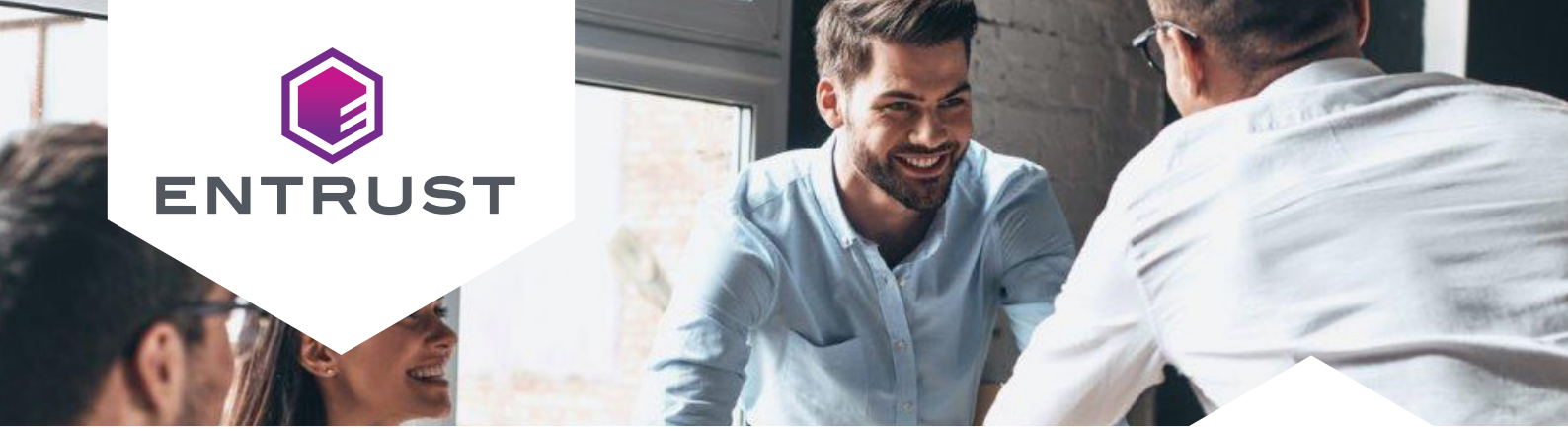


nShield Solo HSM

スタンドアロン型サーバに暗号鍵サービスを提供する認定済みのPCIeカード

ハイライト

nShield Solo ハードウェア・セキュリティ・モジュール（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、FIPS認定を受けた PCIe カードです。耐タンパ性のカードが、認証局、コード署名、カスタムソフトウェアなどを含む広範なアプリケーションに対して、暗号化、デジタル署名、鍵の生成と保護などの機能を実行します。

nShield Soloシリーズには、nShield Solo+や新たに登場した高性能のnShield Solo XCが含まれます。

柔軟性の高いアーキテクチャ

nCipher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提供する統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

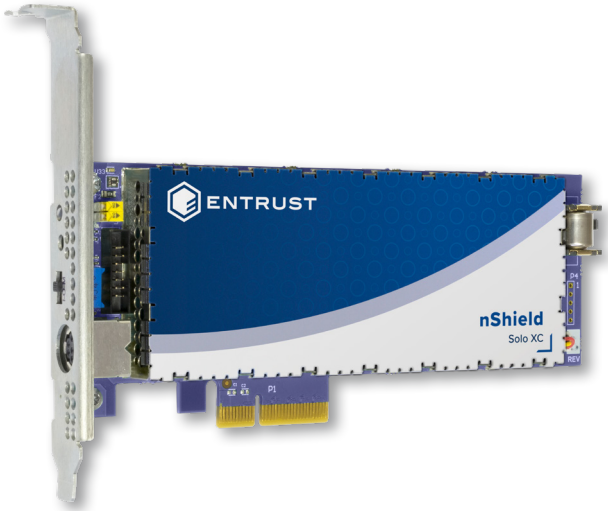
nShield Solo HSMは高いトランザクションレートをサポートするため、企業、小売業、IoTなどスループットが重要となる環境に最適です。

ユーザ独自のアプリケーションとデータを保護

CodeSafeオプションにより、nShield境界内での高いアプリケーションを実行するための安全な環境を提供します。

主な機能と利点

- 高い暗号化トランザクションレートと柔軟な拡張性により、パフォーマンスと可用性を最大化
- 認証局やコードサイニングなどさまざまなアプリケーションをサポート
- nShield CodeSafeがnShieldの安全な実行環境内でアプリケーションを保護
- nShield Remote Administrationにより、現場まで出向く必要性とコストを削減



詳細をチェック：ENTRUST.COM/ja/HSM

nShield Solo HSM

技術仕様

サポート対象の暗号化アルゴリズム

- 非対称アルゴリズム：RSA、Diffie-Hellman、ECMQV、DSA、El-Gamal、KCDSA、ECDSA、ECDH、Edwards（X25519、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 HMAC、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ビット）、HAS-160、RIPEMD160
- ブレインプール曲線やカスタム曲線を含む、ライセンスされたECCによる完全なSuite Bの実装

サポート対象プラットフォーム

- RedHat、SUSE、仮想マシンとして、または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
- VMware ESX、Microsoft Hyper-V、Linux KVM、Citrix XenServerなどのSolo XC仮想環境をサポート

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およびCNG、nCore、Webサービス（Web Services Option Packが必要）

ホスト接続

- PCI Expressバージョン2.0（Solo+コネクタ：1レーン、Solo XCコネクタ：4レーン）

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認定取得
- Solo+：コモンクライテリアEAL4+（AVA_VAN.5）認定取得
- Solo+：適格電子署名生成装置として認定
- Solo 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認証取得
- Solo XC：BSI AIS 20/31準拠

安全基準および環境基準への準拠

- UL、UL/CA、CE、FCC、カナダのICES、KC、FCC、VCCI、RCM
- RoHS2、WEEE、REACH

管理とモニタリング機能

- nShield Remote AdministrationおよびnShield Monitor（ともに別売）
- 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

利用可能なモデルとパフォーマンス

nShield Soloのモデル	500+	XC Base	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	3,000	3,500	8,600
4096ビット	80	100	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	2,400	7,515[1]	14,400[1]

寸法	重量		電力	
	Solo+	Solo XC	Solo+	Solo XC
56.2 × 167.1 × 15.4mm	230g	280g	10W	24W
2.2 × 6.6 × 0.6インチ	0.5ポンド	0.62ポンド		

注1：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。

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