cpl.thalesgroup.com

THALES

フレセッツ株式会社：事業者向けウォレット管理サービスの秘密鍵をHSMで管理より高度なセキュリティレベルを達成

サマリ

暗号資産（仮想通貨）市場が再び活発化しています。銀行や証券会社等の既存金融機関の参入が予想されたり、セキュリティトークンやステーブルコイン等、暗号資産の枠組みにとどまらないデジタル資産も脚光を浴びるなか、市場拡大の最大要件として、セキュリティ基盤の強化に期待が集まっています。

ブロックチェーンにおいてセキュリティの要となるのは秘密鍵管理です。暗号資産の取引所・大規模事業者向けにウォレット管理システムを提供するフレセッツ株式会社（以下フレセッツ）は、秘密鍵をHSM（Hardware Security Module）で管理できる機能強化を実現しました。

フレセッツは、Thales Protect Server HSMを採用することで、各事業者の個別ニーズにもきめ細かく対応しつつ、最も強固で安全な鍵管理の仕組みを構築することに成功したのです。

選定のポイント

フレセッツが提供するウォレットサービスは「Fressets EWM System™」。複数のホットウォレット[1]とコールドウォレット[1]をそれぞれマルチシグ[2]で複合利用できる世界初の事業者向け仮想通貨ウォレット・パッケージです（国内特許取得）。

すでに、ビットコイン、ビットコインキャッシュ、イーサリアム、イーサリアムERC20ベーストークン、ライトコイン、リップル等の通貨に対応しており、日本で最も豊富な導入実績を誇ります。また、コールドウォレット、マルチシグ対応を順次加えてセキュリティ強化を重ねてきた企業姿勢・技術力が評価され、暗号資産をはじめとしたデジタル資産ウォレットサービスの業界標準と認識されています。

一方で、暗号資産はこれまでに数多くの流出事故が起きており、市場規模が拡大するほど悪意ある攻撃を受けるリスクも増大します。市場拡大の機運を受けて、フレセッツはHSM対応による、よりセキュリティレベルの高いウォレット実現に踏み切りました。

HSMを選んだのは、電子鍵を格納する専用ハードウェアを用いることで、セキュリティレベルを金融機関のコンプライアンス標準のレベルにまで高めることができるからです。

Fressets

「多くの事業者がしっかりとしたウォレットシステムを導入・運用されている一方で、サーバールームを破壊して侵入するなど、物理的な攻撃については対策が十分ではありません。物理的に秘密鍵を保護できるHSMは、今後の市場拡大を支える重要なテクノロジーです。フレセッツがこれから海外展開していくうえでも、有力なソリューションとなるでしょう。」

– フレセッツ株式会社
代表取締役 CEO　柚木庸輔 氏

1　ホットウォレット、コールドウォレット
仮想通貨を一時的に保管する財布がウォレット。インターネットに接続されているのがホットウォレット、インターネットから遮断された状態にあるのがコールドウォレット。Fressets EWM System™は、オンライン環境とオフライン環境の中継に紙媒体（QRコード）を用いることでコールドウォレットの署名作業を完全オフライン化している

2　マルチシグ
Multi Signatureの略。暗号資産の送金等にあたって複数の承認者による署名（送金の承認）を必須とする技術。1つの秘密鍵で署名を行うシングルシグに比べてセキュリティレベルが高く、内部不正やヒューマンエラーを未然に防げる

また、インターネット経由でサーバーに侵入されても秘密鍵を取り出すことは原理的に不可能であること、物理的な盗難に遭っても外部からの解析による秘密鍵窃取は不可能であること、複数の秘密鍵を同一のHSM筐体に保管できるため複数人の承認（電子署名）を要求することができ内部犯行を防止できること、専門的なIT知識がなくとも安全に秘密鍵を保管できることーーなども評価しました。

さらに、各社のHSMやHSM以外のハードウエアウォレットを比較検討したうえで、タレスのHSMを選定したのは、第1に、ワールドワイドでのシェアの高さ、実績、知名度を重視したためです。金融機関にも導入実績が豊富で、事業者様が安心してご利用いただけます。

第2に、「カスタマイズ可能なHSM」としてThales Protect Server HSMを選びました。

Fressets EWM System™は、暗号資産ごとに専用のウォレット・パッケージを開発してオンプレミスまたはSaaSで提供するサービスです。実装を作り込むことで各事業者のビジネスメリットを創出するサービスであるため、セキュリティを担保したままで柔軟に機能拡張のできるThales Protect Server HSMが必要でした。

ソリューション

HSMを組み込み可能とするFressets EWM System™のアップデートは、2020年1月に完了しました。

効果はすぐに現れました。

従来技術ではブロックチェーンレイヤーでのマルチシグを実装できなかったイーサリアムが、HSMを活用することで、完全オフライン環境でのセキュアなマルチシグ実装に成功したのです。

フレセッツが用いたのは、HSMと閾値署名技術です。閾値署名とは、複数の承認者が鍵シェアを互いに明かさずに通信して、秘密鍵を一度も復元することなく、電子署名を生成する技術です。今回、この閾値署名をHSM上で実現したことで、完全オフライン環境のコールドウォレットとして、きわめて安全性の高いマルチシグを実現できました。

HSM対応のFressets EWM System™は、機能強化を検討するサービス導入済み事業者はもちろんのこと、ウォレットシステムを含む取引システムを新規に構築しようとしている銀行・証券会社等から多数の引き合いを受けています。

暗号資産のみならず、ブロックチェーンによって管理されるデジタル資産全体の市場規模拡大に向けて、フレセッツのセキュリティ基盤は万全の準備が整いました。

課題

- 暗号資産市場が活性化している。市場規模が拡大すれば脅威も増大するため、セキュリティ強化が不可欠
- 事業者の多くは、サーバールーム破壊等の物理的な攻撃に対しては対策が十分とは言えない
- 事業者向けウォレット管理サービスを、コールドウォレット、マルチシグ対応で順次強化してきたが、HSM対応を加えて物理的な攻撃に備えるとともに、金融機関のコンプライアンス標準レベルのセキュリティを達成したい

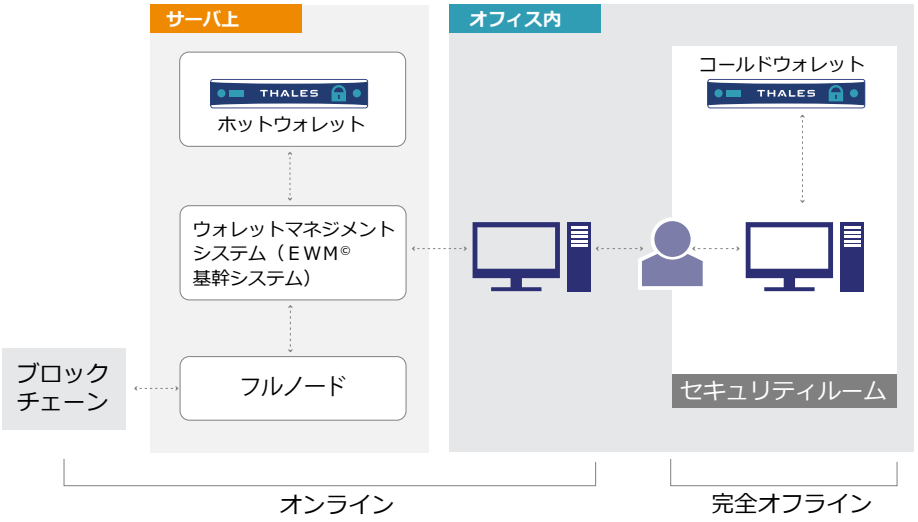
ソリューション

- 事業者向けウォレット管理サービスで初めて、秘密鍵をHSMで管理できる機能強化を実現
- カスタマイズができる「Thales Protect Server HSM」を採用することで、各事業者の個別ニーズにもきめ細かく対応しつつ、強固な鍵管理の仕組みを開発

メリット

- ウォレット管理サービスの秘密鍵管理に、金融機関のコンプライアンス標準レベルのセキュリティを実現
- 金融機関への導入実績も豊富なタレスのHSMは知名度も高く、事業者にセキュリティレベルを納得してもらいやすい
- Thales Protect Server HSMは、セキュリティを担保したままで柔軟に機能拡張ができて、事業者のビジネスユースに沿った作り込みができる
- 開発にあたっては、機能拡張部分が想定通りに動作したので予定通りの期間で開発を完了できた。ドキュメント類もしっかりしているので開発しやすかった
- 従来技術ではブロックチェーンより下位レイヤーでのマルチシグを実装できなかったイーサリアムにおいて、HSMを活用することで完全オフライン環境でのマルチシグ実装に成功
- 新規参入を考える銀行、証券会社等から多数の引き合いあり。暗号資産市場の規模拡大に向けて、フレセッツは準備万端

Fressets EWM System©におけるHSMの活用例



Thales Protect Server HSMは、秘密鍵をコールド環境で安全に保管すると同時に、ホットウォレットと連携して、暗号化・デジタル署名サービス等を高速処理する

タレスについて

プライバシーを保護するためにあなたが信頼を寄せている人達は、そのデータを保護するためにタレスを利用 しています。データセキュリティに関して、組織が重要な決断を下さなければならない瞬間はますます増えてい ます。それ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、タレ スを利用すればデジタルトランスフォーメーションを推進できます。

決断の瞬間のための、確実なテクノロジー。

© Thales - January 2021 • EH V6

> cpl.thalesgroup.com <

お問い合わせ先 – 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。