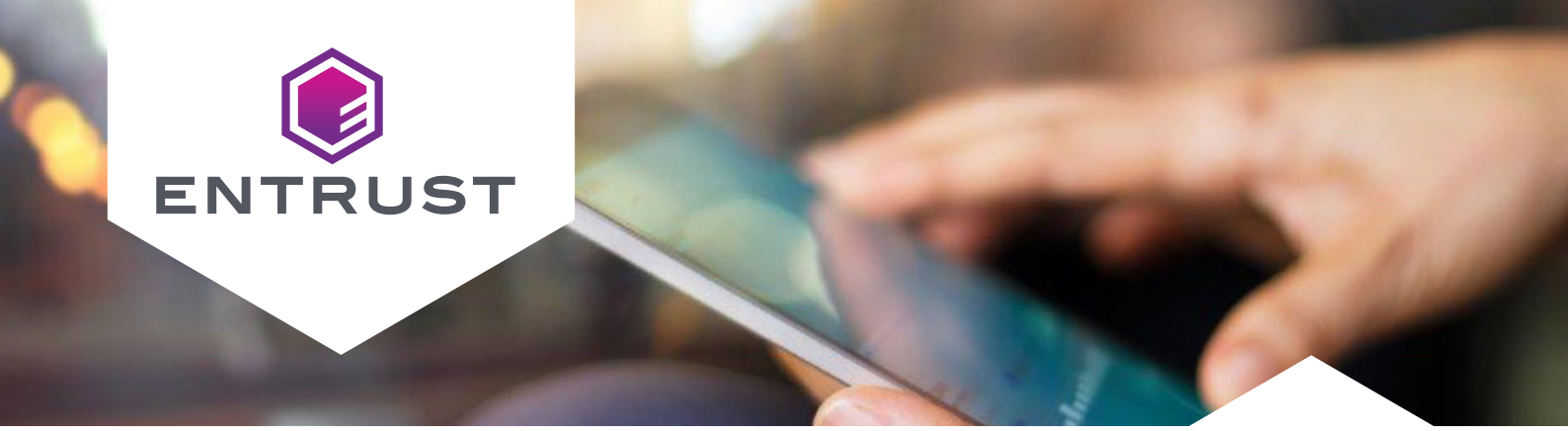

nShield Web Services Option Pack

高保証ハードウェア・セキュリティ・モジュール向けの クラウド対応RESTfulインターフェイス

ハイライト

- クラウド、データセンター、オンプレミス型のアプリケーションに高度なセキュリティ保護を提供
- nShieldハードウェア・セキュリティ・モジュールの暗号化サービスへの効率的で簡単な接続
- 迅速で拡張可能な動的なアプリケーション展開を実現
- 柔軟なOSおよびアーキテクチャサポート

nShield Web Services Option Pack（WSOP）は、暗号鍵やデータ保護サービスを必要とするアプリケーションと、FIPS認定のnShieldハードウェア・セキュリティ・モジュール（HSM）の間にRESTful[1] APIを提供します。nShield HSMは、暗号化、復号化、署名、検証、鍵の生成といったさまざまな暗号化機能を実行します。これらの主要な機能は、世界共通のHTTPSプロトコルを利用したシンプルなWebサービスインターフェイスを介して、アプリケーションで使用できるようになっています。

主な機能と利点

- **クラウド、データセンター、オンプレミス型のアプリケーションからのリモート暗号化サービスへの効率的なアクセス:** クラウド内、リモートデータセンター内、またはローカルに存在するアプリケーションは、RESTful APIを介してhttpsベースのWebサービスを呼び出すことでnShieldサービスにアクセスでき、今日の多様なコンピューティング環境にさらなる柔軟性をもたらします。
- **合理化された開発プロセス:** 効率的な最新のWebサービスインターフェイスにより、nShield HSMの暗号化サービスにアクセスするアプリケーションの開発速度を向上します。
- **クライアント側での統合が不要:** 通常、アプリケーションをnShield HSMと統合するには、ローカルホストのライブラリに結び付け、ローカルサービスを展開する必要があります。WebサービスのRESTful APIを使用することにより、開発者は展開の複雑さを軽減することができます。

nShield Web Services Option Pack

- **柔軟なOSおよびアーキテクチャサポート:** WebサービスのRESTfulインターフェイスは、クライアントアプリケーションのインフラストラクチャから独立しており、アプリケーション用のOS別ソフトウェアを必要としないため、特にカスタム環境での統合が簡素化されます。
- **動的な拡張性:** さらなるHSMの構成、サポートソフトウェアのインストール、またはクライアントライセンスを必要とすることなく、新規や追加のアプリケーションワークロードをスピンアップできます。コンテナアーキテクチャに展開されたWSOPのノードを含め、簡単に需要に対応できるよう、容量を調整します。
- **専用のCOTS（商用オフザシェルフ）アプライアンスを使用したロードバランシングをサポート:** WSOPにより、COTSのロードバランサーでHSMのワークロードを管理することができます。このプロセスの簡素化により、HSMのプールを常に最大限に活用できます。

nShield Web Services Option Packの使用を開始するには

必要なもの:

- Security Worldソフトウェアv12.6x以降
- nShield Solo HSM、nShield Connect HSM、nShield as a Serviceサブスクリプション

RESTful APIを使用するには、nShield WSOPをnShieldクライアントサーバにインストールすることで、サービスをアクティブ化し、アプリケーションから即時に直接接続できるようになります。

WSOPはデフォルトで、テスト目的にのみ使用する一時的かつ短期的なTLS証明書によって構成されています。構成は、継続的なテストまたは本番環境での使用に適した証明書によって更新する必要があります。

nShield Connect HSMの場合: 標準のクライアントライセンスは、Webサービスを実行しているクライアントサーバにのみ必要です。クライアントライセンスは、アプリケーションの接続には必要ありません。

注1: REST（REpresentational State Transfer）はWeb標準ベースのアーキテクチャで、データ通信に世界共通のHTTPプロトコルを使用します。HTTPは、各コマンドが独立して実行され、その前に実行されたコマンドを認識しないため、ステートレスプロトコルとみなされます。RESTはリソースベースであり、すべてのコンポーネントが、HTTPを呼び出す共通のインターフェイスによってアクセスされるリソースとみなされます。

WSOPのRESTfulの属性は次の通りです。
- 「リソース」を一意に識別する明確に定義されたURI（/keys、/sign、/verifyなど）。
- リソースでアクションを実行する動詞としてのHTTPメソッド。例: 鍵の一覧表示などの読み取り操作には「GET」、鍵の作成などの書き込み操作には「POST」、鍵の削除などの削除操作には「DELETE」。

詳細をチェック: ENTRUST.COM/ja/HSM

nShield Web Services Option Pack

技術仕様

nShieldとの互換性

nShield WSOPは、nShield Solo HSMおよびnShield Connect HSMのすべてのモデルと互換性があります。WSOPは、サポートされているバージョンのLinux OSを実行するホストにインストールする必要があり、また、nShield Security Worldソフトウェアのインストールが必要です。WSOPは、オペレーターカードセットとソフトカードで保護された鍵をサポートします。またWSOPは、nShield Container Option Packとも互換性があり、コンテナ化された環境にWSOPを連携することができます。

APIとの互換性

nShield HSMは、webサービスAPIを使用するアプリケーションと、サポートされている他のAPI（PKCS#11、Java、CNGなど）を使用するアプリケーションをサポートします。

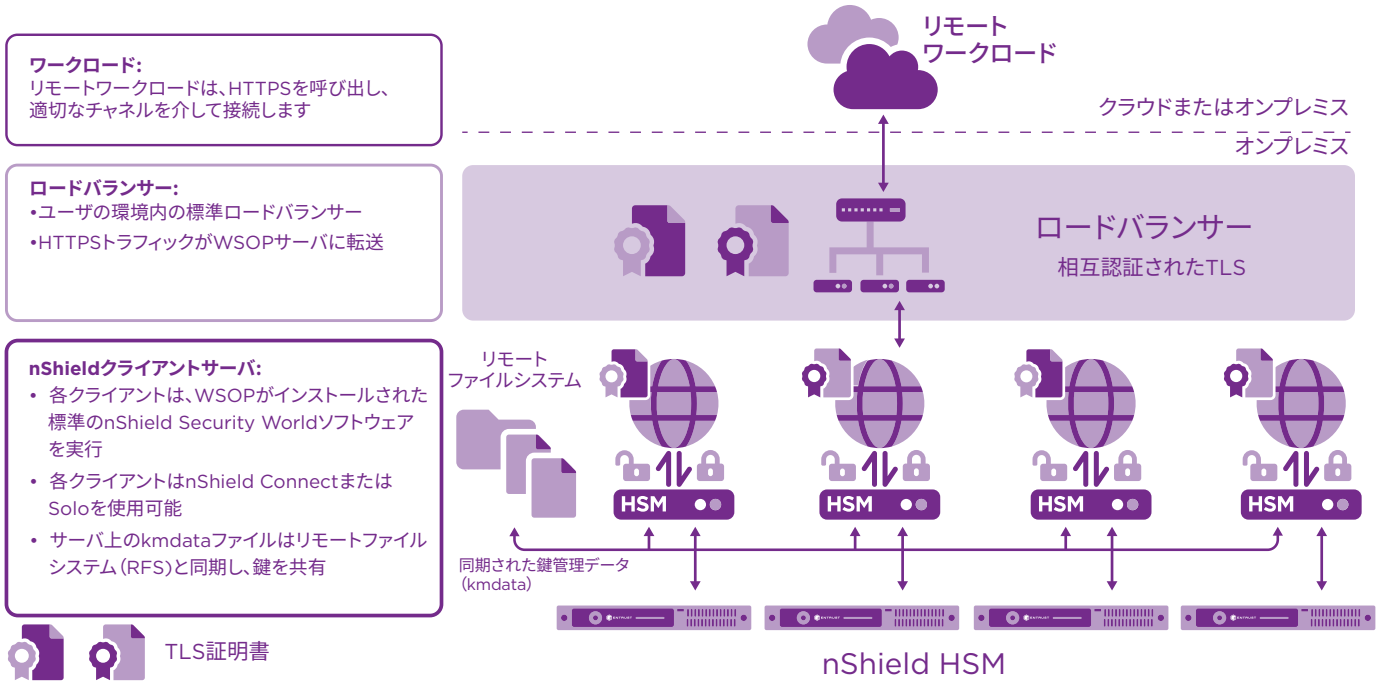

図1: 典型的なWSOPの展開

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、データ向けの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