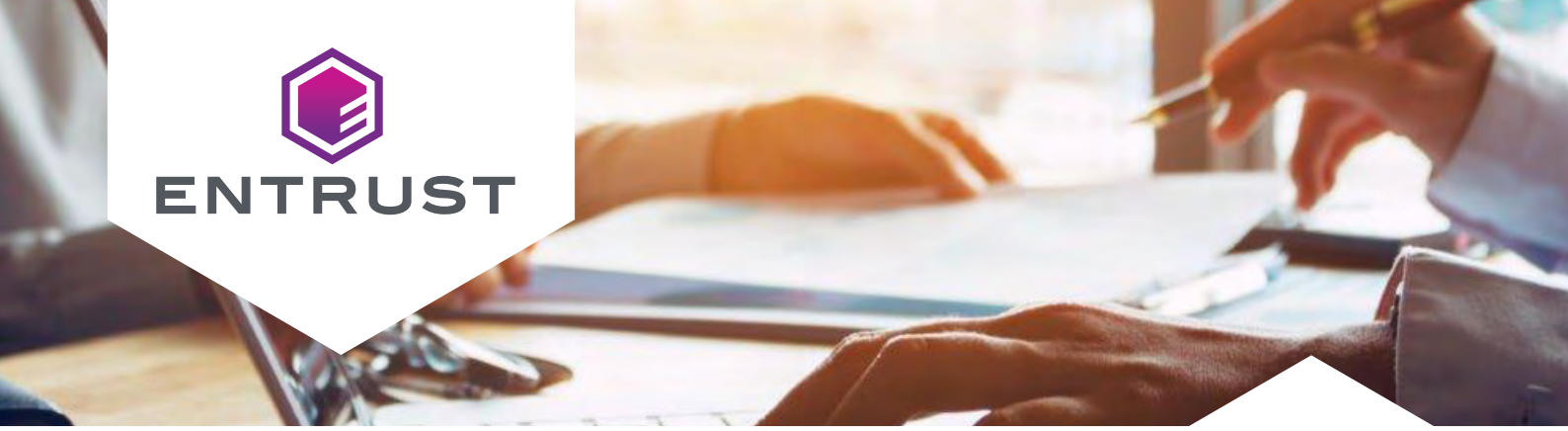

ブロックチェーンの保護

ブロックチェーンの高保証セキュリティ

ハイライト

- ハードウェアセキュリティモジュール（HSM）を信頼の基点として、機密コードを処理する
- 多様な楕円曲線暗号（ECC）アルゴリズムで、増加するアプリケーションをサポートする
- クラスターのHSMの展開で、暗号化機能を拡張する
- Entrust専門サービスで実装を迅速化する

ブロックチェーン：機会と障壁

ブロックチェーンと分散型台帳テクノロジーは、確立された組織と新しく市場参入する組織の両方にとって重要な新しい機会を提示します。ブロックチェーンの実装は、特定のビジネスのユースケースを根本的に変化させ、運用の簡素化、コスト削減、トランザクションの合理化が可能になります。

ブロックチェーンを広く採用する上での主な障壁の1つは、セキュリティです。清算・決済、支払い、医療、取引、財務、政府規制への準拠などのユースケースは、高保証セキュリティを必要とします。

組織はブロックチェーンの新しく革新的なユースケースを継続的に発見するため、セキュリティを最初から組み込む必要があります。ブロックチェーンに送信された各トランザクションが確実にデジタル署名される場合のみ、私たちはこの革新的なテクノロジーの使用を促進し、約束された報酬を得ることができます。そのため、ブロックチェーンプロセスで使用される署名鍵を保護し、コンセンサスロジックを改ざんから保護することが不可欠です。

詳細をチェック：ENTRUST.COM/ja/HSM

ブロックチェーンの保護

鍵を保護し、システムを保護する

他の暗号化インフラストラクチャと同様に、基盤となる鍵を保護することは、ブロックチェーンシステムのセキュリティを確保するために最も重要です。ブロックチェーンシステムの成功には、HSMによる強力な鍵保護と、分散型台帳モデルの要求をサポートできる拡張性が必要です。

当社のアプローチ

Entrustは、ブロックチェーンの実装に関連する基本的なセキュリティの課題である、署名鍵とコンセンサスロジックの保護に取り組みます。nShield® HSMを使用することで、企業は以下が可能になります。

- secp256k1、Edwards Curve (Ed25519) などのECCアルゴリズムを使用して、自信を持ってトランザクションに署名する
- FIPS認定の改ざん防止ハードウェア境界内で署名鍵を保護する
- nShield HSMの独自のCodeSafe機能を使用して、署名プロセスを裏付けるビジネスロジックを保護する

ブロックチェーンに送信されたトランザクションは、秘密鍵を使用してデジタル署名され、エントリが本来のユーザーからのものであることを確認し、改ざんを防ぎます。Entrust nShield HSMは、秘密鍵の発行と失効に使用される基盤のルート鍵を保護します。

承認されたコンプライアンスを満たすトランザクションのみがブロックチェーンに追加されるようにするために、nShield HSMの独自のCodeSafe機能は、コンセンサスロジックコードを実行できる安全な環境を提供します。CodeSafeは、nShield HSMの安全な境界内に格納されているため、最も機密性の高いコードに対してFIPS140-2レベル3認定の保護を提供します。

さらに、Entrust専門サービスチームは、数十年の経験を生かして、nShield HSMの安全な基盤上に構築された安全かつ効果的なブロックチェーンアプリケーションの実装を支援できます。

Entrust HSM

Entrust nShield HSMは、最高のパフォーマンスを発揮し、非常に安全で、簡単に統合できるHSMソリューションのひとつであり、規制への準拠を促進すると同時に、企業、金融機関、政府機関に最高レベルのデータセキュリティとアプリケーションセキュリティを提供します。当社独自のSecurity World鍵管理アーキテクチャは、鍵へのアクセスおよび鍵の使用を厳重にかつきめ細かく制御します。

詳細

Entrust nShield HSMの詳細については、**entrust.com/ja/HSM**をご覧ください。アイデンティティ、アクセス、通信、データに関するEntrustのデジタルセキュリティソリューションの詳細については、**entrust.com/ja**をご覧ください。

詳細は下記URLをご覧ください:
entrust.com/ja/HSM

ENTRUST

お問い合わせ:
HSMinfo@entrust.com