nShield Connect HSM

アプリケーションの安全性は鍵の保管場所次第

ハイライト

包括的な機能

nShield Connect ハードウェア・セキュリティ・モジュール（HSM）は、FIPS 140-2およびコモンクライテリアEAL4+（EN 419 221-5）認定を受けたアプライアンスであり、ネットワーク全体に拡張可能で可用性の高い暗号鍵サービスを提供します。

- 高速なトランザクションレートと柔軟な拡張性
- 150社以上のアプリケーションベンダーとの統合実績
- nShieldの安全な実行環境内でアプリケーションとビジネスロジックを保護するためのCodeSafeオプション

nShield Connect HSMは耐タンパ性を備えたプラットフォームで、次のようなさまざまなユースケースで暗号化、デジタル署名、鍵の生成および保護などの機能を実行します。

- 認証局
- コードサイニング
- カスタムソフトウェア
- クラウドおよびコンテナ化されたアプリケーション
- ウェブサービス
- ブロックチェーン
- データベースの暗号化

nShield Connectには、nShield Connect+シリーズと高性能のnShield Connect XC シリーズがあります。

詳細をチェック：ENTRUST.COM/ja/HSM

nShield Connect HSM

主な機能と利点

柔軟性の高いアーキテクチャ

独自のSecurity Worldアーキテクチャにより、nShield HSMを組み合わせて、柔軟な拡張性、シームレスなフェイルオーバーおよび負荷分散を実現する複合システムを構築することができます。

より多くのデータをより高速で処理

nShield Connect HSMは高いトランザクションレートをサポートするため、企業、小売業、IoTなど、スループットが重要となる環境に最適です。

強力なリモート機能オプション

データセンターへの訪問回数を削減

nShield Remote Administration - 認証スマートカードを離れた場所にあるHSMに安全にアクセスさせ、ファームウェアの更新、新しいHSMの登録、既存のHSMの再割り当て/再構成などの保守タスクを実行できるようにします。詳細はnShield Remote Administrationのカタログをご覧ください。

Remote Configuration - Connect XCのシリアルコンソール版は、データセンタースタッフのための簡単なインストール、リモートネットワークの構成、およびフロントパネル設定を可能にします。

nShield Monitorは、すべてのnShield HSMの一元管理ダッシュボードを提供し、操作の最適化とアップタイムの向上をサポートします。詳細はnShield Monitorのカタログをご覧ください。

ユーザ独自のアプリケーションを保護

CodeSafeオプションは、機密性の高いアプリケーションをのFIPS 140-2認定を受けたnShieldの物理的境界内で実行するための安全な環境を提供します。詳細はCode Safeのカタログをご覧ください。

利用可能なモデルと性能

nShield Connect	500+	XC Base	1500+	6000+	XC Mid	XC High
NIST推奨の鍵長でのRSA署名パフォーマンス(tps)						
2048ビット	150	430	450	3,000	3,500	8,600
4096ビット	80	100	190	500	850	2,025
NIST推奨の鍵長でのECCプライム曲線署名パフォーマンス(tps)						
256ビット	540	680	1,260	2,400	7,515[2]	14,400[2]
クライアントライセンス						
含まれる数	3	3	3	3	3	3
最大数	10	10	20	無制限[1]	20	無制限[1]

注1:企業向けクライアントライセンスが必要です。

注2:記載された性能の実現には、ECDSA向け高速RNG(乱数生成)機能のアクティベーションが必要です。これはEntrust nShield Technical Supportがご要望に応じて無料で提供します。

nShield Connect HSM

技術仕様

サポート対象の暗号アルゴリズム（完全なNIST Suite Bの実装を含む）

- 非対称アルゴリズム：RSA、Diffie-Hellman、ECMQV、DSA、El-Gamal、KCDSA、ECDSA（NIST、Brainpool曲線、secp256k1曲線を含む）、ECDH、Edwards（Ed25519、Ed25519ph）
- 対称アルゴリズム：AES、Arcfour、ARIA、Camellia、CAST、DES、Triple DES、MD5 HMAC、RIPEMD160 HMAC、SEED、SHA-1 HMAC、SHA-224 HMAC、SHA-256 MAC、SHA-384 HMAC、SHA-512 HMAC、Tiger HMAC
- ハッシュ/メッセージダイジェスト：MD5、SHA-1、SHA-2（224、256、384、512 bit）、HAS-160、RIPEMD160

サポート対象プラットフォーム

- RedHat、SUSE、仮想マシンとしてやコンテナ内で実行される主要なクラウドサービスプロバイダーからのディストリビューションを含む、WindowsおよびLinuxオペレーティングシステム

アプリケーションプログラミングインターフェイス（API）

- PKCS#11、OpenSSL、Java（JCE）、Microsoft CAPI/CNG、nCore、Web サービス（Web Services Option Packが必要）

ホスト接続

- 2ポートのギガバイトイーサネット（2つのネットワークセグメント）

セキュリティ関連のコンプライアンス

- FIPS 140-2レベル2およびレベル3、NIST SP 800-131A 認定取得
- IPv6認定取得、USGv6準拠
- Connect XC：オランダのNSCIBスキームに基づく、EN 419 221-5保護プロファイルに対するeIDAS規則準拠と、コモンクライテリアEAL4+ AVA_VAN.5およびALC_FLR.2認定取得
- Connect+：コモンクライテリアEAL4+（AVA_VAN.5）認定取得
- Connect+：適格電子署名生成装置として認定
- Connect XC：BSI AIS 20/31準拠

安全基準および環境基準への準拠

- UL、CE、FCC、RCM、カナダのICES RoHS2、WEEE

高い可用性

- すべてのソリッドステートストレージ
- 現場で保守可能なコンポーネント、ホットスワップ電源 2 基

管理およびモニタリング機能

- nShield Remote Configuration（シリアルコンソール構成のConnect XCモデルに付属）
- nShield Remote Administration（別売）
- nShield Monitor（別売）
- 安全な監査ログ取得
- Syslog診断サポートおよびWindowsパフォーマンスモニタリング
- SNMPモニタリングエージェント

物理的特徴

- 標準的な1Uサイズ・19インチのラックマウント型デバイスの寸法：43.4 x 430 x 705mm（1.7 x 16.9 x 27.8インチ）
- 重量：11.5kg（25.4ポンド）
- 入力電圧：100～240V AC自動切替50～60Hz
- 消費電力：110V AC、60Hzで最大2.0A、220V AC、50Hzで1.0A
- 熱放散：327.6～362.0BTU/時（全負荷）
- 信頼性 - MTBF（平均故障間隔）[3]、Connect XC：107,384時間、Connect+：99,284時間

注3：Telcordia SR-332「電子機器の信頼度予測手順」のMTBF標準を使用して、摂氏25度の動作温度で計算

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