

Entrust 暗号セキュリティプラットフォーム

ハイライト

すべての暗号資産を1つのプラットフォームで管理

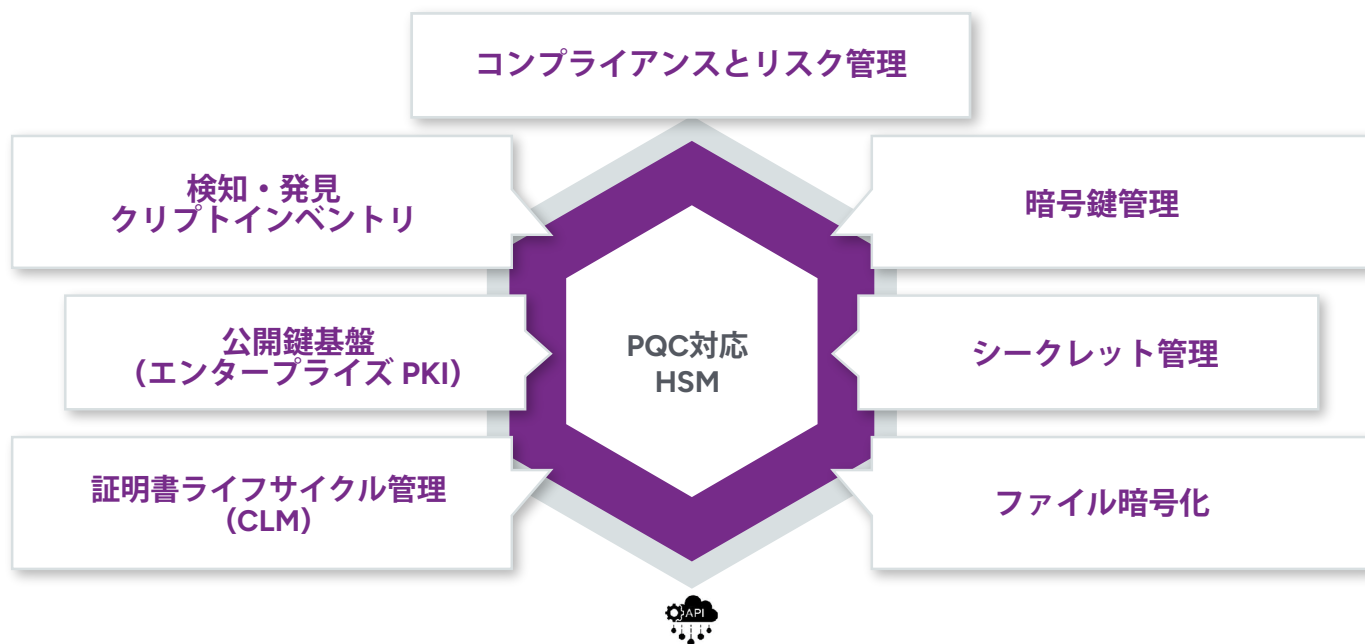
暗号技術は、身元確認、データの完全性、可用性、および安全な通信において極めて重要です。組織が管理する鍵、秘密情報、証明書が増加する中、強固なライフサイクル管理と資産の発見・管理は、侵害の防止、コンプライアンスの確保、グローバルなITインフラ全体でのセキュリティ維持に不可欠です。

Entrust暗号セキュリティプラットフォーム(CSP)は、PKI、証明書ライフサイクル管理、鍵管理、シークレット管理、ハードウェアセキュリティモジュールを運用するための豊富な機能を組み合わせ、すべてを耐量子の統合された単一システムで提供することで、暗号管理を一元化することができます。

ITセキュリティにおける今後の懸念事項

- **TLS証明書の有効期限が47日に短縮(2029年)**:今までは人手で行っていた管理も、1か月半で有効期限を迎えるとなると、かなり管理が難しくなります。CSPはライフサイクル管理を自動化するため、そのほかのIT業務に時間を費やすことができます。
- **「今収穫し、後で解読」するハーベスティング攻撃が現在進行中**:耐量子暗号(PQC)への対応の第一歩は暗号資産の把握にあります。合併や部署ごとに異なるシステムの利用などで資産が分散されている企業も多いことでしょう。CSPは暗号資産の検知および発見をすることができるため、簡単に暗号資産をすべて把握することが可能です。

Entrust暗号セキュリティプラットフォーム(CSP)の機能



単一のプラットフォーム

暗号セキュリティプラットフォームは、下記のような機能を提供します。

企業全体の可視性: 暗号資産の検索およびモニタリング、監査基準の更新、セキュリティ監視強化のためのアラート受信を、すべて一元管理されたダッシュボードから確認することができます。

暗号化リスク管理: 分散した機能、部門、チーム全体にわたって暗号化リスクの状況を自動的に評価し、ポリシーを適用し、鍵、シークレット、証明書を保護します。

スケーラブルなアーキテクチャ: 最新の標準規格に対応した高性能で将来を見据えた暗号化ソリューションを、オンプレミスおよびマネージドサービスのオプションで展開します。

相互運用可能: オープンAPIによるカスタマイズを可能にしながら、トップクラスのセキュリティ、ID、IT管理システムとの広範な統合を実現します。

コンプライアンスの強化: 金融業界など、規制の多い業界では特に、規制の更新にすぐに対応しなくてはならず、何が最新で何が準拠できているのか確認に時間を取られます。暗号セキュリティプラットフォームでは設定された規制を自動的に更新し、準拠の状態をモニタリングすることができます。

どのように暗号セキュリティプラットフォームが機能するかを、ぜひ簡単なデモをお試しください。



日本語デモ

