

Brochure

THALES

CYBERSECURITY

ハードウェア セキュリティ モジュール (HSM)

デジタルトラストの基盤

cpl.thalesgroup.com

HSMとは?

HSM(ハードウェアセキュリティモジュール)は、暗号鍵を保護するために特別に設計された専用デバイスです。HSMはトラストアンカーとして機能し、強固な耐タンパー性を備えたデバイス内で暗号鍵を安全に管理・処理・保管することにより、世界有数のセキュリティ意識の高い組織の暗号インフラを保護します。

強固な暗号基盤の必要性

信頼の基点(Root of Trust)は、暗号システムの基盤です。デジタルセキュリティは、データの暗号化と復号、署名と署名検証などの機能を実行する暗号鍵に依存しています。そのため、HSMなどの安全な環境内で暗号鍵と暗号処理の完全性を確保することが極めて重要です。

Luna HSM - デジタルトラストの基盤

Luna HSMは、30年以上の実績を誇るデジタルトラストの基盤であり、組織のデバイス、アイデンティティ、トランザクションを保護し、エコシステム全体の信頼を構築します。Luna HSMは、従来のテクノロジーと新たなテクノロジーの両方で、セキュリティと高いパフォーマンスを両立できるように設計されているため、アジリティ、使いやすさ、スケーラビリティを妥協する必要はありません。さらに次のようなメリットもあります。

- リスクの低減:** 専用設計で、認証取得済みの、クリプトアジリティに対応した強固なセキュリティアーキテクチャにより、重要なデジタルインフラを保護します。ITセキュリティの担当者として、強力な認証、ロール分離、「鍵をハードウェア内で保護する」アプローチにより、データとアイデンティティを保護できます。



- 柔軟性と可視性の確保:** 戦略的にデータとアイデンティティを保護することにより、暗号鍵、重要なデータ、デジタルアイデンティティを、その所在を問わず保護し、柔軟性と可視性を確保します。
- Luna HSMの容易な導入、プロビジョニング、管理:** 運用を効率化することで、SLAを満たし、ダウンタイムを削減します。現代の無人運用(lights-out)データセンター向けに設計されたLuna HSMは、運用効率に優れ、信頼性が高く、一元管理を実現します。
- 統合と開発の簡素化:** 多様なAPI、柔軟な導入オプション、優れたパフォーマンスを備え、テクノロジーパートナーとの、すぐに使えるハイブリッド統合により、何百ものアプリケーションを迅速に保護できます。

Luna HSMの特長

鍵の所在を常に把握

独自の「鍵をハードウェア内で保護する」アプローチにより、Luna HSMの耐タンパー性ハードウェア内で暗号鍵を安全に分離します。暗号の強度は暗号鍵に施されるセキュリティによって決まるため、Luna HSMは最高レベルの鍵セキュリティを念頭に設計されています。アプリケーションはクライアントを介してLuna HSM内の鍵とやり取りしますが、鍵がHSMの外部に出ることはありません。

コンプライアンス要件への対応

GDPRやeIDAS、PCI-DSSなど、どのようなコンプライアンス要件であってもLuna HSMはソリューションの一部です。Luna HSMは、コモンクライテリア、FIPS 140-3、ITIなど、業界最多の認証を取得しています。国際的に認められた、認証取得済みのHSM暗号基盤によってインフラ全体に確かな信頼をもたらします。

アプリケーション/ワークロードの実行場所を問わず鍵を保護

特定の場所やクラウドサービスプロバイダーに縛られることはありません。Luna HSMは、オンプレミス、クラウドベース、一部のクラウドサービスプロバイダーを通じて利用できる専用HSMなど、柔軟な導入オプションを提供します。これにより、鍵のオーナーシップと管理を維持しながら、セキュリティ、コンプライアンス、運用要件に最適なモデルを選択できます。

高パフォーマンスのユースケースに対応できるスケーラビリティ

最も要求の厳しいアプリケーションをサポートし、サービスレベルアグリーメント(SLA)を満たすために、高スループット要件にも対応します。

HSMリソースを容易に管理および監視

タレスのCrypto Command Centerで暗号リソースを管理します。これは、オンデマンドの監視、レポート、プロビジョニング、アラートを数分で実行できる一元化されたプラットフォームです。

投資対効果 (ROI) を拡大

数百種類の主要なエンタープライズアプリケーションと統合できる、業界最大規模のパートナーエコシステムを提供しています。さらに、PKCS #11、Java、OpenSSL、Microsoft、Ruby、Python、Goなど、幅広いAPIをサポートしています。

新しいテクノロジーを安全に保護

タレスの比類のない製品と機能の組み合わせにより、進化し続ける脅威から保護し、PKI、IoT、AI、デジタルアセット、コード署名、クラウド、PQC、5Gなどを支える、安全なデジタルトラストの基盤を構築します。

人手を最小限に抑えた無人運用を実現

最新のデータセンターにHSMを容易に導入し、管理できます。

ニーズに合わせてHSMを選択

すべてのLuna HSMに共通のアーキテクチャのメリットを得られます。同じ暗号処理を実行し、同じ統合、API、メカニズム、認証方式を利用するため、特定のHSMに合わせてアプリケーションを設計する必要がありません。また、必要に応じて、フォームファクター間で鍵を移動できる柔軟性があります。



タレスの汎用HSMポートフォリオ

次世代HSM「Luna 8」登場 ポスト量子時代のデジタルトラストの基盤

Luna Network HSM (ハードウェアセキュリティモジュール) で、機密データ、アイデンティティ、トランザクション、重要なアプリケーションを保護しましょう。Luna Network HSMは、暗号鍵を安全に保管・保護・管理するために設計された、量子安全性、高い信頼性、耐タンパー性を備えたアプライアンスであり、スケーラビリティに優れたマルチテナントセキュリティと市場をリードするPQC性能を提供します。

これらのネットワーク接続型HSMは、幅広いアプリケーションに容易に統合でき、既存および新たな暗号ユースケースやコンプライアンス要件に対応します。また、シームレスな導入を支援し、暗号インフラ全体の量子安全な信頼の基点 (Root of Trust) として機能します。

Luna 8は、タレスが新たに開発したHSMプラットフォーム上で提供される初の次世代HSMです。タレス独自設計の暗号プロセッサを搭載し、現在はネットワークフォームファクターで提供されています。最も厳格なセキュリティ要件に対応するように設計されており、FIPS 140-3 Level 3およびEUコモンクライテリアの認証取得に向けたプロセスが進行中です。

Luna 8の主なメリット

- **量子対応**: 既存の投資を保護しながら、ポスト量子暗号へのシームレスな移行を可能にします。
- **パフォーマンス**: 桁違いに高速な暗号処理により、最も要求の厳しいアプリケーションに必要なパフォーマンスを提供します。
- **スケーラビリティ**: エンタープライズ環境からハイパースケール環境まで容易に拡張でき、急速に増大する暗号ワークロードにも妥協することなく対応します。
- **将来への対応**: アップグレード可能なアーキテクチャにより、新しいアルゴリズム、標準、機能を容易に取り込むことができ、長期にわたり安全性、適応性、将来への対応力を維持します。
- **シームレスな移行**: Luna 7からLuna 8への移行では、既存のアプリケーションを変更する必要がなく、同じ周辺機器とインターフェースをそのまま利用できるため、既存のお客様もスムーズかつ安全に移行いただけます。



当社史上最速のHSM | 量子安全かつクリプトアジリティ対応 | マルチテナント対応でスケーラブルなアーキテクチャ
タレス独自設計の暗号プロセッサを搭載

Luna 7: 環境に合わせて選べる導入モデル

複数のフォームファクター。1つのデジタルトラストの基盤。



Luna Network HSM

Luna Network HSMは、高保証・耐タンパー性を備え、市場をリードするPQC性能を提供する、タレスのプレミアムなネットワーク接続型アプライアンスファミリーです。暗号鍵を保管・保護・管理することで、機密データと重要なアプリケーションを保護します。金融、医療、政府など規制の厳しい業界において、FIPS 140-3 Level 3、HIPAA、PCI-DSS、eIDAS、GDPR、BSI、NATO などのコンプライアンスおよび監査のニーズに対応します。



Luna PCIe HSM

Luna PCIe HSMは、高い信頼性と耐タンパー性を備えた薄型PCIeカードで、機密データと重要なアプリケーションの暗号鍵を保管・保護・管理します。専用設計された高性能暗号プロセッサへの専用アクセスをアプリケーションに提供します。このコスト効率の高いソリューションをサーバーやセキュリティアプライアンスに直接、容易に組み込むことで、FIPS 140-3 Level 3 検証済みの鍵セキュリティを実現できます。



Luna USB HSM

Luna USB HSMは、すべての鍵マテリアルをHSM内部にのみ保持することで、ポータブルアプライアンスとして業界トップクラスの鍵管理を実現します。小型のフォームファクターとオンボードの鍵保管を特長とし、特にオフラインでの鍵保管を必要とするお客様に適しています。



Luna Cloud HSM

[タレスData Protection on Demand](#) [オンラインマーケットプレイス](#)で提供されるLuna Cloud HSMは、物理的なHSMインフラの導入と管理が不要な、専用の暗号鍵保護を提供するクラウドベースのHSMサービスです。クラウド、オンプレミス、またはその両方を組み合わせた環境のいずれに導入する場合でも、すべてのLuna HSMが共通のアーキテクチャを採用しているため、認証取得済みでクリプトアジリティに対応した強固なデジタルトラストの基盤によって、重要なインフラを保護できます。

管理用オプション



Crypto Command Center

Crypto Command Centerは、オンプレミス、ハイブリッド、クラウド環境向けの完全な監視、レポート、管理ツールです。Luna Network HSMの暗号リソース管理を一元化し、ITセキュリティインフラのコストを削減できます。

追加のHSMオプション



ProtectServer HSM

ネットワーク接続型およびPCIeフォームファクターで提供されるProtectServer HSMは、暗号鍵を侵害から保護するとともに、暗号化、署名、認証サービスを提供するように設計されています。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、HSMの安全な領域内で実行できる、独自の柔軟性を提供します。

タレスへのお問い合わせ

Luna汎用HSMの詳細や、最新のテクノロジーを活用したアプリケーションの保護、ユーザー・デバイス・インフラのセキュリティ確保については、タレスまでお問い合わせください。オンプレミス、クラウド、ハイブリッド、マルチクラウドなど、さまざまな環境でデータとデジタルアイデンティティを保護する方法についても、お気軽にご相談ください。

タレスについて

タレスはサイバーセキュリティのグローバルリーダーとして、世界で最も信頼される組織が、重要なアプリケーション、データ、ID、ソフトウェアを場所を問わず大規模に保護できるよう支援しています。タレスの統合プラットフォームを通じて、リスクの可視化、サイバー攻撃の防御、そしてコンプライアンスギャップの解消を可能にし、毎日数十億人の消費者に安心で信頼性の高いデジタルエクスペリエンスを提供します。



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、
cpl.thalesgroup.com/ja/contact-usをご覧ください。

cpl.thalesgroup.com

