Solution Brief

THALES
CYBERSECURITY

タレス Luna HSM によるデジタル資産の保護

高まるリスクと変化する規制要件に対応するデジタルトラストのハードウェア基盤

cpl.thalesgroup.com

THALES

CYBERSECURITY

デジタル資産とは？

デジタル資産とは、デジタル形式で表現・取引される、あらゆる形態の価値を指します。これには、決済や取引に利用される暗号資産やステーブルコインに加え、有価証券、預金、実物資産などをトークン化した資産も含まれます。これらの資産は、ブロックチェーンなどの分散型プラットフォーム上で作成・管理・交換され、分散化、プログラマブルマネー、デジタル所有権を基盤とする現代のデジタル金融の土台を形成しています。

はじめに：デジタル資産の急速な普及と高まる金融リスク

デジタル資産は、いまや世界の金融において重要な位置を占めるようになっています。ステーブルコインの取引額は、現在VisaとMastercardの合計取引額を上回っており、国際的なブロックチェーン決済量は年間6兆ドルを超えています（Delphi Digital, 2025）。また、分散型台帳プラットフォーム上での実物資産（RWA）や金融資産のトークン化も勢いを増しており、資本市場、決済、クロスボーダー決済などの分野で、金融機関による実証実験が拡大しています（Bank for International Settlements, 2024）。その結果、銀行、決済事業者、資本市場に携わる金融機関は、顧客ニーズに応えるとともに、急速に進化する市場環境で競争力を維持するため、デジタル資産戦略の推進を加速させています。

このような成長に伴い、強固なセキュリティ基盤の重要性も高まっています。2025年には、暗号資産関連のハッキングによる損失は約34億ドルに達し、デジタル資産業務の拡大に伴う堅牢な鍵管理とセキュリティ統制の必要性が改めて浮き彫りとなりました。成熟したセキュリティプログラムを持つ中央集権型プラットフォームにおいても、秘密鍵は依然として重大なリスク要因の一つです。2025年第1四半期には、カストディ型取引所やデジタル資産プラットフォームなどの中央集権型サービスが、盗難被害総額の88%を占めており、秘密鍵の操作をハードウェアレベルで保護する重要性が示されています（Chainalysis, 2025）。

デジタル資産の利用が規模と複雑さの両面で拡大し続ける中、金融機関には、秘密鍵の保護を中核に据えたセキュリティアーキテクチャが求められています。信頼性と実績を備えたHSM（ハードウェアセキュリティモジュール）はこの基盤となり、鍵を保護するためのハードウェアベースの信頼の起点（Root of Trust）を提供するとともに、鍵を中心に構築されるデジタル資産の各種ワークフローを支えます。

課題：セキュリティ上のギャップと世界的な規制強化

デジタル資産への取り組みが加速する一方で、多くの金融機関は依然として、安全な大規模運用に必要な統制の整備が追いついていません。秘密鍵は、不正アクセスを防止しながら、大量の署名処理、複数当事者による承認ワークフロー、職務分掌をサポートできる方法で生成・保管・利用する必要があります。ソフトウェアベースの鍵保管方式は、もはや十分とは言えません。攻撃者が不正や窃取の主要な手段として秘密鍵を狙うようになっている現在では、不十分になりつつあります。

同時に、規制上の要請はより厳格になり、主要な金融センター間で規制の整合化が進んでいます。たとえば、香港証券先物委員会（SFC）の「仮想資産取引プラットフォームガイドライン」、シンガポール金融管理局（MAS）の各種通知、EUのMiCA、ドイツ連邦金融監督庁（BaFin）のガイドライン、スイス金融市場監督機構（FINMA）の要件などでは、カストディ管理、鍵管理、オペレーショナルレジリエンス、監査可能性に関する明確な要件が定められています。そのため金融機関は、デジタル資産インフラが、導入形態を問わず、一貫したポリシー適用、検証可能な鍵保護、透明性の高いガバナンスを実現できることを証明する必要があります。

これらの要件を満たすには、秘密鍵を保護し、トランザクション署名を適切に管理するとともに、イノベーションのスピードを損なうことなくコンプライアンスを支援する、信頼できるセキュリティ基盤が求められます。認証取得済みのHSM（ハードウェアセキュリティモジュール）は、耐タンパ性を備えたハードウェア内で重要な処理を保護し、規制当局や金融機関のリスク管理チームが求める高い信頼性を提供することで、こうしたセキュリティ基盤を実現します。

ソリューション：Luna HSMによる金融機関レベルのデジタル資産セキュリティ

タレスLunaHSMは、ハードウェアベースの信頼の起点（Root of Trust）を提供することでデジタル資産を保護し、秘密鍵と署名処理を、認証取得済みの耐タンパ性を備えたハードウェア内で安全に保護します。オンプレミスまたはサービスとして提供され、現代のデジタル資産プラットフォームのニーズに対応します。また、実績ある安全な鍵生成を提供し、署名アプリケーションで使用される秘密鍵を、お客様が所有するFIPS認証取得済みのハードウェア内で保護します。これにより、鍵はアプリケーション層、オンラインシステム、クラウド環境といった攻撃の多くが発生する領域から完全に隔離された状態で保持されます。

Luna HSMは、耐タンパ性を備えたハードウェア内で鍵の生成、保管、署名処理を行うことで、さまざまなデジタル資産カストディモデルのセキュリティを強化します。初期のデジタル資産プラットフォームの多くは、ソフトウェアのみのシンプルさを優先していましたが、現在では、機関顧客や規制当局は、秘密鍵を認証取得済みのHSMによって保護することを強く求めるようになっています。オンプレミスまたはサービスとして導入でき、標準APIを介して利用できるため、ハードウェアベースのセキュリティは、進化するカストディアーキテクチャにも柔軟に対応し、運用の制約となることはありません。これにより金融機関は、ソフトウェアベースの鍵管理ワークフローを支える検証可能な信頼の起点（Root of Trust）を確立し、単一障害点を減らし、承認、署名ポリシー、ガバナンスルールを一貫して適用できます。このアプローチは、金融機関レベルのデジタル資産運用に求められる統制と保証を実現します。

Luna HSMは、主要なカストディプラットフォーム、ブロックチェーン基盤、ウォレット技術、トークン化エンジンと連携できます。導入形態は、オンプレミス、クラウド、または**タレスData Protection on Demand (DPoD) クラウドマーケットプレイス**から選択でき、いずれの場合も一貫したセキュリティ、ガバナンス、運用管理を維持できます。このように、導入モデルを柔軟に選択できることに加え、クリプトアジリティと耐量子セキュリティが組み合わさることで、金融機関は信頼、パフォーマンス、規制適合性を強化しながら、デジタル資産の機能を拡張するための強固な基盤を構築できます。

メリット：

鍵の完全なオーナーシップと認証による保証：鍵は、お客様が所有するFIPS認証およびコモンクライテリア認証を取得したLuna HSM内で生成、保管、使用されます。署名処理も、最高水準の保証を備えたハードウェア内で実行されます。Luna HSMはクリプトアジリティを備えており、NISTが標準化した耐量子暗号アルゴリズムをサポートするほか、今後登場する暗号方式にも柔軟に対応できます。

金融機関向け環境とのシームレスな連携：Luna HSMは、規制対象インフラと連携し、多様なカストディアーキテクチャに対応したカストディプラットフォームやブロックチェーンシステムと接続できます。これにより、セキュリティ、ガバナンス、監査の各チームの運用負荷を軽減します。

ホット、ウォーム、コールドの各署名ワークフローに対応：金融機関は、リアルタイムのオンライン承認から、完全オフライン署名まで、管理された仕組みで運用できます。この柔軟性により、多様なリスクモデルやカストディ方式に対応できます。

高度なガバナンスとポリシー管理：LunaHSMは、複数承認による署名、アドレスホワイトリスト、トランザクション上限など、きめ細かなポリシー制御を実現します。また、改ざん不能（イミュータブル）なログにより、監査可能性と規制対応の透明性を確保します。

資産のトークン化とスマートコントラクトへの対応：Luna HSMは、トークン化された資産のオンチェーンライフサイクルを保護し、ステーブルコインや実物資産（RWA）のトークン化を含む、スマートコントラクトとのやり取りに必要な署名処理をサポートします。

デジタル資産エコシステム全体との接続性：LunaHSMは、オンランプ、オフランプ、流動性プロバイダー、発行者、決済プラットフォームと連携しながら、秘密鍵をハードウェア内で安全に保護します。

グローバル規制への対応を前提に設計：LunaHSMは、SFC、MAS、MiCA、BaFin、FINMAなどのフレームワークへの対応を支援します。鍵、テナント、ポリシーをきめ細かく分離できるため、事業部門、地域、規制要件ごとに環境を適切に区分して管理できます。

デジタル資産向けLuna HSMの導入モデル

クラウド、オンプレミス、ハイブリッド環境に対応した、デジタル資産向けLuna HSMの柔軟な導入オプション：

デジタル資産環境にLuna HSMのセキュリティを提供する多様な導入モデル

Luna HSMは、デジタル資産エコシステム全体において、鍵生成、アクセス制御、トランザクション署名を担う認証取得済みのハードウェアベースの信頼の起点（Root of Trust）を提供し、さまざまなフォームファクターで利用可能です。

まとめ

デジタル資産が金融機関の中核業務へと浸透するにつれ、秘密鍵の保護の重要性はかつてないほど高まっています。鍵の侵害は依然としてデジタル資産プラットフォームにおける金銭的損失の最大の要因の一つです。タレスLuna HSMは、お客様が所有する認証取得済みのハードウェア内で鍵生成、保護、トランザクション署名を実行することにより、金融機関がこうしたリスクに対処するための信頼できる手段を提供します。FIPS認証およびコモンクライテリア認証を取得済みのHSM内で鍵を保持することで、セキュリティ態勢を強化し、規制要件に対応し、不正利用や盗難のリスクを大幅に低減します。Luna HSMは、主要なカストディプラットフォーム、ブロックチェーンプラットフォーム、トークン化プラットフォーム、広範なデジタル資産エコシステムと連携します。クリプトアジリティと耐量子セキュリティを基盤とし、柔軟な導入モデルで利用可能なLuna HSMは、デジタル資産の活用における信頼の起点（Root of Trust）を提供します。これにより、金融機関は、安全性を確保しながら運用規模を拡大できるだけでなく、顧客や規制当局に対して適切な統制を実証できます。

タレスについて

タレスはデータセキュリティのグローバルリーダーとして、世界中で高い信頼を得ているさまざまな組織が、あらゆる場所で重要なアプリケーション、機密データ、およびIDを包括的に、かつ最高の投資対効果（ROI）で保護できるよう支援しています。フォーチュン・グローバル500企業の58%を含む3万社以上の顧客を抱え、そのソリューションは世界148カ国で導入されています。タレスは、革新的なサービスと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保証の高いデジタルエクスペリエンスを提供します。

Luna HSMの詳細はこちら

DPoD上で提供されるHyperledger Fabric向けLuna クラウドHSMの無料トライアルはこちら

cpl.thalesgroup.com

お問い合わせ先 – 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。