プロダクト ブリーフ

# SafeNet ProtectServer PCIe HSM

**（旧称SafeNet ProtectServer Internal-Express 2）**

ジェムアルトのSafeNet ProtectServer PCIe HSMは、高パフォーマンスの対称および非対称暗号操作を必要とするサーバシステムとアプリケーションに、不正防止ハードウェアセキュリティを提供します。

## さまざまなパフォーマンスレベル

SafeNet ProtectServer PCIe HSMは、多様なシステム要件を満たす、さまざまなパフォーマンスレベルで利用可能なPCI Express x4対応のカードです。1秒あたり25、220、または1500のRSA 1024ビット署名をサポートしています。

## 広範な暗号処理

SafeNet ProtectServer HSMは、安全なストレージと専用の暗号化プロセッサを提供し、暗号操作の処理およびトランザクションの高速化を実現します。HSMは、eコマース、PKI、文書管理、Electronic Bill Presentation and Payment（EBPP; 電子請求および電子決済）、データベース暗号化、金融のEFTトランザクション、その他多数を対象とした、暗号化、ユーザーおよびデータ認証、メッセージの完全性、セキュアな鍵保管と鍵管理を含む、広範な暗号化サービスを提供します。

## 強力なセキュリティ - ハードウェアに鍵を保管

安全性の低いサーバ環境で動作することが多い機密の暗号処理に、最高レベルの保護を提供します。SafeNet ProtectServer PCIe HSMは、FIPS 140-2レベル3検証済みであり、機密情報を得ようとするHSMを物理的に攻撃しても安全に保護する不正防止セキュリティを特徴としています。物理的攻撃が検出されると、内部鍵保管メモリは完全に消去されます。また、暗号鍵が使用できる形でHSMの外部にさらされることはありません。

セキュアな保管と処理によって、他のソフトウェアからは得られないセキュリティレベルをお客様に提供するとともに、お客様の期待と業界団体のセキュリティ要件を満たす認定レベルの機密性と完全性を提供します。

## 拡張API/ツールキットおよびカスタマイゼーション

暗号化アプリケーションが業界セキュリティ標準とプラットフォーム環境に準拠できるように、幅広いアプリケーションプログラミングインターフェイス（API）を利用できます。これには、市場で入手できる広範なPKCS#11関数セット、Java JCA/JCE、JCProv、Microsoft CryptoAPI/CNGプロバイダー実装、そしてOpen SSL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卓越した柔軟性と拡張性を実現し、独自の暗号化アプリケーションを作成する機能（完全に新しいアルゴリズムを含む）、およびHSMの保護領域内で安全にダウンロードして実行する機能を提供します。

## 使用例

- データベースなどの暗号化
- ユーザーおよびデータ認証
- メッセージの完全性
- セキュアな鍵保管
- eコマースの鍵管理
- PKIの鍵管理
- 電子文書管理
- Electronic Bill Presentation and Payment（EBPP; 電子請求および電子決済）
- EFTトランザクション

## 利点

**パフォーマンス**

- 特殊な暗号電子機器により、暗号処理ホストシステムからオフロード

**セキュリティ**

- FIPS 140-2レベル3検証（in process）
- 不正防止環境

**容易な管理**

- 直観的なGUI
- コマンドラインインターフェイス
- インフィールドでのセキュアなファームウェアアップグレード
- HSMのネットワークリモート管理

## 容易な管理

直観的なグラフィカルユーザーインターフェイス（GUI）の分かりやすいナビゲーションとユーザー操作により、HSMデバイス管理と鍵管理を簡素化します。緊急のスピードが重視される管理タスク（鍵の変更、追加、削除など）をリモートから安全に実行できるため、管理コストと応答時間が削減されます。

## 柔軟なプログラミング

SafeNet ProtectServer HSMは、アプリケーション開発者が独自のファームウェアを作成してHSMのセキュアな領域内でそれを実行する、他にはないレベルの柔軟性を提供します。機能モジュールと呼ばれるツールキットで、カスタムファームウェアの開発と導入のために包括的な機能を提供します。柔軟な開発ツール群を完全なものにするフル機能のソフトウェアエミュレータは、開発者にとって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行えるようにします。このエミュレータは、SafeNet ProtectServer HSMをインストールせずに、アプリケーションをテストする貴重なツールとしても使用できます。準備ができたら、開発者はHSMをインストールして、通信をハードウェアにリダイレクトするだけです。ソフトウェアの変更は必要ありません。

## 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、転送のための最高のセキュリティと管理上の利便性を提供します。HSMをサービス受付に戻すコストや手間をかけずに、効率よくインフィールドアップグレードを実行できます。

## 複数スロット

SafeNet ProtectServer PCIe HSMは、複数の暗号鍵保管スロットをサポートしています。保管スロットは、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じように機能しますが、物理的なカードリーダーは不要です。これらの仮想スロットは、効果的にセキュリティを確保する鍵用フォルダであり、各フォルダが一意のユーザーとセキュリティ担当者のパスワードで保護されます。これにより、単一のProtectServer HSMを複数のアプリケーションで使用できるため、コストが削減でき柔軟性も向上します。

## ジェムアルトのSafeNetアイデンティティおよびデータ保護ソリューションについて

ジェムアルトは世界でも最高クラスの完全性を持つエンタープライズセキュリティソリューションを提供しています。本ソリューションにより、お客様はエッジからコアまで、業界をリードするデジタルアイデンティティ、取引、決済、データの保護が受けられます。ジェムアルトが新たに展開するSafeNetアイデンティティおよびデータ保護ソリューションは、重要なデータおよびデータが保管される場所を保護するための、革新的な暗号化、クラス最高の暗号管理技術、強固な認証およびアイデンティティ管理ソリューションを活用することにより、主要な金融機関や政府機関を含む多くの業種でセキュリティに対してデータ中心のアプローチを取ることを可能にします。これらのソリューションを通して、ジェムアルトは、ますますデジタル化が進む世界において組織が顧客の信頼を守るために、厳しいデータプライバシーの規制などを遵守する手助けをし、企業の機密情報、顧客情報、電子取引を情報漏洩や改ざんから守ります。

## 技術仕様

**オペレーティングシステム**

- Windows and Linux

**暗号化API**

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

**暗号処理**

非対称アルゴリズム

- RSA（最大4096ビット）、DSA、ECDSA Diffie Hellman（DH）、ECC Brainpool曲線（名前指定およびユーザー定義）、その他

対称アルゴリズム

- AES、DES、3DES、CAST-128、RC2、RC4、SEED、ARIA、その他
- ECB、CBC、OFB64、CFB-8 (BCF)などのモードをサポート

ハッシュアルゴリズム

- MD5, SHA-1, SHA-256, SHA- 384, SHA- 512, MD2, RIPEMD128, RIPEMD160, DES MDC-2 PAD1

メッセージ認証コード

- SHA-1, SHA-256, SHA-384, SHA-512, 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

物理的特性

- 寸法: フルハイト、ハーフレングス 4.16” x 6.6” (106.7mm x 167.65mm)
- 消費電力: 最大12W、標準8W
- 温度: 動作温度0°C～50°C

セキュリティ認定

- FIPS 140-2レベル3
- BAC & EAC電子パスポートのサポート

安全および環境コンプライアンス

- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE

ホストインターフェイス

- PCI-Express X4, PCI CEM 1.0a

信頼性

- MTBF 216,204時間

**お問い合わせ先：**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、safenet.gemalto.jpをご覧ください。

**フォローする：**blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free