nShield Bring Your Own Keys: BYOKによりクラウドユーザによるデータセキュリティのきめ細かな制御が可能

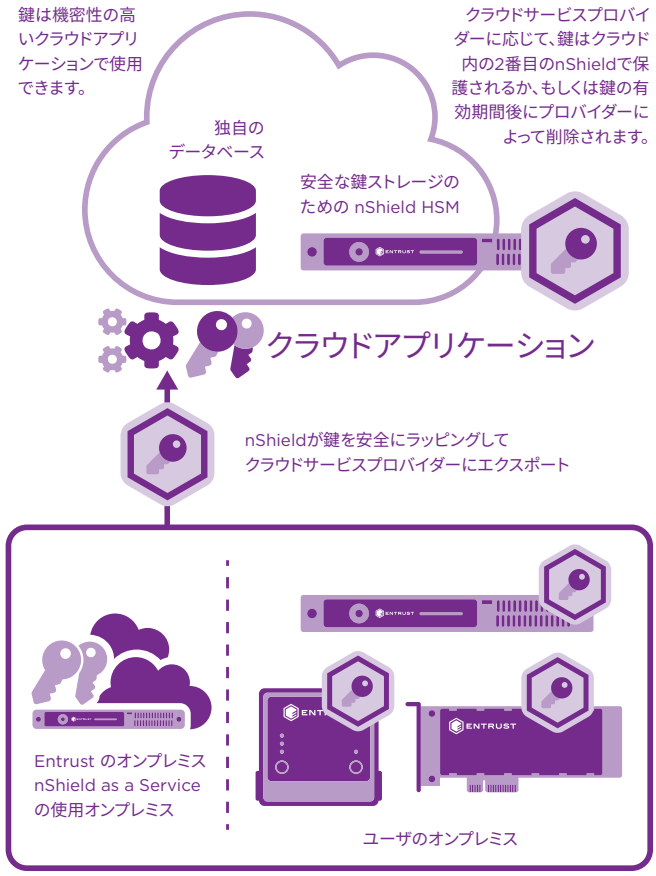
クラウドの利便性とセキュリティの両立

ハイライト

- クラウド内の機密データのセキュリティを強化する、より安全な鍵管理
- FIPS認定ハードウェアで保護されたEntrust nShield®の高エントロピー乱数ジェネレーターを使用した、より強力な鍵生成
- より優れた鍵制御：独自の環境で独自のnShield HSMを使用して鍵を作成し、クラウドへ安全にエクスポート
- クラウドとオンプレミスのどちらで鍵を使用しても、より一貫した鍵管理を実現

nShieldハードウェア・セキュリティ・モジュール（HSM）を採用することで、Amazon Web Services（AWS）、Google Cloud Platform（GCP）、Microsoft Azureのいずれを使用する場合でも、クラウドアプリケーションへの独自の鍵の持ち込み（Bring Your Own Keys: BYOK）が可能になります。

高保証のnShield HSMを使用することで、クラウドサービスが持つ柔軟性と経済性を活用しながら、鍵管理の安全性を高め、より優れた鍵制御を実現することができます。



Entrust独自のSecurity Worldアーキテクチャが、マスター鍵の安全な長期保管と災害復旧保護を提供

詳細をチェック：ENTRUST.COM/ja/HSM

クラウドユーザによるデータセキュリティの自主管理を実現

nShield BYOKの役割

nShield BYOKにより、nShield HSMを使用して、機密性の高いクラウドホスト型アプリケーション、データベース、大容量ストレージの保護に不可欠な鍵の生成、保管、管理が行えます。nShield BYOKが提供する機能は次のとおりです。

- ハードウェアの信頼の基点を基盤として使用: nShield HSMは、信頼性が高く、FIPS 140-2レベル3認定を受けた耐タンパ性デバイスです。同HSMは、クラウドサービスの信頼の基点として機能し、暗号鍵と署名鍵を安全に生成して保護します。
- nShieldを使用して鍵を管理：クラウドホスト型アプリケーションに機密データが存在する場合、nShield HSMが鍵を生成してラッピングし、クラウドアプリケーションに安全に送ります。
- 鍵の可用性を制御：オンプレミスであってもnShield as a Service環境であっても、nShield HSMを完全に自主制御できるため、鍵の生成やエクスポートのタイミングを独自に決定することができます。また、マスターコピーを制御することで、クラウドプロバイダーへのさらなるエクスポートを実施するタイミングを制御することができます。
- クラウドプロバイダーを選択可能：nShield BYOKでは、それぞれの鍵に使用するクラウドプロバイダーを自由に選択できます。これにより、nShieldの信頼性の高い鍵の生成・保護機能を活用すると同時に、オンプレミスやnShield as a Service環境から、さまざまなアプリケーションに最適なクラウドを柔軟に選択することができます。

nShield BYOKを利用するには

AWS、GCP、またはAzureでnShield BYOKの利用を開始するには、nShield HSMが必要です。以下のソリューションから選択できます。

- nShield Connect: ネットワーク接続型アプライアンス
- nShield Solo: サーバー組み込み型PCIeカード
- nShield Edge: 低容量アプリケーション向けのUSB接続型デバイス
- nShield as a Service: サブスクリプションベースのnShield Connect HSMを使用

最高の保証を得るには、Entrust BYOKをMicrosoft Azureと併せてご使用ください。参照：**https://protect-eu.mimecast.com/s/PYBnCWnYocOBORVImMJzG?domain=docs.microsoft.com** 実装の支援が必要な場合は、次のオプションパッケージを購入できます。

Bring Your Own Key、Azureプロフェッショナルサービス
このパッケージには、nShield Edge、Entrustプロフェッショナルサービスチームによって提供される統合サポート、および1年間のメンテナンスが含まれています。

nShield Connect、nShield Solo、nShield Edge とプロフェッショナルサービスを個別に購入することも可能です。

Microsoftオープンスタンダード方式を使用してAWS、GCP、またはMicrosoft AzureでnShield BYOKを使用するには、次のEntrustパッケージが必要です。

Cloud Integration Option Pack
このオプションパックには、オンプレミス型のnShield HSMを使用して鍵をラップし、Azure BYOKを使用してAWS、GCP、またはMicrosoft Azureに鍵を安全に転送および貸し出すために必要なものがすべて含まれています。

nShield BYOKとAWS、GCPまたはAzureをご自分で統合する場合も、Entrustプロフェッショナルサービスをご利用いただくことで、シームレスかつ効率的に接続することができます。

クラウドユーザによるデータセキュリティの自主管理を実現

nShield BYOKの仕組み

Entrustは、nShield HSMを使用して鍵を生成し、長期保管を保証し、鍵をクラウドにエクスポートするメカニズムを提供します。オンプレミスまたはnShield as a Serviceから鍵をクラウドにエクスポート後、次のいずれかの方法で鍵を管理します。

Microsoft Azureを使用する場合：

Microsoft Azureを使用して最高の保証を得るために、Entrust BYOKを選択することができます。これにより、鍵をAzureにアップロードするために満たす必要のある条件を制御し、Microsoftが鍵を使用してできることを厳しく制限することができます。

Azureのインフラストラクチャ内で運用されているnShield HSMに鍵を安全に転送して、両サイドでHSMの安全性を確保します。

AWSまたはGCPを使用する場合：

クラウドで一時的に使用するため、AWSまたはGCPに鍵を貸し出します。所定の期間が経過すると、クラウド内の鍵は破棄されます。必要に応じて、HSMに保管された鍵を再び貸し出すことができます。

どのパブリッククラウドサービスを選択する場合も、独自の鍵を生成し、鍵のエクスポートを制御することで、クラウド内の機密データとアプリケーションを強力に保護することができます。

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にかつきめ細かく制御します。

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