおよびAWSへのBYOK

KeyControl BYOKではMicrosoft AzureとAWSのユーザマスター鍵およびAzureとAWSのネイティブ鍵に対して、単一の管理コンソールで鍵を一元管理することができます。これはMicrosoft AzureおよびAWSで生成したネイティブ鍵のライフサイクル管理を可能にするだけでなく、独自の暗号鍵を生成したい場合は制御、自動化および管理を最大限に行うことができ、自社環境で作成した鍵のMicrosoft AzureおよびAWSへの持ち込みも可能となります。これには、以下のような多数のメリットがあります。

- Bring Your Own Key（BYOK）の安全な鍵生成とMicrosoft AzureおよびAWSへのエクスポートの工程を簡素化
- nShield HSMを活用し、エントロピーソースから暗号鍵要素を作成
- Microsoft AzureおよびAWS上でのマスター鍵の完全な管理
- 鍵はKeyControl BYOKにバックアップ（復元可能）され、ユーザによる制御を維持
- きめ細かな鍵のライフサイクル管理：期限切れへの対応（無効化、鍵要素の削除）および鍵の交換

KeyControl BYOKの詳細は、entrust.com/ja/cloud-securityをご覧ください。

Entrust KeyControl BYOK

対応するプラットフォーム

パブリッククラウドプラットフォーム: AWSおよびMicrosoft Azure

対応するオペレーティングシステム

CentOS、Red Hat Enterprise Linux、Ubuntu、SUSE Linux Enterprise Server、Oracle Linux、AWS Linux、Windows Server Core 2012/2016/2019、Windows Server 2012 R2/2016/2019、Windows 8.1/10

デプロイメントメディア

OVA (Open Virtual Appliance)、AMI (Amazon Web Services marketplace)、ISO、VHD (Microsoft Azure marketplace)

技術仕様

VMware認定取得済みKMS（vSphere 6.5/6.7/7.0、vSAN 6.6/6.7/7.0、vSphere Trust Authority 7.0）に対応

アクティブクラスタ構成による高可用性(HA)対応(1クラスタあたりKMSサーバ8台まで)

オプションでEntrust nShield HSMを連携させることにより、オンプレミスまたはas a serviceにおいてFIPS 140-2 Level 3に準拠

すべての登録クライアント間でTLS 1.2の使用をサポート

Entrust KeyControl BYOKのライセンスは標準のKeyControl（KMIP準拠のワークロード用製品）とは別のライセンスとなります。KeyControl BYOK単体、または標準のKeyControlと一緒に実装してライセンス共有となります。KeyControl BYOKは一連のデータ暗号化とマルチクラウド鍵管理シリーズの一製品です。詳細は下表をご覧ください。

ENTRUSTの製品	製品の特長	備考
KeyControl BYOK	独自の暗号鍵を生成し、AWS、Microsoft Azure、あるいはGoogle Cloud Platformに持ち込むためのソフトウェア	KeyControl BYOK単体でライセンス取得、またはKeyControlやDataControlと使用してライセンスを共有
KeyControl	KMIPが有効になっているワークロードのための暗号鍵管理ソフトウェア	KeyControl単体でライセンス取得、または KeyControl BYOKやDataControlと使用してライセンスを共有
DataControl	マルチクラウド環境における仮想マシンのきめ細かなエージェントベースの制御および暗号鍵の管理	DataControl単体でライセンス取得、またはKeyControlやKeyControl BYOKと使用してライセンスを共有
CloudControl	クラウドの機密データを不適切な構成から保護するワークロードセキュリティポリシー実施および仮想化環境およびコンテナ環境におけるコンプライアンスの自動化	

詳細は下記URLをご覧ください。
entrust.com/ja/cloud-security

エントラストジャパン株式会社
DPS事業本部
東京都港区台場二丁目3番1号
トレードピアお台場
HSMinfo@entrust.com