Entrust DataControl

データ暗号化、マルチクラウドの鍵管理、およびワークロードのセキュリティ

ハイライト

- ワークロードライフサイクルの暗号化徹底管理
- エンタープライズ鍵管理サーバ（KMS）
- 仮想マシン（VM）の強力できめ細かい暗号化：起動（OS）とデータパーティションの暗号化
- 管理者の権限分散を実現するアクセス制御
- Entrust nShield® HSMとのシームレスな統合により、FIPS 140-2 レベル3認定取得済みの「信頼の基点（Root of Trust）」を確立

暗号化されたワークロードの管理は、特にマルチクラウド環境で複雑に

ワークロードはステージングからデプロイメント、バックアップ、そして最終的なデコミッショニングまで、さまざまなライフサイクルを経ます。その段階ごとに、データの窃盗や不正使用といったさまざまなリスクをもたらします。

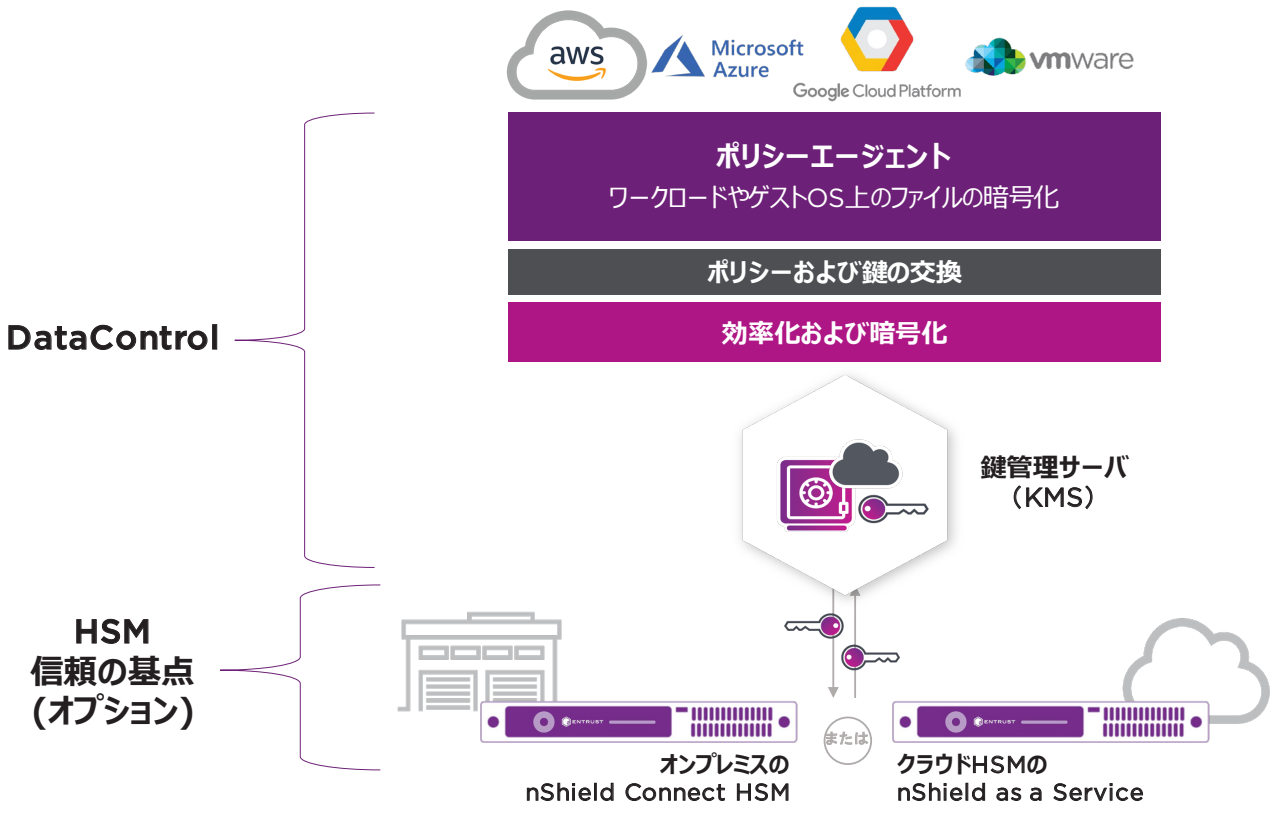
ワークロードの暗号化だけでは不十分

セキュリティ確保のためには、データの暗号鍵を頻繁に交換することが重要です。しかし、各クラウド事業者のプラットフォームでワークロードの暗号化を管理することは複雑で、ポリシーの不整合や人的ミスが起こるリスクが高くなります。それに対し、内蔵の鍵管理ポリシーを利用することで複雑さを軽減し、一貫性を確保することができます。

Entrust DataControl（旧HyTrust製品）は、マルチクラウドのワークロードをライフサイクルを通じて保護し、異なるクラウドプラットフォームのワークロードの保護を簡素化します。これにより、自社の重要で機密性の高い情報の保護を強化することができ、データプライバシー規制の遵守にも対応することができます。

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

Entrust DataControl



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
- AWS Linux
- Windows Server Core (2012 R2 / 2016 / 2019)
- Windows Server (2012 / 2012 R2 / 2016 / 2019)
- Windows 8.1 / 10

デプロイメントメディア

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

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

Entrust DataControl

主な機能および特長

マルチクラウドインフラにおける暗号化ワークロードの管理

DataControlでは、オンプレミスや主要なパブリッククラウドプラットフォームなど、さまざまなインフラに存在する暗号化されたワークロードを管理することができるうえ、すべての暗号鍵を一元管理できる、拡張可能なソリューションを利用することができます。DataControlとVMware認定の鍵管理サーバ（KMS）であるEnturst KeyControlを使用することで、より良いセキュリティを確保することができます。

強固なワークロード保護

DataControlは、きめ細かな暗号化により、優れたセキュリティを実現します。ハイパーバイザーやデータストアの保護に留まらず、VMも個別に暗号化されます。VM内では、起動（OS）ディスクやスワップパーティションなど、各パーティションに固有の鍵を割り当てて暗号化を行うことができます。

導入および管理の容易さ

DataControlでは、1つのインターフェイスですべてのワークロードの暗号化が可能なため、プラットフォームごとに異なる暗号化機能を使用する手間を省くことができます。

- 優れたユーザエクスペリエンス
- ゼロダウンタイムの暗号化
- 高可用性クラスタリングによる、ディザスタリカバリの確保

アクセス制御

DataControlはポリシーベースの堅牢なアクセス制御により、異なるユーザペルソナ間で権限分散を実現します。暗号化されたボリュームに対してアクセス制御を施行することで、ルートユーザやシステム管理者が機密データにアクセスできないように設定することができます。

重複排除に対応

従来はデータを暗号化すると、すべてのデータブロックが異なる内容になるため、暗号化と重複排除は両立できないという問題がありました。それに対しDataControlでは独自のアプローチにより、ストレージでの91%の重複排除効果を保ちながら、AES 256ビットの暗号化を実現します。

対応するプラットフォーム

- **プライベートクラウドプラットフォーム**
  - vSphere
  - OVHCloud
  - VxRail
  - Pivot3
  - NetApp
  - Nutanix
- **パブリッククラウドプラットフォーム**
  - Amazon Web Services (AWS)
  - IBM Cloud
  - Microsoft Azure
  - VMware Cloud (VMC) on AWS
  - Google Cloud Platform (GCP)
- **対応するハイパーバイザー**
  - ESXi
  - AWS
  - Azure
  - KVM
  - GCP

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

Entrust DataControl

技術仕様

- 起動（OS）、スワップ、およびデータの各パーティションの暗号化
- UEFIセキュアブートドライブを含む、Windows GPTブートドライブの暗号化に対応
- パーティションごとの個別鍵
- Intelハードウェアアクセラレーションを使用した強力なAES（128/256ビット）暗号化対応
- FIPS 140-2 レベル1認定取得の暗号鍵管理。FIPS 140-2 レベル3認定取得のEntrust nShieldハードウェア・セキュリティ・モジュールとシームレスに統合可能
- 鍵変更の自動化により、ゼロダウンタイムの暗号化を実現
- Windows VM向けのパーティションのサイズ変更
- アクティブ - アクティブの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）
- 単一の暗号鍵で重複排除に対応
- VMware vSphereとvSANの暗号化に関する 認定取得済み
- DevOpsを実現する、RESTベースのAPIインテグレーション
- ブートおよびクローンの保護により、暗号化されたワークロードを不正アクセスから保護

DataControlは、データ暗号化、マルチクラウド鍵管理、仮想マシンおよびコンテナ化ワークロードのセキュリティポリシーコンプライアンスをサポートする製品シリーズの一部です。詳細は下表をご覧ください。

ENTRUST製品	製品の特長	備考
KeyControl BYOK	独自に生成した暗号鍵をAWS、Microsoft Azure、Google Cloud Platformに持ち込む場合に利用	KeyControl BYOK単体でライセンス取得、またはKeyControlやDataControlと組み合わせ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	KeyControl単体でライセンス取得、またはKeyControl BYOKやDataControlと組み合わせ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と組み合わせて導入が可能
CloudControl	仮想化環境およびコンテナ化環境におけるワークロードのセキュリティポリシーの自動適用とコンプライアンス対応により、クラウドの設定ミスに対する機密データの保護	

詳細は下記URLをご覧ください

entrust.com/ja/cloud-security

ENTRUST

エントラストジャパン株式会社
データセキュリティソリューション営業本部
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