# 独自の鍵を保持することで、高保証の鍵管理を実現

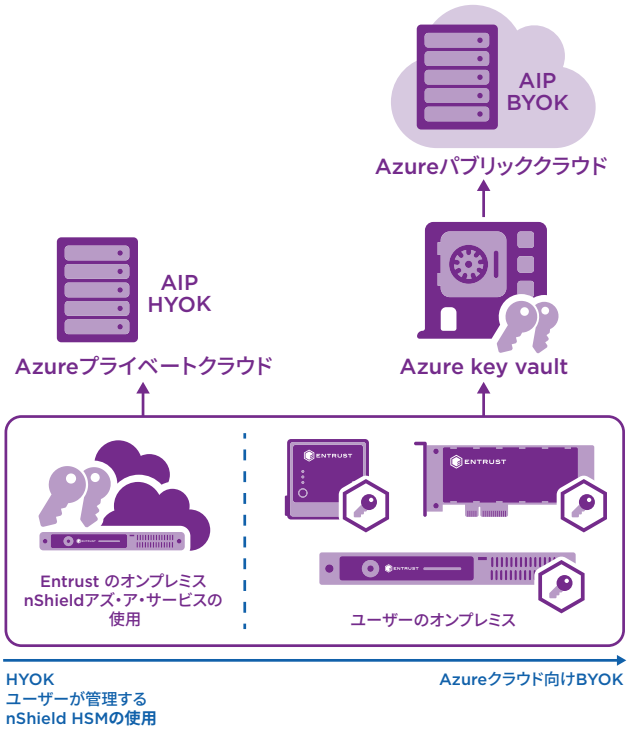
## MicrosoftとEntrustが持続的な情報保護と鍵管理オプションを提供し、ユーザによるクラウドセキュリティ管理を実現します

**ハイライト**

- 交換するデータへのアクセスおよび使用の制御を適用する
- 制御するHSMで鍵を自ら保持し、保護する
- FIPS 140-2認定を受けた鍵のライフサイクル管理を提供する
- Microsoftへの鍵の非開示を保証する

Microsoft Azure Information Protection (AIP)は、データタイプを問わず、データ資産に強制力のあるセキュリティポリシーを埋め込むことにより、共同作業環境内で利用されるデータを保護します。クラウドサービスとして、ITインフラストラクチャを使用せずにオンデマンドでAIPを実行し、企業全体で情報を確実に保護することができます。

AIPは暗号化を採用し、データへのアクセス制御と持続的な保護を提供します。AIPのセキュリティは、重要な暗号鍵に与えられている保護レベルに基づいており、暗号鍵が公開されると、機密データが危険にさらされることになります。




AIPをオンプレミス、ハイブリッド構成、またはクラウドで使用する場合でも、Entrust nShield® HSMが重要な鍵をしっかりと制御します。

**詳細をチェック：ENTRUST.COM/ja/HSM**

# 独自の鍵の保持により高保証の鍵管理を実現

## 課題: 機密性の高いデータをオンプレミスで保持するには暗号鍵が必要

ほとんどのデータはAzure内で安全に管理できますが、一部の機密データは、共有したり独自のセキュリティ境界外に送信することは一切できません。このような機密コンテンツは、アクセスと共有を最小限に制限し、オンプレミスでのみセキュリティ管理を行う必要があります。

AIPは、独自のセキュリティ境界内で機密性の高いデータを管理するために、オンプレミスコンポーネントによって有効化されるHold Your Own Key（HYOK: 独自の鍵の保持）のオプションを提供します。このオプションでは、ユーザーのオンプレミス、またはサービス環境で使用されるEntrustハードウェア・セキュリティ・モジュール（HSM）を介して、鍵管理を行います。

Entrust nShield® HSMは、重要な鍵を保護し、機密データのセキュリティを強化する、ロックされた保管庫を作成します。

## ソリューション: Entrustの強力な鍵制御を備えたHYOKを展開

Entrust nShield HSMは、AIPの展開で使用される暗号鍵の管理と使用を厳重に制御します。

Entrust nShield HSMは、重要な鍵を保護するハードウェアソリューションを提供します。nShield HSMは、ソフトウェア環境から完全に独立した鍵を保護・管理し、鍵の保持と完全な自主制御を可能にします。

鍵は、独自のnShield HSMのセキュリティ境界内で生成・管理されるため、機密性の高いデータを保護することができます。

## Entrust HSMをAIPやHYOKと併せて使用する理由

Entrust HSMにより、オンプレミス、クラウド、ハイブリッド構成のいずれの場合でも、データセキュリティのニーズに合わせてAIPを柔軟に使用することができます。nShield HSMの機能は次の通りです。

- FIPS 140-2認定の暗号境界内で鍵を保護する
- 鍵が許可された目的にのみ使用されるよう、義務の分離が強制された厳重なアクセス制御メカニズムを採用する
- 鍵の管理、保管、によって鍵の可用性を保証する

Azure Key Vaultで鍵を保存し、鍵をAIPと共に使用する場合、Entrustが鍵のセキュリティを強化するようサポートし、ユーザは自ら管理するnShield HSMを使用して鍵を生成し、Azure Key Vaultに安全に転送することができます。また、Bring Your Own Key（BYOK: 独自の鍵の持ち込み）機能により、鍵とクラウド内のデータのセキュリティをユーザによって制御することができます。

# 独自の鍵の保持により高保証の鍵管理を実現

## Entrust nShield HSM：

- 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、企業の規制要件に準拠
- FIPS 140-2レベルおよびコモンクライテリア認定を取得

## Entrustは特定のパフォーマンスと予算のニーズに合わせすことができます。

- 大容量の鍵の生成と管理を行う（またはハイブリッド展開の一部として使用する）場合は、nShield Solo HSMの組み込み型PCIeカード型や、nShield Connect HSMのネットワーク接続型アプライアンスが、高性能のハードウェアセキュリティを提供
- nShield Connect HSMは、ユーザのオンプレミスまたはnShield as a Service環境に導入可能
- BYOK機能の一部としてオンプレミスで低容量の鍵を生成する場合は、nShield Edgeが、便利なUSB接続型ハードウェアセキュリティを提供

## 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。

## Microsoft

Microsoftは、企業による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に変革を起こしました。Microsoftのソリューションに基づくシステムが、生産性を最大限に高めます。データを保護するため、Microsoft AIPは暗号化で、次のような信頼できるビジネス環境を確立します。

- 企業全体のIDを管理
- 認証用の証明書を配布
- データリソースへのユーザアクセス権を制御
- 総合的な情報保護を提供

**www.microsoft.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**

ENTRUST



**お問い合わせ：**
**HSMinfo@entrust.com**