MicrosoftとEntrust独自のBYOKソリューションにより、クラウド環境におけるセキュリティと信頼を強化

Microsoft

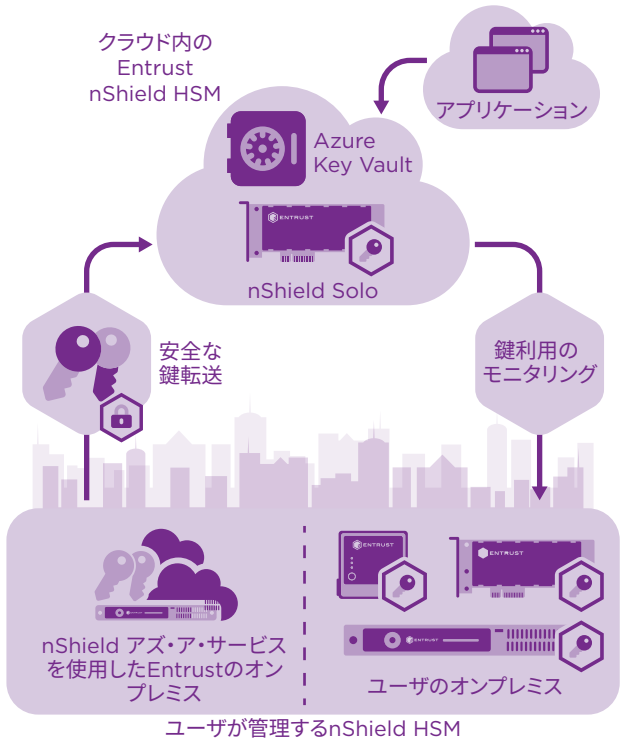
Microsoft Azure Key VaultとEntrust nShield HSMによるクラウド上の機密データおよび鍵の制御権を提供

ハイライト

- FIPS140-2認定取得済み環境において鍵を保護
- クラウド上のアプリケーションにとって鍵が可視的とならないことを保証
- アプリケーション管理機能と鍵管理機能を分離
- 暗号鍵とアプリケーションシークレットに関するきめ細かな制御が可能
- 従量制サービスの提供により迅速な拡張が可能

問題点：パブリック・クラウド・サービスでは通常、制御権を放棄する必要がある

パブリック・クラウド・インフラストラクチャでは、共有サービスに関して、テナントの実行とストレージスペースにおける明確な境界を常に設けているわけではありません。クラウド・サービス・プロバイダーは、暗号を使用して機密データへのアクセスを制御するほか、機密データの守秘性および整合性を保護します。ただし、このようなサービスのセキュリティは、暗号鍵に与えられた保護レベルに依存しており、暗号鍵が漏洩した場合には機密データが流出する可能性があります。



Entrust nShield HSMを使用することで、独自の鍵を生成して使用することにより、クラウド内でデータを保護できるようになります。

詳細をチェック：ENTRUST.COM/ja/HSM

独自のBYOKソリューションにより、クラウド環境におけるセキュリティと信頼を強化

課題：機密データを保護する暗号鍵の制御権を維持すること

クラウドサービスは、必要に応じて迅速に導入や拡張が行えます。このような環境でデータを保護するためには、クラウドアプリケーションで使用している暗号鍵を制御する必要があります。暗号鍵とアプリケーションシークレットに関する制御権を維持することは、パブリック・クラウド・サービスの信頼性と堅牢性を高めるために不可欠です。

ソリューション：Microsoft Azure Key Vaultと、Entrust nShield HSMにより強化された鍵管理を組み合わせて使用する

Microsoft Azure Key Vaultは、クラウド上にユーザ独自の安全なコンテナを作成することができます。Entrust nShield®ハードウェア・セキュリティ・モジュール（HSM）で機密データと鍵を保護および管理し、Microsoft Azure Key Vaultでユーザによる制御権の維持を可能にします。Entrust nShield HSM は、クラウド上のソフトウェア環境とは別に暗号鍵を保護するため、クラウドで実行されている認証済みアプリケーションは鍵を使用できますが、鍵を見ることはできません。

独自の鍵の持ち込み（BYOK）オプションを使用すると、所有するEntrust nShield HSMを使用して鍵を生成した後、それらの鍵を、Microsoftが所有するクラウド内にあるHSMに安全に転送できます。Microsoftは鍵のキャッシュコピーを取得し、Azure内の許可されたアプリケーションがその鍵を利用できるようになります。この鍵はディザスタリカバリのために複数のHSM間で複製できますが、ハードウェアは鍵がHSMの外部で可視的にならないようにします。BYOKは、これらの鍵がnShieldの「Security World」と呼ばれる認定取得済みのセキュリティ境界内で鍵がかかった状態で維持されることを保証します。セキュリティを強化するために、ほぼリアルタイムの使用ログが提供されており、ログを参照することで、Azureによって鍵がいつどのように使用されたかを正確に確認できます。ユーザは鍵の所有者として、鍵の利用状況をモニタリングし、必要に応じて鍵へのアクセスを取り消すことができます。

Entrust HSMを Microsoft Azure Key Vaultと組み合わせて使用する理由

Entrust nShield HSMは、クラウド上の機密データの暗号鍵の保護と管理を行います。Entrust nShield HSMは次のことを可能にします。：

- Security Worldによって作成されたセキュリティ境界を出ることなく、暗号鍵を生成して安全に転送
- FIPS 140-2認定取得済みの暗号境界内でMicrosoftの所有下にある期間中も鍵を保護
- 堅牢なアクセス制御メカニズムと強制的な権限分散を通して、暗号鍵が常に利用可能な状態にあり、許可された目的にのみ使用されることを保証

独自のBYOKソリューションにより、クラウド環境におけるセキュリティと信頼を強化

高保証のクラウドセキュリティ

クラウドは共有セキュリティインフラストラクチャを備えた共有サービスにすぎないため、クラウドで維持されている機密データは脆弱であるという認識を、Entrust nShield HSMは覆します。Entrust nShield HSMは、次のことを可能にします。

- 強化された耐タンパ環境で鍵を保護
- セキュリティ機能を管理タスクから分離し、セキュリティポリシーを適用
- 公共部門、金融サービス、企業の規制要件を満たすこと

Entrust HSM

Entrust nShield HSMは、最高の性能と安全性を備え、簡単に統合できるHSMソリューションの1つであり、規制コンプライアンス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ています。

当社独自のSecurityWorld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。

Microsoft

Microsoftは、企業によるアプリケーションの実行ならびにコンテンツの作成および共有の方法や、コラボレーションプロセスの構築方法を変革してきました。Microsoft Azure Key Vaultに基づくシステムは、クラウドサービスをよりアクセスしやすく、かつ安全なものにしています。Microsoft Azure Key Vaultは、暗号を使用してデータを保護することで、次のことを可能にする、信頼できるビジネス環境を確立します。

- Active Directoryへのアンカーを使用して、データや鍵に関する制御権を維持
- 迅速で拡張可能な配備とコストパフォーマンスに関するクラウドへの期待を維持
- アプリケーション管理と鍵管理の権限分散をサポート

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。

Microsoft Partner
Microsoft
Gold Application Integration
Gold Datacenter

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