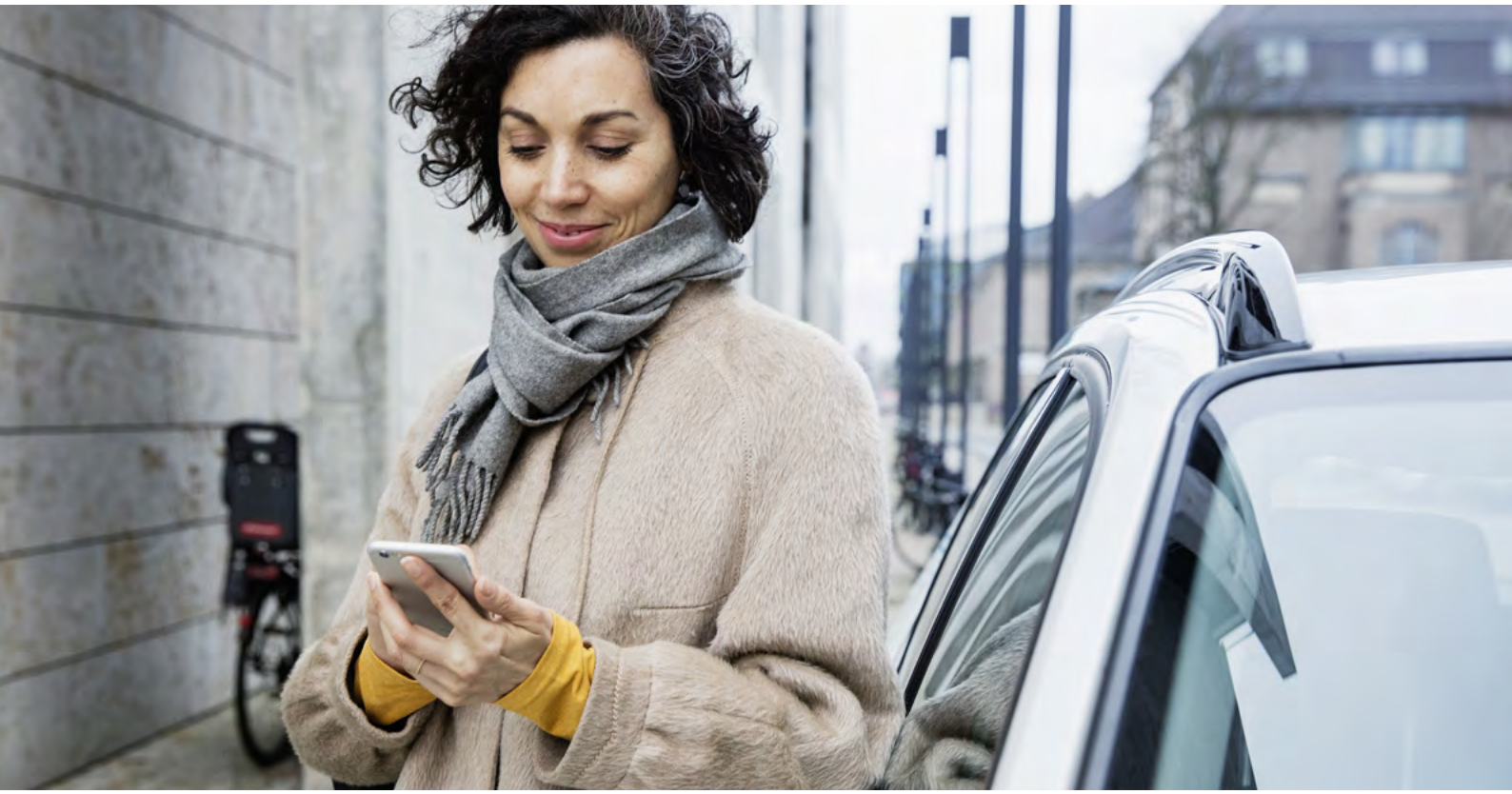
ソリューションカタログ

# 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

# Contents





# 信頼できるセキュリティ

Entrust nShieldハードウェアセキュリティモジュール（HSM）は、企業の機密性の最も高いデータを保護する、堅牢な耐タンパ性デバイスです。FIPS認定を取得した適格モジュールは、暗号鍵や署名鍵の生成、管理、保管などの暗号化機能に加え、保護された境界内での機密性の高い機能を実行します。

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。

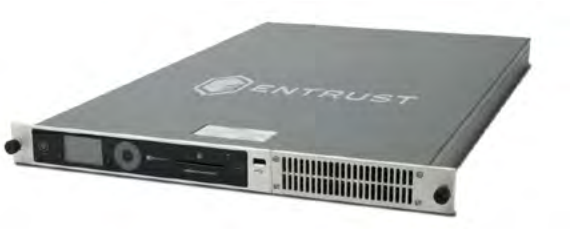
- より高度なデータの安全性と信頼性を実現
- 重要な規制基準に確実に準拠
- 量子耐性技術による将来を見据えたデータセキュリティ

# nShieldシリーズ

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

## ネットワーク接続型HSM

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。高性能な最新モデルnShield 5cがあります。

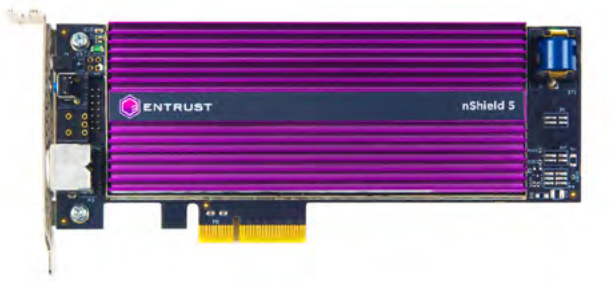



## ポータブルUSBベースHSM

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。


## サーバ組み込み用PCIe HSM

nShield HSMnShield 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、薄型PCIeカードモジュールです。 高性能な新型nShield 5sがあります。




## nShield as a Service

FIPS認定を取得した専用のnShield HSMへのアクセスを提供するサブスクリプション型モデルです。耐量子アルゴリズムのサポートを含め、オンプレミス型HSMと同等の機能を提供すると同時に、クラウドサービス導入のメリットも兼ね備えています。これにより、ユーザは「クラウドファースト」の目標を達成しつつ、これらの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。

nShield as a Serviceでは、お客様が鍵を所有します（HSMそのものではありません）。また、オンプレミスの nShield HSM を導入した場合と同じく nShield HSM 独自のSecurity World 鍵管理アーキテクチャを採用しているため、暗号処理をオンプレミスからクラウドへ容易に移行できるほか、オンプレミスとクラウドベースのHSMを組み合わせたハイブリッド方式を採用することで、冗長性と信頼性をさらに高めることも可能です。

nShield as a Serviceは、EU（ドイツ）、英国、米国、オーストラリアにある完全に冗長化されたデータセンターを利用します。各地域のデータセンターは、クラウドデータのセキュリティおよびデータ主権に関する規制要件を満たすためのジオフェンシングを実現します。お客様の多様なニーズに応えるため、幅広いサービスオプションが用意されています。 コストを重視するお客様には、ご希望のロケーションでセルフマネージド型のHSMをご利用いただけます。スタンダード、プレミアム、エンタープライズのお客様は、 最適なパフォーマンスと価格帯を選択しつつ、運用、災害復旧、データ主権の要件を満たすHSMロケーションを指定することができます。

# 幅広い用途をサポート

Entrustのお客様は、nShield HSMを「信頼の基盤」として、以下のようなさまざまなビジネスアプリケーションで活用しています。

- 公開鍵基盤（PKI）
- TLS/SSL暗号化鍵の保護
- コード署名
- デジタル署名
- 5G通信アプリケーション
- ブロックチェーン

モノのインターネット（IoT）の成長に伴い、デバイスIDや証明書への需要が高まる中、nShield HSMはデジタル証明書を用いたデバイス認証などの重要なセキュリティ対策を今後も引き続きサポートしていきます。

また、nShield HSMは、以下のような幅広い暗号アルゴリズムにも対応しています。

- 耐量子時代の到来に備えるための、**NISTが標準化した新しい量子耐性アルゴリズム**
- スマートメーターなどの今日の低消費電力コンピューティング環境に最適な**楕円曲線暗号アルゴリズム**
- 通信アプリケーション向けの**5G対応アルゴリズム**

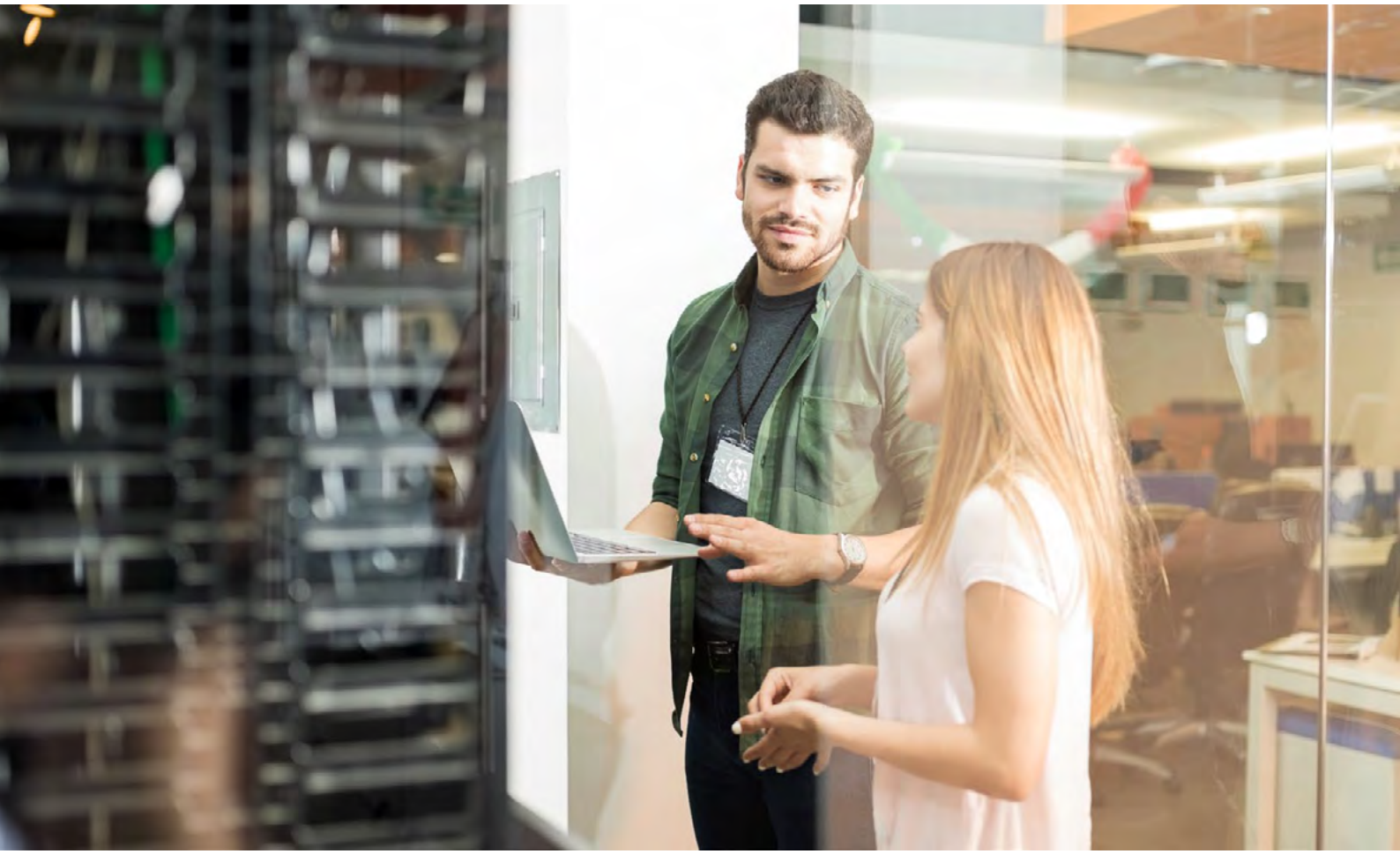
# nShieldシリーズの機能

## クラウド対応のWebサービスインターフェイス

nShield Web Service のRESTfulインターフェースは、アプリケーションをnShield HSMと直接統合する必要性を排除し、OSやアーキテクチャ構成への依存を解消することで、導入において革新的なアプローチを提供します。

## 耐量子セキュリティ

nShield HSMシリーズは、耐量子暗号アルゴリズムをサポートすることで、組織が量子時代の到来に対応できるようサポートするように設計されています。NISTの耐量子暗号標準に準拠したnShield HSMを利用することで、ハードウェアによる高速処理を活かした量子耐性のあるセキュリティを導入することが可能です。



## オンプレミスまたはクラウドでのコンテナ環境に対応

The nShield Container Option Packは、Entrustの高い信頼性の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開発や導入をシームレスに実現します。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。

## Entrust nShield Cloud Integration Option Pack による、クラウドデータの強力な鍵管理

Bring Your Own Key (BYOK) の導入をサポートする nShield Cloud Integration Option Packを利用することで、オンプレミス型のnShield HSMで強力な鍵を生成し、Amazon Web Services、Google Cloud Platform、Microsoft Azure、またはSalesforceのいずれかを使用している場合は、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。BYOKを利用することにより、鍵管理のセキュリティを強化し、鍵に対する制御を高めるとともに、クラウド上のデータを安全に保つ責任を共有することができます。

nShield HSM による BYOK には、次のようなメリットがあります。

- クラウド上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 認定ハードウェアによって保護された高エントロピーの乱数生成器を使用した、より強力な鍵生成
- 自社環境内の nShield HSM を使用して鍵を作成し、安全にクラウドへエクスポートすると同時に、自社でバックアップを保持することで、鍵に対する管理を強化

## Hold Your Own Key (HYOK) で鍵を最大限にコントロール

規制産業では通常、セキュリティポリシーやデータの取り扱い方針、政府の規制（たとえばデータ主権に関する要件）や、組織全体のセキュリティ体制によって、選択肢が規定されています。近年、欧州連合ではデータ主権が「ホットトピック」となっており、Schrems IIに関する法的判決の結果、5,000を超えるEUの組織が自社の暗号鍵および暗号化データの保管場所について慎重に検討せざるを得なくなりました。これを受けて、クラウドサービスプロバイダーであるAWSは、Key Management Service External Key Store（AWS KMS XKS）を提供しています。この機能により、組織は暗号鍵を自社で所有・保持・管理し、オンプレミスまたは自社管理のクラウド環境において運用することが可能になります。これらはすべて、AWSのエコシステムの外部で完全に管理されます。nShield HSMは、AWS KMS XKSとシームレスに連携します。さらに、Microsoft Azure Information Protection（AIP）環境においては、nShield HSMは、Microsoft 365内の最も機密性の高いコンテンツを保護することを目的として設計されたダブル鍵暗号（Double Key Encryption）をサポートしています。

## リモート管理による運用の効率化

nShieldのネットワーク接続型HSMおよびPCIe型 HSMで利用可能なnShield Remote Administrationは、以下の機能を実現します

- HSM環境を24時間365日把握し、管理下に置きながら、運用コストを削減
- nShield Monitorを使用して、HSMのパフォーマンス、インフラ計画、稼働時間を最適化し、負荷傾向、使用状況の統計、改ざんイベント、警告、アラートについて通知
- 強力かつ安全なインターフェイスを通じてHSMを容易に管理でき、移動コスト時間を節約

## リモート構成

nShieldのネットワーク接続型モデルは、シリアルコンソールオプションを提供しており、HSMの物理的な設置作業をラックへの設置、ケーブル接続、電源投入に簡素化。その他すべてのHSM構成およびネットワーク構成設定は、その後リモートで実行することができるため、データセンターを再度訪問することなく、導入および再導入を容易に行うことができます。この機能はプロバイダー／テナントモデルにも対応しており、プロバイダーがネットワーク構成を管理し、テナントは自社の鍵要素を完全に管理することができます。

## 柔軟性に優れたSecurity Worldアーキテクチャ

nShield Security Worldアーキテクチャは、独自の柔軟な鍵管理環境を構築することで、nShield HSMをサポートします。このアーキテクチャにより、異なるnShield HSMモデルを組み合わせて、拡張性、シームレスなフェイルオーバー、負荷分散を実現する統合エコシステムを構築することができます。また、1台のHSMを導入する場合でも、数百台のHSMを導入する場合でも相互運用性を提供し、無制限の数の鍵を管理できるほか、鍵要素のバックアップと復元を自動的かつリモートで行うことができます。

nShield Security Worldアーキテクチャは、以下のメリットを提供します。

- 必要に応じて、nShield HSM環境を容易に拡張可能
- システムのレジリエンスを維持
- 時間のかかるHSMバックアップ作業を排除し、時間を節約

## KeySafe 5による一元的なリモート管理

Entrust KeySafe 5は、nShield HSMとnShield as a Service HSMが混在する拡張可能なSecurity Worldアーキテクチャにおいて、セットアップおよび構成を一元的かつリモートで管理し、その状態を確認する機能を提供します。

## 安全な実行環境

InShieldのネットワーク接続型およびPCIe型HSMは機密性の高い鍵を保護するだけでなく、ユーザ独自のアプリケーションを実行するための安全な環境も提供します。CodeSafe®ソフトウェア開発ツールキットにより、FIPSレベル3を取得したnShield HSMの物理的境界内でコードの開発および実行が可能となり、潜在的な攻撃からアプリケーションを保護します。

CodeSafeツールキットは、以下を実現します。

- 認証取得済み環境内で機密性の高いアプリケーションを実行および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で、高い保証レベルを実現
- 内部不正、マルウェア、高度な持続的脅威（APT）などのリスクからセキュリティ上重要なアプリケーションを保護
- コード署名を用いて不正なアプリケーション変更やマルウェア感染のリスクを排除
- nShield HSMのFIPS境界内で動作するCodeSafeソフトウェア開発ツールキットとPost-Quantum Option Packを使用することで、LMSなどの耐量子アルゴリズムを展開可能

## 暗号の俊敏性への対応

暗号俊敏性とは、組織が新たに登場する暗号方式をシームレスに採用できる能力を指します。これは、耐量子暗号アルゴリズムの標準化が進み、新たなアルゴリズムが継続的に導入される状況において、極めて重要です。

nShield 5 HSMは、そのセキュリティプロセッサとしてFPGA（field-programmable gate array）を採用しており、ソフトウェアアップデートによって容易に再プログラム可能なため、導入時から暗号の俊敏性を提供します。これにより、高コストかつ時間のかかるハードウェア更新を削減し、現在利用している暗号技術を脅かす可能性のある量子コンピュータに対する耐性を向上させます。

量子コンピュータがもたらす将来的な課題に備える中で、HSMはITシステム、クラウド、インターネットにおけるセキュリティと信頼性の基盤として不可欠です。nShield 5 HSMは、ML-DSAなどのNIST標準化済みの耐量子暗号アルゴリズムをネイティブにサポートしています。

# 業界リーダーとのパートナーシップ

Entrustは、業界をリードするテクノロジープロバイダーと提携し、幅広い業界のセキュリティ課題に対応しながら、お客様のデジタルトランスフォーメーションの実現を支援する優れたソリューションを提供しています。Entrust Ready Technology Partner Programを通じて、パートナーと協力し、nShield HSMを以下のようなさまざまなセキュリティソリューションに統合しています。

- 認証およびPKI
- データベースセキュリティ
- コードサイニング
- デジタル署名
- 特権アカウント管理
- 5G
- アプリケーション配信
- クラウドインテリジェンス
- ビッグデータインテリジェンス

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、最も強力な暗号処理、鍵の保護、鍵管理を提供するとともに、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ます。

「nShield as a Serviceをはじめとするnshieldの新しいクラウド対応機能が、私たちのお客様にもたらす可能性に大きな期待を寄せています。これらの新機能は、市場の変化、すなわち組織がイノベーションやビジネス上のメリットを最大限に引き出すために、クラウド上でフル稼働するHSMを必要としているというニーズを的確に捉えています」

**CRYPTOMATHIC社 コーポレートディレクター MATT LANDROCK氏**

「EntrustによるnShield as a Serviceの提供開始により、F5のお客様はサブスクリプションモデルでデータ主権を達成できるなど、より多くのセキュリティ選択肢を得ることが可能になります。セキュリティ投資をCapEx（資本支出）からOpEx（運用支出）へとシフトすることで、組織にとってより柔軟でコスト効率の高い運用が実現されます」

**F5 NETWORKS社 セキュリティVP兼GM JOHN MORGAN氏**

「EntrustのnShield HSMは最先端の技術であり、当社のテクノロジーにおいて、より高度で安全性の高いチップの採用を可能にしています」

**MEMJET社 情報システム担当シニアディレクター BILL KAVADAS氏**

## 柔軟性と優れた性能

nShieldのネットワーク接続型およびPCIe型のHSMは、トランザクションレートが中程度の環境からハイスループットを要求されるアプリケーションまで、お客様の環境に応じて選択できる3つの性能レベルで提供されています。クラウド上でnShield HSMへアクセスするためのサブスクリプション型ソリューションであるnShield as a Serviceは、最も高性能なネットワーク接続型HSMを基盤として提供されます。

## エンタープライズKMS向け信頼の基点

組織がHSMを信頼の基点としたエンタープライズ向け鍵管理サービスを必要としている場合は、Entrust暗号セキュリティプラットフォーム（CSP）をご検討ください。このプラットフォームの鍵およびシークレット管理ソリューションは、従来の鍵のライフサイクル管理と、分散型のボルト（Vault）ベースアーキテクチャに、ポリシーおよびコンプライアンスの包括的な一元管理が可能なダッシュボードを組み合わせることで、暗号鍵管理を再定義します。このプラットフォームは、分散しているセキュリティに対し、企業の暗号エコシステム全体にわたって一元的可視性を提供します。これにより厳格な規制要件への準拠を満たしつつ、データ保護を確実に実現します。

Entrust暗号セキュリティプラットフォームは、複雑化するデジタル環境において高まる暗号資産管理のニーズに対応するソリューションです。このプラットフォームは信頼の基点であるnShield HSMが支えるPKIの運用、証明書ライフサイクル管理、鍵管理、シークレット管理といった豊富な機能を統合し、暗号資産管理を一元化します。

## 業界標準の認定取得

Entrustは厳格な標準への準拠により、規制環境におけるコンプライアンス対応を支援し、nShield HSMのセキュリティおよび完全性に対する高い信頼性を提供します。以下は、Entrustが準拠している標準の一部です。すべてのリストは当社ウェブサイトおよびデータシートをご参照ください。

### FIPS 140-2/FIPS 140-3

Federal Information Processing Standard（FIPS）140-2は世界的に認知されている標準であり、米国国立標準技術研究所（NIST）によって策定された暗号モジュールのセキュリティ強度を検証する認証です。2022年には、この規格はNISTの新しい標準であるFIPS 140-3へと置き換えられました。nShield Solo XCおよびConnect XC HSM（以前のモデル）は従来のFIPS 140-2規格に準拠して認証されており、nShield 5sおよび5cは新しいFIPS 140-3 Level 3規格に準拠して認証されています。

FIPS 140-3 Validated,
Certificate #4745

## コモンクライテリアおよびeIDAS規則への準拠

nShield XCおよびnShield 5 HSMは、コモンクライテリアEAL4+の認証を取得しており、eIDAS規則の下で適格電子署名生成装置（QSCD）として認められています。コモンクライテリアEAL4+認定を受けたEntrust Remote QSCDは、トラストサービスプロバイダー（TSP）および署名システムインテグレーター（SI）が、現行のeIDAS規則に準拠したリモート署名サービスを提供するのをサポートしています。Entrust Remote Type 2 QSCDは、**Entrust Signature Activation Module（SAM）**と**Entrust Solo XC HSM**を組み合わせることで、安全性が高く、将来にも対応可能なリモート署名およびeシールに必要な信頼の基点を確立します。

さらに、nShield XCおよびnShield 5 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「トラストサービスのための暗号モジュール」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を支えるセキュリティ基盤として活用することができます。これには、国家IDスキームの実現、越境サービスの提供、電子文書およびトランザクション署名のための適格サービス、認証サービス、タイムスタンプサービス、安全なEメール、ならびに長期文書保存などが含まれます。これらの認証は欧州規制の一環として確立されたものですが、現在ではEUにとどまらず世界各国で採用されています。

Common Criteria

## 詳細情報

詳細については、**entrust.com/ja/HSM**をご覧ください。オンプレミス、クラウド、仮想環境において、ビジネスに重要な情報およびアプリケーションを保護する方法をご紹介しています。

## ENTRUSTについて

Entrustは、アイデンティティを中心としたセキュリティによって、不正行為やサイバー脅威から人、デバイス、データを保護しています。Entrustの包括的なソリューションは、オンボーディング時の本人確認から、日常的な取引における接続の保護や不正対策まで、アイデンティティライフサイクルのあらゆる段階のセキュリティ確保を支援しています。また、継続的なモニタリングによりコンプライアンス対応を支援するとともに、暗号鍵、シークレット、デジタル証明書を保護しています。アイデンティティを中心としたセキュリティを基盤として、お客様が安心してビジネスを展開し、成長できる環境を提供しています。Entrustはグローバルなパートナーネットワークを有し、世界150を超える国々でお客様をサポートしています。

詳細については、www.entrust.com/jaをご覧ください。



ENTRUST
SECURING A WORLD IN MOTION

entrust.com/ja エントラストジャパン株式会社｜東京都港区台場2-3-1 トレードピアお台場22階

HSMinfo@entrust.com

nShield-Family_20260709