cpl.thalesgroup.com/ja

THALES
Building a future we can all trust

# ProtectServer 3 PCIe HSM

**ProtectServer 3 PCIe HSM(ハードウェアセキュリティモジュール)は、高性能な対称および非対称暗号操作を必要とするサーバーシステムやアプリケーション向けに、改ざん防止機能を備えたハードウェアセキュリティを提供します。**

## 多様なパフォーマンスレベル

ProtectServer PCIe HSMは、PCI Express x4準拠のカードで、各種パフォーマンスレベル(25、220、3500 RSA-1024署名/秒)が用意されており、さまざまなシステム要件に対応します。

## 広範な暗号処理

ProtectServer HSMは、セキュアストレージと専用暗号プロセッサを提供し、暗号操作の高速処理と高速トランザクションを実現します。HSMは、暗号化、ユーザー認証、データ認証、メッセージ整合性、eコマース用の安全な鍵ストレージと鍵管理、PKI、文書管理、EBPP(Electronic Bill Presentation and Payment)、データベース暗号化、金融EFTトランザクションなど、幅広い暗号化サービスを提供します。

## メリット

**パフォーマンス**
- 最大で3500 RSA-1024署名/秒
- 特殊な暗号技術でホストシステムの暗号処理の負担を軽減

**セキュリティ**
- FIPS 140-2 Level 3検証済み
- 改ざん防止環境

**信頼性:**
- 高品質のコンポーネント

**容易な管理**
- 直感的なGUI
- 現場での安全なファームウェアアップグレード
- リモート管理

## 強固なセキュリティ – 鍵をハードウェアで保管

安全性の低いサーバー環境で動作することが多い機密性の高い暗号処理に対し、最高レベルの保護が提供されます。ProtectServer PCIe HSMは、FIPS 140-2 Level 3検証済みで、改ざん防止セキュリティを備えており、機密情報を取得しようとするHSMへの物理的な攻撃から機密情報を守ります。物理的な攻撃が検出されると、内部鍵ストレージメモリは完全に消去されます。さらに、暗号鍵がHSMの外部に平文で流出することはありません。

安全な保管と処理は、他のソフトウェア製品では得られないレベルのセキュリティを提供するとともに、顧客の期待や業界組織のセキュリティ要求を満たす認定レベルの機密性と完全性を提供します。

## 広範なAPI/ツールキットとカスタマイズ

幅広いAPI（アプリケーションプログラミングインターフェース）が用意されており、暗号化アプリケーションを業界のセキュリティ標準やプラットフォーム環境に準拠させるために役立ちます。これには、市場で入手可能な最も広範なPKCS#11関数セット、Java JCA/JCE、 JCProv、Microsoft CryptoAPI/CNGプロバイダー実装、 OpenSSLとのシームレスな統合が含まれます。ソフトウェア開発キットは、比類のないレベルの柔軟性と拡張性を実現します。これにより、完全に新しいアルゴリズムを含むカスタム暗号化アプリケーションを作成して、 HSM の保護された領域内で安全にダウンロードして実行することができます。

## 容易な管理

直感的なGUIで、わかりやすいナビゲーションとユーザーインタラクションによってHSMデバイスの管理と鍵管理を簡素化します。鍵の変更、追加、削除など、緊急かつタイムクリティカルな管理タスクを遠隔地から安全に実行できるため、管理コストを削減し、対応時間を短縮できます。

## 柔軟なプログラミング

ProtectServer HSMは柔軟性に優れているため、アプリケーション開発者は独自のファームウェアを作成し、HSMの安全な領域内で実行できます。機能モジュールとして知られるツールキットが、カスタムファームウェアを開発および展開するための包括的な機能を提供します。柔軟な開発ツールを完成させるフル機能のソフトウェアエミュレータにより、開発者は便利なデスクトップコンピュータから、カスタムファームウェアのテストとデバッグを実行できます。このエミュレータは、ProtectServer HSMをインストールすることなくアプリケーションをテストできる貴重なツールでもあります。準備が整ったら、開発者はHSMをインストールし、通信をハードウェアにリダイレクトするだけです。ソフトウェアを変更する必要はありません。

## 利便性

スマートカードは、暗号鍵の安全なバックアップ、リカバリ、転送を実現する最高のセキュリティと管理上の利便性を提供します。アップグレードは現場でコスト効率よく実行できるため、製品をサービス拠点に返送する費用がかかりません。ProtectServer HSMは、互換性のあるPINパッドによるキー入力にも対応しています。

## 多要素認証

ProtectServer HSM は、多要素認証をサポートしています。この認証方式では、記憶されたトークンPINと、110 OTPトークンによってランダムに生成された6桁の数字の両方が必要となるため、セキュリティがさらに強化されます。

## 複数のスロット

ProtectServer PCIe HSMは、複数の暗号鍵ストレージスロットをサポートしています。ストレージスロットは、複数のカードスロットを備えたスマートカードリーダーと同様に機能しますが、物理的なカードリーダーは必要ありません。これらの仮想スロットは事実上、鍵用の安全なフォルダであり、各フォルダは一意のユーザーとセキュリティ担当者のパスワードによって保護されます。これにより、1つのProtectServer HSMを複数のアプリケーションで使用することができ、大幅なコスト削減と柔軟性の向上が実現します。

## 技術仕様

**利用可能なモデル:**

- ProtectServer 3 PCIe HSM - PL25、PL220、PL3500パフォーマンスモデル

**Operating Systems**

- WindowsおよびLinux

**暗号化API**

- PKCS#11, CAPI/CNG, JCA/JCE, JCProv, OpenSSL

**暗号化**

- 非対称: RSA、DSA、Diffie-Hellman、名前付き曲線、ユーザー定義曲線、Brainpool曲線による楕円曲線暗号（ECDSA、ECDH、Ed25519）など
- 対称: AES、AES-GCM、AES-CCM、Triple DES、DES、CAST 128、RC2、RC4、SEED、ARIA、その他
- ハッシュ: SHA-1、SHA-2、SHA-3、MD5、MD2、RIPEMD 128、RIPEMD 160、DES MDC2 PAD1など
- メッセージ認証コード: SHA-1、SHA-2、SHA-3、MD2、RIPEMD128、RIPEMD160、DES MDC-2 PAD1、SSL3 MD5 MAC、AES MAC、CAST-128 MAC、DES MAC、DES3 MAC、DES3 Retail CFB MAC、DES30x9.19 MAC、IDEA MAC、RC-2 MAC、SEED MAC、ARIA MAC、VISA CVV
- デジタルウォレット暗号化: BIP32
- 加入者認証用の5G暗号化メカニズム: MILENAGEおよびTUAK

**物理的特徴**

- ロープロファイルPCIeカード
- 寸法: 2.74” x 6.57” x .074” (69.6mm x 167mm x 187mm)
- 消費電力: 最大18W、標準14W
- 熱放散: 最大61.4 BTU/時、標準47.8 BTU/時
- 温度: 動作時 0°C～50°C、保管時 -20°C～60°C
- 相対湿度: 5%～95% (38°C) 非結露

**ホストインターフェース**

- PCI-Express CEM 3.0, PCI, PCI Express Base 2.0

**セキュリティ認定**

- FIPS 140-2 Level 3

**安全・輸出・環境コンプライアンス**

- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE
- India BIS [IS 13252 (Part 1)/IEC 60950-1]

**信頼性**

- 平均故障間隔(MTBF) 997,508時間
- 高可用性(HA)/ワークロード分散(WLD)
- バックアップ/復元

## タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。



> cpl.thalesgroup.com/ja <

**お問い合わせ先 –** Email: cpl.jpsales@thalesgroup.com
すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。