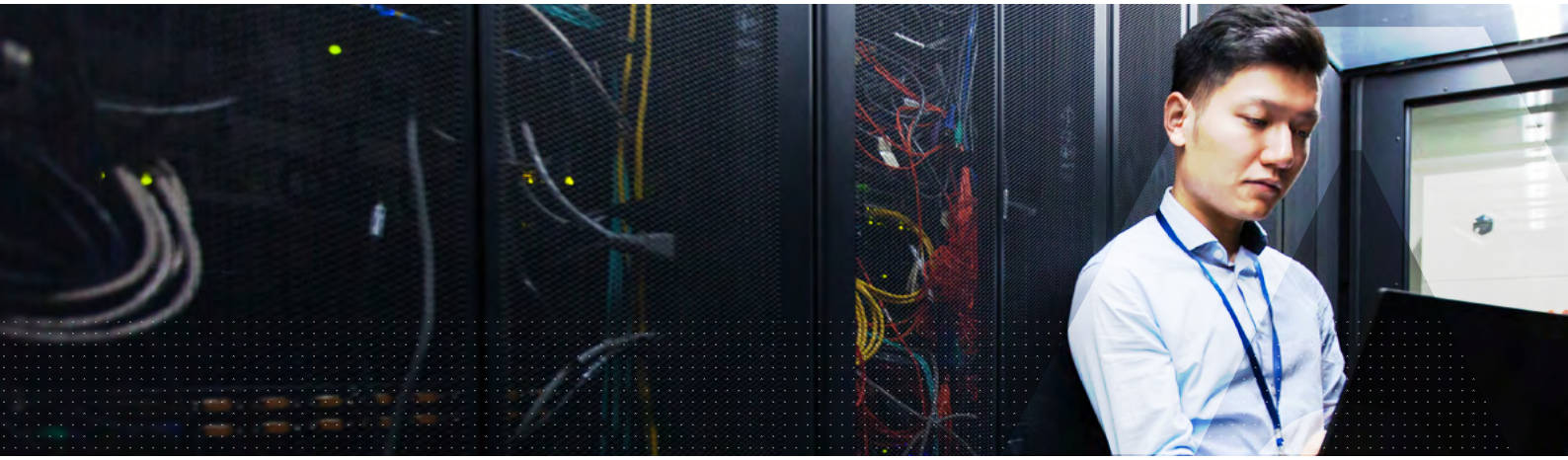
cpl.thalesgroup.com/ja

THALES
Building a future we can all trust

ProtectServer 3 Network HSM
ProtectServer 3 External
ProtectServer 3+ External



タレスProtectServer Network HSM(ハードウェアセキュリティモジュール)は、暗号鍵を侵害から守るとともに、暗号化、署名、認証サービスを提供して機密性の高いアプリケーションを保護するように設計された、セキュリティ強化されたネットワーク暗号化サーバーです。

高い安全性

ProtectServer Network HSMには、安全な暗号処理を高保証で実行する暗号モジュールが搭載されています。改ざん防止セキュリティを備えた堅牢なスチール製アプライアンスで物理的な攻撃に対する防御を備え、暗号鍵、PINS、その他のデータなど機密性の高い情報の保管と処理に対して、最高レベルの物理的・論理的保護を提供します。安全な保管と処理とは、暗号鍵がHSMの外部に平文で流出することがないことを意味し、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とともに、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。

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

ProtectServer 3 External HSM

ProtectServer 3+ External HSM

メリット

パフォーマンス
- 3500 RSA-1024署名/秒

セキュリティ
- FIPS 140-2 Level 3検証済み
- 物理的な改ざん防止
- TRNG(真性乱数発生器)
- スマートカードによる鍵マテリアルのバックアップ

信頼性
- 高品質のコンポーネント

容易な管理
- 直感的なGUI
- 現場での安全なアップグレード
- リモート管理

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。

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。

ProtectServer 3+ HSM

ProtectServer 3 HSMが提供する機能と特徴に加え、ProtectServer 3+ HSMでは、高可用性データセンター用にスワップ可能なAC二重化電源を採用しており、電源障害から保護します。また、アプライアンスを2つの別々の電源に接続できるようにすることで、ビジネス継続性を確保し、いずれかの電源の誤作動からも保護します。これにより、メンテナンスや、故障した電源や給電の交換に必要な柔軟性を確保し、デバイスの継続的動作を保証します。

高いパフォーマンスとスケーラビリティ

ProtectServer Network HSMは、暗号化コマンドを迅速に処理します。専用のデータ暗号マイクロプロセッサ、メモリ、TRNG（真性乱数発生器）などの特殊な暗号技術で、ホストシステムの暗号処理の負担軽減を行い、より多くの要求に対応します。

ProtectServer Network HSMには、幅広い対称および非対称暗号化パフォーマンスレベルが用意されています。さまざまなセキュリティアプリケーション処理要件に対応でき、最大で毎秒3500回のRSA-1024署名処理を実行できます。また、デュアルネットワークインターフェースを搭載しているため、オプションで同一または異なるサブネット上にHSMを統合したり、異なるネットワーク間で共有したりすることで、複数のビジネスドメイン保護や単一ネットワーク内での冗長性を保持できます。

さらに、同時に動作できるHSMの数や管理できる鍵の数に制限がないため、高レベルのスケーラビリティ、信頼性、冗長性、スループットの向上を容易に実現できます。

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。

技術仕様

利用可能なモデル：

- PSE 3には、PL25、PL220、PL3500パフォーマンスモデルを用意
- PSE 3+には、PL3500パフォーマンスモデルのみを用意

OS

- Windows, 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

- ラックマウント型
  - 標準的な1Uサイズの19インチラックマウントアプライアンス
- 寸法
  - 17.20” x 9.84” x 1.73” (437 mm x 270 mm x 44 mm) (PSE 3)
  - 19” x 21” x 1.725” (482.6mm x 533.4mm x 43.815mm) (PSE 3+)
- 重量
  - 6.83lb (3.1 kg) (PSE 3)
  - 28lb (12.7kg) (PSE 3+)
- 入力電圧
  - 100-240V, 50-60Hz (PSE 3)
  - 100-240V, 50-60Hz (PSE 3+)
- 消費電力
  - 最大90W、標準58W (PSE 3))
  - 最大100W、標準84W (PSE 3+)
- 温度
  - 動作時 0°C～35°C、保管時 -20°C～60°C
- 相対湿度
  - 5%～85% (38°C) 非結露 (PSE 3)
  - 5%～95% (38°C) 非結露 (PSE 3+)

ホストインターフェース
- ポートボンディング付き2ギガビットイーサネットポート (PSE 3)
- ポートボンディング付き4ギガビットイーサネットポート (PSE 3+)
- IPv4およびIPv6

セキュリティ認定
- FIPS 140-2 Level 3

管理および監視
- 高可用性(HA)/ワークロード分散(WLD)
- SNMP, Syslog
- バックアップ/復元

安全・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
- ホットスワップ可能な二重化電源 (PSE 3+)
- 平均故障間隔(MTBF) 165,637時間 (PSE 3)
- 平均故障間隔(MTBF) 171,308時間 (PSE 3+)

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。