nShield 汎用ハードウェア・セキュリティ・モジュール

ENTRUST

SECURING A WORLD IN MOTION

目次

信頼できるセキュリティ

EntrustのnShieldハードウェア・セキュリティ・モジュール（HSM）は、企業の機密性の高いデータを保護する、強化された耐タンパデバイスです。FIPS 140-2認定を取得した適格モジュールは、暗号鍵と署名鍵の生成、管理、保管などの暗号化機能と、保護された境界内での機密機能を実行します。

強力なセキュリティを実現するnShield HSMは、以下のようなサポートが可能です。

- より高度なデータの安全性と信頼性を実現
- 重要な規制基準に確実に準拠
- 高いサービスレベルとビジネスの機敏性を維持

nShieldシリーズ

汎用HSMのnShieldシリーズには下記のモデルがあり、あらゆる環境に対応可能です。

nShield Connect

ネットワーク接続アプライアンス

nShield Connect HSMは、ネットワーク全体に分散されたアプリケーションに暗号化サービスを提供します。nShield Connect HSMには、定番のnShield Connect+ HSMシリーズと、高性能なnShield Connect XC HSMシリーズの2つのシリーズがあります。

nShield Edge

ポータブルUSBベースモジュール

nShield Edge HSMは、優れた利便性と経済性を実現するよう設計されたデスクトップデバイスです。nShield Edgeは開発者にとって理想的なHSMで、少量のルート鍵の生成などのアプリケーションに適しています。

nShield Solo

アプライアンスまたはサーバ組み込み用PCIeカード

nShield Solo HSMは、サーバまたはアプライアンスでホストされるアプリケーションに暗号化サービスを提供する、PCIeカードモジュールです。nShield Solo HSMには、定番のnShield Solo+ HSMシリーズと、高性能なnShield Solo XC HSMシリーズの2つのシリーズがあります。

nShield as a Service

クラウド内のnShield HSMをサブスクリプション型のサービスで利用可能なソリューション

nShield as a Serviceはサブスクリプションモデルを介して、FIPS 140-2 レベル3認定を受けた専用のnShield Connect XC HSMへのアクセスを提供します。このソリューションは、オンプレミスのHSMと同じ特長と機能にクラウドサービス環境のメリットを合わせて提供します。これにより、ユーザは「クラウドファースト」を達成し、アプライアンスの保守管理をEntrustのエキスパートに任せることができます。セルフマネージド型とフルマネージド型のサービスオプションがあります。

幅広い用途をサポート

Entrustシステムの利用者は、nShield HSMを、公開鍵基盤（PKI）、SSL/TLS暗号鍵の保護、コーサイニング、デジタル署名、ブロックチェーンなど、さまざまなビジネスアプリケーションの信頼の基点として使用しています。「モノインターネット（IoT）」の成長に伴うデバイスIDと証明書への需要増加に対応し、nShield HSMは、デジタル証明書を使用したデバイス認証などの重要なセキュリティ対策を引き続きサポートします。

またnShield HSMは、今日のコンパクトなコンピューティング環境に最適な、高速トランザクションを提供する楕円曲線（ECC）暗号アルゴリズムや、業界で非常に広く使用されているオペレーティングシステムとAPIなど、幅広い暗号化アルゴリズムをサポートします。

nShieldシリーズの機能

クラウド対応のWebサービスインターフェイス

オプションのnShield Web Services Option Packは、Webサービスの呼び出しを通じてコマンドを実行することにより、アプリケーションとHSM間のインターフェイスを簡素化します。この革新的なアプローチにより、アプリケーションをnShieldに直接統合する必要がなくなり、OSおよびアーキテクチャ構成への依存がなくなるため、展開を簡素化することができます。Web Services Option Packは、クラウドと従来のデータセンターでホストされるアプリケーション双方に対応しています。

オンプレミスまたはクラウドでのコンテナ環境に対応

nShield Container Option Packは、Entrustの高保証ハードウェア・セキュリティ・モジュール（HSM）を基盤とするコンテナ化されたアプリケーションまたはプロセスの、シームレスな開発と展開を可能にします。このオプションは、事前にパッケージ化されたスクリプトを提供し、コンテナアプリケーション環境とnShield HSMの統合作業を大幅に簡素化すると同時に、ユーザのアプリケーションとコンテナ化されたホストの動的な拡張をサポーします。

nShield BYOKによるクラウドデータの強力な鍵管理

nShield BYOK（Bring Your Own Key：独自の鍵の持ち込み）を利用することで、Amazon Web Services、Google Cloud Platform、Microsoft Azureのいずれ（またはその3つすべて）を使用する場合でも、オンプレミス型のnShield HSMで強力な鍵を生成し、生成した鍵をクラウドアプリケーションへ安全にエクスポートすることができます。またnShield BYOKを利用することにより、自社の鍵でセキュリティを強化し、クラウド内のデータの安全性を自社で管理することができます。

nShield BYOKには次のメリットがあります。

- クラウド内の機密データの安全性を高める、より安全な鍵管理の実施
- FIPS認定ハードウェアで保護されたnShieldの真の乱数生成器（TRNG）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、鍵を作成してクラウドへ安全にエクスポート

暗号鍵の転送および使用に対して最高の保証を確保し、厳格な管理を行うには、Microsoft AzureでnShield BYOKをご利用ください。統合と展開に関する現場でのサポートが必要な場合は、BYOK展開サービスパッケージをご検討ください。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る開発支援、および1年間の保守が含まれます。

Amazon Web ServicesやGoogle Cloud PlatformでのBYOKには、EntrustのCloud Integration Option Pack（CIOP）をご利用ください。このオプションパックには、オンプレミス型のnShield HSMを使用して鍵を生成し、Amazon Web Service または Google Cloud Platformにエクスポートするために必要です。さらにCIOPは、新しいオープンプラットフォーム型のMicrosoft Azure BYOKにも、CIOPが必要です。

リモート監視と管理による円滑な運用

nShield SoloやConnect HSMで利用可能なnShield MonitorとShield Remote Administrationを使用することで、HSMの機能を24時間体制で管理しながら、運用コストを削減することができます。

Entrustのリモート監視・管理サービスには、次のメリットがあります。

- nShield Monitorを使用してHSMのパフォーマンス、インフラストラクチャの計画、稼働時間を最適化し、負荷の傾向、使用統計、改ざんイベント、警告、アラートを通知
- nShield Remote Administrationの強力で安全なインターフェイスを通じてHSMを管理することにより、移動を削減しコストと時間を節約

リモート構成

nShield Connect XCモデルはシリアルコンソールオプションを提供し、ラックへのHSMの物理的な設置、ケーブル配線、電力の供給を簡素化し、すべてのHSMのネットワーク構成もリモートで行うことができます。これにより、データセンターを再度訪問する必要がなくなり、簡単に展開や再展開を実行することができます。この機能はプロバイダー/テナントモデルをサポートします。プロバイダーはネットワーク構成を管理しながら、鍵要素はテナントが完全に制御します。

Security Worldの柔軟性に優れたアーキテクチャ

nShield Security Worldは、独自の柔軟な鍵管理環境を作成することにより、Entrust nShield HSMをサポートします。nShield Security Worldは異なるHSMモデルと組み合わせることができ、拡張性、シームレスなフェイルオーバー、負荷のバランシングを実現する統一したエコシステムを築くことができます。

「最先端システムであるEntrust nShield HSMを採用することにより、当社の技術においてより高度で安全なチップを使用できるようになりました」

Memjet、情報システム部門シニアディレクター、Bill Kavadas氏

nShield Security Worldは、展開するHSMの数に関わらず相互運用性を提供し、数量無制限で鍵の管理を可能にし、重要なデータを自動的かつリモートでバックアップ・復元します。

nShield Security Worldには次のメリットがあります。

- ニーズの拡大に応じてnShield HSMの機能を簡単に拡張可能
- システムの復元力を保持
- 時間のかかるHSMのバックアップを排除して時間を節約

CodeSafe - nShieldの安全な実行環境

nShield SoloおよびConnect HSMは、機密性が高い鍵を保護すると同時に、独自のアプリケーションを実行する安全な環境も提供します。CodeSafeオプションを使用することで、nShieldのFIPS 140-2レベル3認定を取得したHSM境界内でコードを開発・実行でき、潜在的な攻撃からアプリケーションを保護できます。

CodeSafeは次のことをサポートします。

- 機密性の高いアプリケーションを実行し、適格な環境内にあるアプリケーションデータのエンドポイントを保護することにより、高水準の保証を実現
- セキュリティに敏感なアプリケーションを、インサイダー攻撃、マルウェア、高度で持続的な脅威などの危険から保護
- コードサイニングを使用して、アプリケーションの不正改変やマルウェア挿入のリスクを排除

業界リーダーとのパートナーシップ

Entrustは、主要な技術プロバイダーと提携することで、業界のあらゆるセキュリティの課題に対処し、顧客のデジタル変革の達成を支援する拡張ソリューションを提供します。Entrustは、自社の技術パートナープログラムを通じてパートナーと協力し、認証とPKI、データベースセキュリティ、コード署名、デジタル署名、特権アカウント管理、アプリケーション配信、クラウドとビッグデータインテリジェンスを含むさまざまなセキュリティソリューションに、nShield HSMを統合しています。nShield HSMはパートナーのセキュリティアプリケーションをサポートし、政府および業界のデータセキュリティ規制への準拠を促進しながら、極めて強力な暗号処理、鍵の保護、鍵の管理を提供します。

「nShield as a Serviceを含むnShieldのクラウド対応の新機能が当社の顧客にもたらす、さまざまな可能性に非常に期待しています。これらの新機能は、変化し続ける市場にしっかりと対応していると思います。当社は、フルサービスを提供するHSMの機能をクラウドで使用し、利用可能なイノベーションと商業的メリットを活用したいと考えています」

Cryptomathic、製品管理ディレクター、
Ed Wood氏

「EntrustからのnShield as a Serviceの発売により、セキュリティの選択肢が広がり、F5のお客様は、サブスクリプションベースのモデルでデータの主権を実現できるようになりました。セキュリティを資本から運用支出にシフトすることで、柔軟性と費用対効果の向上が可能になりました」

F5 Networks、セキュリティ部門部長、
John Morgan氏

汎用性と優れた性能

nShield ConnectおよびSolo HSMは、トランザクションレートが中程度である場合でも、アプリケーションに高いスループットが必要となる場合でも、ご利用環境に合わせて3つの性能レベルから選択できます。nShield as a Serviceは、クラウド内のnShield HSMにアクセスするためのサブスクリプションベースのソリューションであり、最高性能のnShield Connect XCによって支えられています。

業界標準に準拠した認定取得

Entrustが厳格な基準を遵守し、nShield HSMの安全性と整合性を保証するため、ユーザは規制された環境での規則への準拠を達成することができます。以下に、弊社が準拠する基準の一部を記載します。完全なリストは、弊社のウェブサイトやデータシートでご覧いただけます。

FIPS 140-2

世界的に認められているFIPS 140-2は、米国政府が定めるNIST基準で、暗号モジュールのセキュリティの堅牢性を検証します。すべてのEntrust nShield HSMは、FIPS 140-2レベル2およびレベル3認定を受けています。

FIPS Level 3 Validated 140-2

Common Criteria

コモンクライテリアとeIDAS規則への準拠

nShield HSMは、コモンクライテリアEAL 4+認定を受けており、eIDAS規則の下で適格電子署名生成装置（QSCD）として認定されています。さらに、nShield Solo XCおよびConnect XC HSMは、コモンクライテリアのプロテクションプロファイルEN 419 221-5「トラストサービスに対する暗号モジュール」に準拠しています。そのため、nShield HSMは、EU加盟国および企業のデジタル化のためのセキュリティバックボーンとして機能することができます。これには、国別IDスキーム、国境を越えたサービス、電子文書およびトランザクション署名に対するサービスのほか、認証、タイムスタンプ、安全なEメール、文書の長期保存に対するサービスの実現が含まれます。これらの認定はヨーロッパにおける規制の一部として制定されましたが、EUだけでなく世界中の多くの国で採用されています。

詳細

オンプレミス、クラウド、および仮想環境でビジネスに不可欠な情報とアプリケーションを保護するために、弊社が提供しているサービスについては、**entrust.com/ja/HSM**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